DIGITAL BANKING

Navneet Kumar
Debasish Ray

Digital Banking

Digital Banking

Navneet Kumar
Debasish Ray

ACADEMIC
UNIVERSITY PRESS

Digital Banking

Navneet Kumar, Debasish Ray

This edition has been published in arrangement with Books Arcade, India

ACADEMIC
UNIVERSITY PRESS

4378/4-B, Murarilal Street, Ansari Road, Daryaganj, New Delhi-110002.
Ph. No: +91-11-23281685, 41043100, Fax: +91-11-23270680
E-mail: academicuniversitypress@gmail.com

Year of Publication 2023 (Revised)

ISBN : 978-93-95546-63-8

CONTENTS

Chapter 1. An Overview of the Concept of Digital Banking..... 1
— Debasish Ray

Chapter 2. Investigation of Digital Banking Infrastructure in Digital Banking..... 10
— Dr. Zuleika Homavazir

Chapter 3. Analysis of Digital Banking Channels and Platforms..... 17
— Prof. Bhargavi Deshpande

Chapter 4. An Overview of the Concept of Information Technology in Banking System 25
— Meena Desai

Chapter 5. Explain the Role of Reserve Bank of India in Digital Banking and Technology 33
— Dr. Varsha Agarwal

Chapter 6. Analysis of Network Operating System in Digital Banking System 41
— Hansika Disawala

Chapter 7. Investigation of the Concept and Significance of Digital Banking Ecosystem 49
— Dr. Malcolm Homavazir

Chapter 8. Analysis of Technological Foundations in Digital Banking..... 57
— Parag Amin

Chapter 9. An Overview on the Rise of Mobile Wallets and Contactless Payments..... 65
— Kshipra Jain

Chapter 10. Investigation of Customer Experience in Digital Banking..... 74
— Prof. Ameya Ambulkar

Chapter 11. Investigation on the Concept of Cybersecurity in Digital Banking 82
— Shefalika Narain

Chapter 12. Exploration of the Role of Data Analytics in Digital Banking..... 89
— Suresh Kawitkar

CHAPTER 1

AN OVERVIEW OF THE CONCEPT OF DIGITAL BANKING

Debasish Ray, Director
ISME, ATLAS SkillTech University, Mumbai, India
Email id- debasish.ray@atlasuniversity.edu.in

ABSTRACT:

Due to changing customer expectations and technological improvements, digital banking is a revolutionary change in the financial industry. With the use of digital platforms, clients may handle their financial activities without the need for physical branches by using a wide variety of online and mobile banking services. Digital banking has brought about several developments that have improved accessibility and efficiency in banking, such as mobile payments, online account management, and automated financial services. Digital banking makes use of technology like mobile applications, online banking, and artificial intelligence to improve consumer engagement, simplify processes, and provide a flawless user experience. The emergence of digital-only banks, a growth in the use of fintech products, and the incorporation of cutting-edge security measures to safeguard private financial information are characteristics of the move towards digital banking. This summary emphasizes the salient features of digital banking, stressing its effects on financial organizations as well as customers. It also covers its advantages, difficulties, and future possibilities. Driven by continued technical breakthroughs and shifting market factors, digital banking is positioned to play a vital role in defining the financial services landscape as the banking sector continues to grow.

KEYWORDS:

Artificial Intelligence, Digital-Only Banks, Fintech Solutions, Mobile Payments, Online Banking.

INTRODUCTION

The financial services sector has seen a radical change with the introduction of digital banking, which has completely changed the way that banking services are provided, used, and administered. Fundamentally, digital banking is the process of incorporating digital technology into every facet of banking operations, enabling financial institutions to do business online and via mobile platforms. This change in focus from conventional banking, which was typified by physical branches and in-person contacts, to a digital-first strategy is a reflection of greater improvements in technology as well as shifting customer expectations [1], [2]. Automated Teller Machines (ATMs) were the first electronic banking devices, and their debut in the 1960s marked the beginning of the history of digital banking.

Originally intended to provide basic financial services outside of normal branch hours, these devices set the stage for later, more advanced digital alternatives. The introduction of online banking in the 1990s allowed users to access their accounts and conduct transactions using the Internet, which was a huge advancement. The spread of internet connectivity and personal computers, which together changed how people interacted with their banks, was the driving force behind this growth. Financial institutions started making significant investments in digital technology as Internet use increased in the early 2000s, which paved the way for the creation of extensive online banking systems. Convenience and accessibility were greatly increased by these platforms, which let users manage their accounts, transfer money, pay bills, and apply for financial products from the comfort of their homes [3], [4]. The development of mobile banking apps, which further transformed the banking experience by providing on-the-go access to

financial services, was accelerated by the proliferation of smartphones and mobile technology. With the advent of mobile banking applications, consumers may now use their smartphones or tablets for a variety of transactions, making them a crucial part of digital banking. Numerous important variables, such as the rising need for more control over financial management, the expanding acceptance of digital technology, and the increasing demand for convenience, have contributed to this transition towards mobile and online platforms.

Several essential elements and technologies are reshaping the landscape of digital banking as it continues to develop. The creation and use of cutting-edge core banking technologies, which serve as the foundation for financial institutions' digital operations, are essential to digital banking. These systems manage essential tasks including data storage, account administration, and transaction processing. They are designed to easily interact with digital channels to provide a cohesive client experience [5], [6]. The ability to store and handle enormous volumes of data on a flexible and scalable infrastructure is made possible by cloud computing, which has become a key component of digital banking.

Banks may save costs, increase operational efficiency, and quickly roll out new services and features by using cloud-based solutions. Digital payment systems, which provide safe and effective transactions across a variety of channels, such as contactless payments, digital wallets, and electronic money transfers, have also grown to be essential components of the digital banking ecosystem. These payment methods support the overarching objective of becoming a cashless society by facilitating smooth transactions. The emergence of fintech technologies, which are transforming the financial services industry, is intimately associated with the idea of digital banking.

Fintech enterprises use state-of-the-art technology, like blockchain, artificial intelligence (AI), and machine learning, to provide creative solutions that improve the effectiveness, safety, and usability of financial services. For example, the application of AI and machine learning in fraud detection, risk management, and customized client experiences is growing. With its decentralized and unchangeable structure, blockchain technology offers viable answers for safe and transparent transaction processing, especially in domains like international money transfers and digital identity authentication [7], [8]. Neobanks and challenger banks are two examples of the new business models that have emerged as a result of the fintech technologies' integration with conventional banking operations.

Neobanks, which only have online operations and no physical branches, provide a variety of financial services via digital channels with an emphasis on user-friendly design and affordable prices. Conversely, challenger banks are usually digital-only institutions that take on the established players in the banking industry by offering creative solutions and better client experiences [9], [10]. Digital banking offers several advantages, such as increased convenience, cost savings, and better client experiences, but certain issues need to be resolved. Due to the digital nature of banking operations, organizations and clients are vulnerable to several dangers, including identity theft, data breaches, and hacking. For this reason, cybersecurity is still a major issue.

Banks must put strong security measures in place, such as encryption, multi-factor authentication, and frequent security audits, to reduce these threats. Another major obstacle is regulatory compliance, which requires financial firms to manage a complicated web of rules intended to safeguard customers and maintain the integrity of the financial system. Maintaining confidence and avoiding financial and legal repercussions depend on compliance with data privacy rules, know-your-customer (KYC) regulations, and anti-money laundering (AML) regulations. Furthermore, the effective use of digital banking systems depends heavily on

customer uptake and confidence. While many consumers find digital channels to be convenient, others could be reluctant to accept new technology because they worry about privacy, security, and the loss of in-person connections. For this reason, financial institutions need to make investments in clear communication, consumer education, and assistance if they want to allay these worries and increase confidence in their digital products.

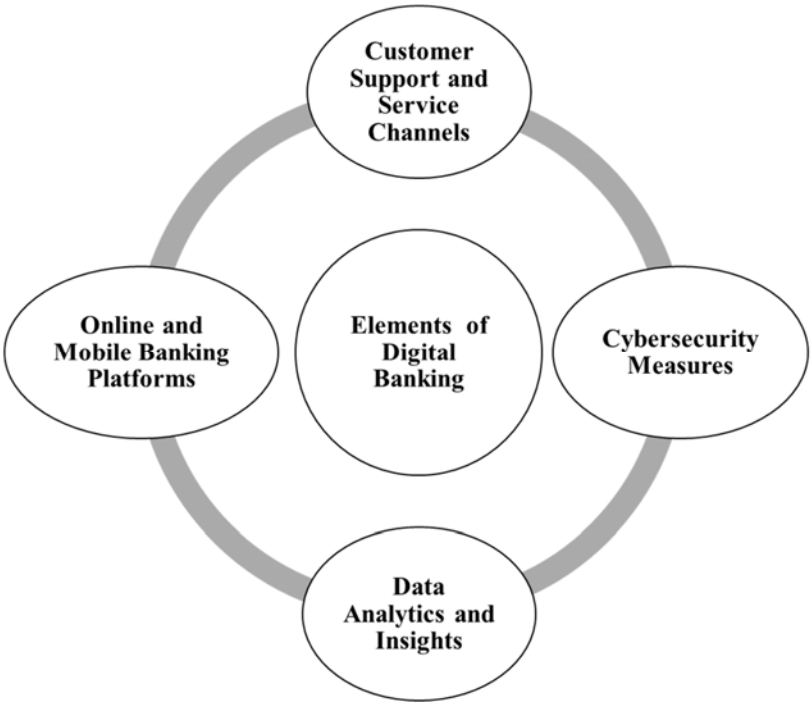

Figure 1: Represents the elements of digital banking.

Figure 1 shows the Elements of Digital Banking. Digital banking is expected to continue expanding and innovating in the future. New technologies that have the potential to improve digital banking systems further and solve current issues include enhanced biometrics and quantum computing. The future of digital banking will also be shaped by the continuing development of regulatory frameworks and the growing emphasis on sustainability and financial inclusion. Financial institutions need to be flexible and adaptable to new trends, client demands, and technology breakthroughs as digital banking keeps changing the financial environment. Through a commitment to innovation, a heightened sense of security and compliance, and the cultivation of robust client connections, financial institutions may adeptly traverse the dynamic landscape of digital banking and leverage its attendant prospects.

DISCUSSION

A change from conventional banking procedures to a more dynamic, technology-driven paradigm is reflected in the history and development of digital banking, which represents an amazing journey of technical innovation and revolution in the financial industry. Digital banking has its roots in the late 20th century when the introduction of personal computers and other early electronic communication devices started to completely change the way people performed financial transactions. In the beginning, banking was typified by in-person meetings at physical branches, manual transaction recording, and reliance on paper-based statements and documentation by clients. Even while this conventional methodology worked, it was often laborious and had limitations in terms of both reach and physicality.

Automated Teller Machines (ATMs) were originally introduced in the 1960s and 1970s, marking a crucial turning point in the development of digital banking. Customers no longer needed to visit a bank office to conduct routine banking operations like cash withdrawals and account balance checks thanks to ATMs. With its introduction, the banking industry began to transition to electronic and self-service methods, paving the way for further developments in digital financial services. Online banking development started to pick up steam in the 1980s and 1990s. As personal computers and the internet became more widely used, banks began to provide online services that let users pay bills, check their accounts, and transfer money via secure websites. The early Internet banking systems were rather simplistic and often demanded a certain amount of technological know-how from their users. But in terms of accessibility and convenience, they were a huge step forward, allowing consumers to handle their accounts from the comfort of their homes.

Developments in internet connection mobile computing, and digital banking technologies saw a significant spread in the late 1990s and early 2000s. With the advent of mobile banking apps, the banking industry saw even more change as clients could now use their tablets and smartphones to complete financial transactions. At this time, digital-only banks referred to as challenger banks began to appear. These banks conducted all of their business online and didn't have any physical locations. By using technology to provide cutting-edge services at low prices, these banks upended established banking paradigms and pushed the sector toward more digitization.

With the introduction of advancements in fintech, or financial technology, and the increasing use of smartphones, the development of digital banking has continued to pick up speed. Blockchain-based solutions, digital wallets, and peer-to-peer payment systems are just a few of the innovative services that fintech businesses have brought to market. These developments brought forth new methods of money management and transmission in addition to improving the efficiency and ease of financial operations. For example, people might use their cell phones to make payments instead of utilizing cash or credit cards thanks to digital wallets and mobile payment applications.

The banking sector has seen significant transformation in recent times due to the incorporation of artificial intelligence (AI) and machine learning into digital banking. These days, AI-powered solutions are used for several tasks, such as automated customer support, tailored financial advice, and fraud detection. For instance, chatbots and virtual assistants provide consumers with immediate help and guidance, while machine learning algorithms examine transaction data to find trends and flag possible security risks. These developments have not only increased banking operations' efficiency but also improved the clientele's overall experience.

Another noteworthy advancement in the development of digital banking is the emergence of open banking. The practice of banks and other financial institutions sharing their information and services via Application Programming Interfaces (APIs) with outside vendors is known as "open banking." By giving fintech businesses and other service providers access to banking data and allowing them to provide new goods and services, this strategy promotes more competition and innovation. Increased financial inclusion and a more competitive and diversified financial environment might result from open banking.

A further feature of the continuing digital transition in banking is the growing focus on data protection and cybersecurity. The increasing ubiquity of digital banking has made safeguarding confidential financial data and thwarting online attacks crucial. To protect consumer information and guarantee the integrity of their digital platforms, banks and other financial

organizations make significant investments in cybersecurity solutions. To reduce risks and fix any vulnerabilities, this entails putting strong encryption techniques, multi-factor authentication, and frequent security assessments into place.

Amidst social distancing efforts and limitations on physical branch access, the COVID-19 epidemic hastened the spread of digital banking as an increasing number of consumers resorted to online and mobile channels for financial management. This change brought attention to the significance of the infrastructure for digital banking and encouraged many institutions to improve their digital capabilities and make investments in cutting-edge technologies. Customers now demand easy, quick, and secure access to their financial services, making digital banking an essential component of today's financial scene.

It seems probable that changing consumer expectations and ongoing technological improvements will define the direction of digital banking. It is anticipated that new technologies like sophisticated artificial intelligence (AI), block chain, and quantum computing will spur more innovation and change in the banking industry. The emergence of digital currencies like central bank digital currencies (CBDCs) and decentralized finance (DeFi) may also have a significant effect on the financial sector, perhaps changing how financial services are provided and transactions are carried out.

The financial sector has changed due to the rapid development of digital banking, which provides unparalleled ease and accessibility to banking services via mobile apps and internet platforms. Financial institutions must, however, manage a complicated variety of cybersecurity threats and fraud risks as a result of this change to safeguard their clients and maintain confidence. In digital banking, cybersecurity refers to protecting a variety of sensitive data against malicious attacks, illegal access, and data breaches. This includes financial transactions, account details, and personal identity information.

The risks are great since violations may result in large-scale monetary losses, harm to one's reputation, and legal implications. Phishing attacks, in which scammers use false emails, websites, or messages to deceive people into giving their personal and financial information, are one of the main concerns in the world of digital banking. Phishing tactics may be quite complex and often imitate bank communications to provide the impression of legitimacy or urgency. Attackers could, for instance, pose as banks in emails they send out, requesting the receiver to click a link and provide their login information on a fake website. Malware, which includes ransomware, trojans, and viruses, is another serious concern. Malware may infect a user's device, giving hackers access to private data without authorization or interfering with financial processes. Ransomware is a kind of virus that is especially dangerous for digital financial systems because it encrypts data and demands a fee to unlock it. Distributed denial-of-service (DDoS) attacks pose a hazard in addition to these others because they may overload financial systems with traffic, disrupting services and perhaps jeopardizing security. Digital financial institutions use a multi-layered strategy for cybersecurity to counter these attacks. This involves putting cutting-edge encryption technology into practice to safeguard data both in transit and at rest and make sure that private data cannot be accessed by unauthorized persons. Online transactions and interactions between users and financial systems are often secured using encryption methods like SSL/TLS (Secure Sockets Layer/Transport Layer Security).

Using robust authentication techniques is also essential. When logging into an account using multi-factor authentication (MFA), users must give two or more verification factors, such as a password, a mobile device, and biometric data, to get access. MFA adds layer of security to prevent unwanted access, which greatly improves security. Financial organizations also spend

money on intrusion detection systems and ongoing monitoring to quickly spot and address any questionable activity. These systems examine network activity, look for irregularities, and sound an alarm if they find anything that would indicate a security breach. Frequent vulnerability assessments and security audits are also carried out to find and fix holes in the financial infrastructure.

Digital banking fraud protection techniques are equally important. Using real-time transaction monitoring systems to identify anomalous activity, such as transactions that diverge from a customer's customary spending habits, is one of the main strategies. By flagging potentially fraudulent transactions for further examination, these technologies help lower the chance of financial loss. To find abnormalities and stop fraud, behavioral analytics which studies user behavior patterns can also be used. For instance, the system can sound a warning or ask for further verification if a person starts a big transaction out of the blue from a strange place. Financial institutions should also teach their clients about cybersecurity best practices, which include spotting phishing efforts, coming up with strong passwords, and not using public Wi-Fi for banking. To avoid fraud and improve overall security, customer knowledge and attentiveness are essential. Another essential component of cybersecurity and fraud protection is regulatory compliance.

Financial organizations must abide by some laws and guidelines, including the Payment Card Industry Data Security Standard (PCI DSS), which establishes security guidelines for credit card data. Following these rules contributes to the banks' high degree of security and adherence to industry best practices.

Despite these precautions, cybercriminals are always finding new ways to exploit weaknesses, and their approaches are becoming more and more sophisticated. Digital banking companies must thus continue to be flexible and aggressive in their approach to cybersecurity. Investing in cutting-edge technology that may improve threat detection and response capabilities, such as machine learning and artificial intelligence (AI), is part of this.

AI-driven technologies help banks keep ahead of changing cyber dangers by analyzing massive volumes of data, seeing trends, and forecasting possible attacks. In summary, fraud prevention and cybersecurity are essential elements of digital banking that need a thorough and multifaceted strategy to safeguard private data and guarantee the accuracy of financial transactions. Financial institutions need to be on the lookout for ways to reduce risks and protect the future of banking as digital banking develops. Some of these ways include adopting cutting-edge technology, putting strong security measures in place, and educating clients.

When compared to conventional payment methods, digital payment systems and processes provide more convenience, efficiency, and security, hence bringing about a revolutionary change in the way transactions are carried out. Technological improvements and shifting customer tastes are driving this evolution, resulting in the creation of a wide variety of digital payment solutions that meet different demands and situations. The capacity to perform transactions electronically, doing away with the necessity for actual currency or paper-based techniques, is at the core of digital payment systems. Technological advancements such as the widespread use of cell phones, increased internet access, and safe payment processing platforms have made this transition easier. A wide range of techniques are included in digital payments, and each one has special benefits and features to suit various transaction kinds and user preferences.

Online payments, which let customers utilize a variety of platforms and devices to conduct transactions via the Internet, are among the most extensively used digital payment methods. Users may submit their payment information to complete purchases on websites and mobile

applications, which are often used to enable online payments. Payments for utilities, internet services, and e-commerce are among the common uses for this technology. By securely transporting payment information between the merchant's website and the financial institutions engaged in the transaction, payment gateways play a critical role in the processing of online payments. Well-known examples of online payment systems include Square, PayPal, and Stripe. They provide a variety of payment alternatives and have user-friendly interfaces.

Another important development in digital payment techniques is mobile payments. Through specialized applications or digital wallets, mobile payment systems allow consumers to transact using their smartphones or other mobile devices. To enable contactless transactions, mobile payments make use of technologies like Near Field Communication (NFC) and QR codes. Users of NFC-enabled mobile wallets, like Samsung Pay, Apple Pay, and Google Pay, may make payments by only touching their phones on terminals that accept them. Mobile payments using QR codes need scanning a code to complete a transaction. These types of payments are found in apps like WeChat Pay and Alipay. By eliminating the need to carry actual cards or cash, mobile payments provide the ease of having a virtual wallet with you.

Software programs that securely store payment information and enable digital transactions are called digital wallets, or e-wallets. Customers may use a digital wallet to pay with their credit or debit cards at real shops as well as online.

Additional functions like recording transaction history, integrating reward programs, and securely storing payment credentials are often offered by digital wallets. PayPal, Apple Wallet, and Google Wallet are a few of the well-known digital wallets. The rising acceptability of mobile payment methods and the simplicity of use of digital wallets have propelled their widespread use.

Cryptocurrencies provide an alternative to conventional fiat currencies and are a revolutionary advancement in digital payments. Blockchain technology, which is used by cryptocurrencies to function on decentralized networks, guarantees transaction immutability, security, and transparency. Peer-to-peer transactions are made possible by cryptocurrencies like Bitcoin, Ethereum, and others, eliminating the need for middlemen like banks. The benefits of cryptocurrencies include reduced transaction costs, quicker international transfers, and financial inclusion for marginalized groups. They do, however, also bring with them difficulties, such as unstable prices and unclear regulations. Some platforms and payment processors that enable Bitcoin transactions have emerged as a result of the emergence of cryptocurrencies, including Coinbase and BitPay.

Traditional digital payment methods like bank transfers and electronic funds transfers (EFT) have changed over time as technology has advanced. Bank transfers, usually via online banking sites or mobile banking applications, let people and companies transfer money electronically between bank accounts. EFT systems make it easier to move money between accounts both locally and internationally. Examples of these systems include wire transfers and Automated Clearing House (ACH) transfers. Large-value transactions, bill payments, and payroll deposits are often handled using these techniques. Electronic transfers are now even faster and more efficient because of the development of real-time payment systems like the Real-Time Payments (RTP) network in the US and the Faster Payments Service (FPS) in the UK.

Peer-to-peer (P2P) payment systems are becoming more and more popular because they provide people with a simple method to send and receive money right from their cellphones. With peer-to-peer (P2P) payment applications like Venmo, Cash App, and Zelle, users may send money to friends, family, or companies using email addresses or cellphone phones. Additional features including budgeting tools, social payment interactions, and fast transfers

are often offered by these applications. P2P payment systems, which provide a quick and easy method to handle personal accounts and make small-value payments, have become a crucial component of contemporary financial operations.

Digital payment systems include not just these techniques but also new and developing technology and innovations that are constantly changing the way that financial transactions are conducted. To improve the security of digital payments, for instance, biometric authentication such as fingerprint or face recognition—is being utilized more and more. Compared to conventional passwords and PINs, biometric technologies provide a better degree of security, lowering the possibility of fraud and unwanted access. In a similar vein, real-time fraud detection, tailored suggestions, and improved customer service are made possible by the integration of artificial intelligence (AI) and machine learning in payment processing systems.

Security and regulatory concerns have followed the proliferation of digital payment systems. The establishment of regulatory frameworks that guarantee the security, confidentiality, and equity of digital payment transactions is a top priority for both governments and financial organizations. Payment data collection, storage, and usage are governed by data protection rules, such as the California Consumer Privacy Act (CCPA) in the US and the General Data Protection Regulation (GDPR) in Europe. To guard against fraud, data breaches, and cyberattacks, financial institutions and payment service providers also make significant investments in cybersecurity solutions. A strong digital payment security plan must include encryption technology, safe authentication procedures, and ongoing monitoring.

The trajectory of digital payments is anticipated to be influenced by the continuous progress of technology and the changing desires of consumers. Payment system innovation will be fueled by the ongoing expansion of digital financial services, mobile technology, and e-commerce. Digital payments might undergo a revolution as a result of the integration of cutting-edge technologies like blockchain, artificial intelligence, and 5G connection, which will improve security, lower transaction costs, and open up new payment experiences. Furthermore, the growth of digital banking services and financial inclusion programs will provide underprivileged people more access to digital payments, promoting increased financial empowerment and economic engagement.

CONCLUSION

Customers may now handle their funds in a more accessible, efficient, and easy manner thanks to digital banking, which has completely changed the financial environment. The shift from conventional banking techniques to digital platforms has yielded notable advantages, such as improved accessibility, instantaneous transaction capabilities, and decreased operating expenses for financial establishments.

The client experience has changed as a result of innovations like mobile payments, online account management, and the emergence of digital-only banks, which have put banking services at the fingertips of consumers everywhere. But there are drawbacks to the quick development of digital banking as well, such as the need for strong cybersecurity defenses, regulatory compliance, and bridging the digital gap across various demographics. As technology develops, digital banking will probably witness further breakthroughs and the incorporation of cutting-edge technologies like blockchain and artificial intelligence, which will increase the efficiency and customization of financial services. With its ability to improve financial inclusion and transform the provision and consumption of banking services, digital banking is only going to become more important in the financial industry.

REFERENCES:

[1] D. Medenica Mitrović and M. Raičević, "Concept of Online Customers Experience in Digital Banking," *Mednar. Inov. Posl. = J. Innov. Bus. Manag.*, 2020, doi: 10.32015/jibm.2020.12.2.8.79-86.

[2] Rachna Kalsan, "Impact of Digital Banking in India: Trends & Challenges," *Int. J. Res. Eng. Appl. Manag.*, 2020, doi: 10.35291/2454-9150.2020.0013.

[3] D. K. Panjwani and D. N. Shili, "The Impact of Fintech on Development of Islamic Banking Sector in the Contemporary World," *Saudi J. Econ. Financ.*, 2020, doi: 10.36348/sjef.2020.v04i07.006.

[4] D. V. Pasinitsky, "Digital Transformation in the Concept of Internal Banking Risk Management," *Digit. Transform.*, 2020, doi: 10.38086/2522-9613-2020-3-45-50.

[5] E. P. Yıldız, M. Çengel, and A. Alkan, "Determination of digital citizenship levels of university students at sakarya university Turkey," *Int. J. High. Educ.*, 2020, doi: 10.5430/IJHE.V9N3P300.

[6] T. Yigitcanlar *et al.*, "Artificial intelligence technologies and related urban planning and development concepts: How are they perceived and utilized in Australia?," *J. Open Innov. Technol. Mark. Complex.*, 2020, doi: 10.3390/joitmc6040187.

[7] R. N. Kailashbhai, "Digital economy in India-current situation," *Acad. An Int. Multidiscip. Res. J.*, 2020, doi: 10.5958/2249-7137.2020.01671.7.

[8] A. Belke and E. Beretta, "From cash to central bank digital currencies and cryptocurrencies: a balancing act between modernity and monetary stability," *J. Econ. Stud.*, 2020, doi: 10.1108/JES-07-2019-0311.

[9] M. C. Arthi and K. Shanmugam, "Financial Inclusion via Mobile Banking – A Comparison Between Kenya and India," in *IFIP Advances in Information and Communication Technology*, 2020. doi: 10.1007/978-3-030-64849-7_50.

[10] P. K. Singh and A. Dutta, "Socio-metrics of digital payments in demographic dividend: Descriptive analysis of dichotomous preferences," *Applied Innovative Research (AIR)*. 2020.

CHAPTER 2

INVESTIGATION OF DIGITAL BANKING INFRASTRUCTURE IN DIGITAL BANKING

Dr. Zuleika Homavazir, Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- zuleika.homavazir@atlasuniversity.edu.in

ABSTRACT:

Modern financial services are supported by a complicated and vital framework that is revealed by the examination of digital banking infrastructure. The technology, procedures, and systems required to provide safe and effective online and mobile banking services are all included in the digital banking infrastructure. Core banking systems, data centers, cloud computing resources, cybersecurity safeguards, and payment processing technologies are all part of this infrastructure. Real-time transactions, safe data management, and scalable operations are made possible by a strong foundation for digital banking. Digital platforms, such as online portals and mobile applications, are essential elements that make it easier for users to access and engage with financial services. Large volumes of financial data can be handled by data centers because they have the processing power and storage needed, and cloud computing can be scaled and flexible to meet changing needs. An essential component that guarantees the safety of private financial data against theft and breaches is cybersecurity. To improve operational efficiency and speed transactions, digital payment systems and APIs (Application Programming Interfaces) interact with a range of financial services. Changes in customer expectations, regulatory restrictions, and technology breakthroughs are driving the continuous growth of digital banking infrastructure. Resilience, security, and innovation in the banking industry depend on financial organizations' ability to comprehend the elements and difficulties of the digital banking infrastructure that they embrace and integrate. This study focuses on the fundamental components of the infrastructure supporting digital banking, highlighting their significance in influencing the direction of financial services and satisfying the needs of the digital economy.

KEYWORDS:

Core Banking Systems, Cybersecurity, Cloud Computing, Data Centers, Digital Payment Technologies.

INTRODUCTION

The fundamental architecture that underpins the provision of financial services via digital platforms is known as digital banking infrastructure. Together, this infrastructure—which consists of network systems, hardware, software, and security protocols—allows financial institutions to provide a plethora of services, including digital payments, online and mobile banking, and automated financial management tools [1], [2]. The development of digital banking infrastructure has been propelled by technological advancements, alterations in consumer behavior, and the growing need for financial services that are more easily available and convenient. Comprehending the constituents and complexities of this framework is crucial to comprehending the functioning of contemporary banking in an ever-more digitalized society. The network architecture, which enables the smooth movement of data between banks and their clients, is the foundation of digital banking infrastructure. Strong, fast internet connections provide the foundation for this network, enabling real-time transactions and communication. Financial organizations make significant investments in data centers, which

hold the storage and server equipment required to handle massive data volumes. Because of their high availability and redundancy features, these data centers reduce the possibility of outages and guarantee that financial services are always available [3], [4]. Because cloud computing provides scalable and adaptable options for processing and storing data, it has also become a crucial component of the infrastructure of digital banks. Banks may save the costs of maintaining physical infrastructure, launch new services more rapidly, and swiftly adjust to changing needs by using cloud services.

The sensitive nature of financial data and the growing danger of cyberattacks make security in digital banking a top priority. Several security layers are included into digital banking infrastructure to safeguard consumer data and guarantee transaction integrity. Data is often protected while it moves across networks via encryption, which renders it unreadable to unauthorized parties. Furthermore, in addition to standard passwords, multi-factor authentication (MFA) is used to confirm users' identities when they access digital financial services. Advanced intrusion detection and prevention systems (IDPS) are also used by financial organizations to monitor network traffic for unusual behavior and instantly react to any attacks [5], [6]. The use of machine learning algorithms and artificial intelligence (AI) has improved security even further by facilitating the identification of irregularities and trends that point to fraudulent activity. These systems can recognize and highlight potentially fraudulent activity by continually monitoring transaction data, which enables banks to take preventative action to safeguard their clientele.

User interfaces including websites, mobile applications, and digital wallets that consumers engage with make up the front end of the digital banking infrastructure. Customers can access their accounts, complete transactions, and handle their money with ease thanks to these interfaces, which are designed to provide a smooth and simple user experience. The creation of these interfaces heavily relies on user experience (UX) design, which aims to create an environment that is both aesthetically pleasing and easy to use. Functionalities like customizable dashboards, user-friendly navigation, and adaptable design are crucial for satisfying the varied demands of clients on various gadgets. Customers may now access financial services while they're on the move thanks to mobile banking applications, which have emerged as a crucial element of the infrastructure of digital banking. Users' convenience and security are increased by these applications' frequent inclusion of features including mobile check deposit, immediate alerts, and biometric identification.

Because they manage data, conduct transactions, and integrate with other financial systems, back-end systems play an equal role in the architecture of digital banking. Digital banking relies heavily on core banking systems to manage the accounts, transactions, and client data necessary for day-to-day operations. High transaction volumes are supported by these technologies, which also guarantee correctness and uniformity across all financial services. Digital banking infrastructure comprises payment gateways and processors that enable online and mobile transactions in addition to basic banking services. These systems are in charge of processing and approving payments, making sure that money is moved between accounts safely [7], [8]. Payment gateways enable users to choose the most convenient payment method for their transactions from a variety of integrated payment methods, such as digital wallets, bank transfers, and credit and debit cards.

Because banks need to be able to connect and interact with other financial institutions, payment networks, and third-party service providers, interoperability is a crucial factor in the architecture of digital banking. This interoperability is made possible in large part by Application Programming Interfaces (APIs), which facilitate the smooth interchange of functionality and data across various systems. In the context of open banking, where financial

institutions offer standardized interfaces to third-party developers to access their data and services, APIs have grown in significance [9], [10]. This makes it possible to create fresh financial services and solutions that may be combined with current banking systems to provide clients more options and flexibility. In the financial industry, open banking can spur innovation and lead to the development of new business models and alliances that are advantageous to financial institutions as well as customers.

Another essential component of the infrastructure of digital banking is regulatory compliance, as financial organizations have to abide by a complicated and ever-changing set of laws that control financial transactions, security, and data protection. Strict guidelines for how banks handle and safeguard consumer data are imposed by regulatory frameworks like the Payment Card Industry Data Security Standard (PCI DSS) in the US and the General Data Protection Regulation (GDPR) in Europe. Maintaining client confidence and avoiding fines and other consequences depend on compliance with these standards. Systems and technologies included in digital banking infrastructure assist financial organizations in enforcing and monitoring regulatory compliance. To guarantee adherence to legal standards, these systems often come with automatic reporting capabilities, audit logs, access restrictions, and data encryption. Figure 1 shows the Data Analytics Infrastructure.

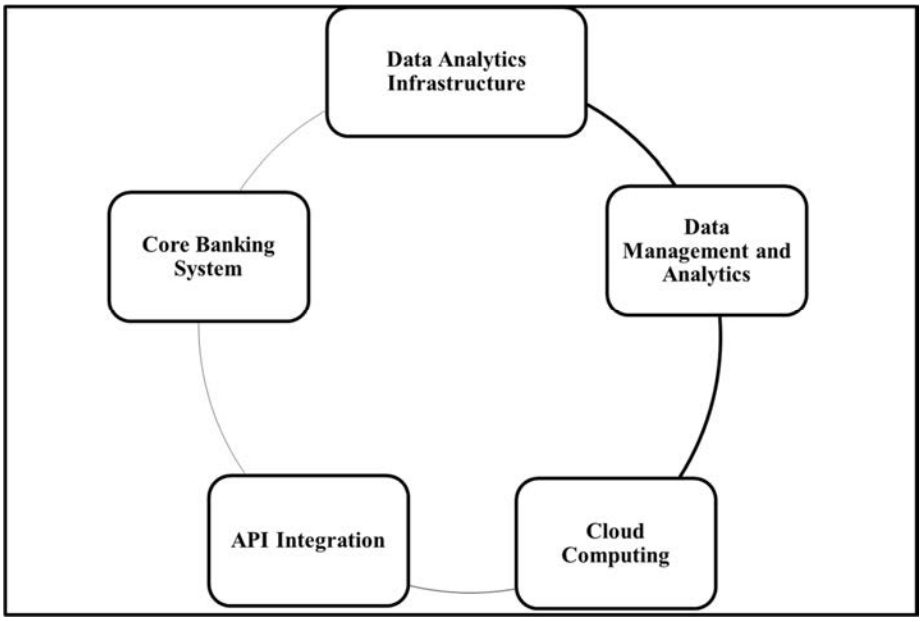

Figure 1: Represents the data analytics infrastructure.

The future of digital banking infrastructure is being shaped by the integration of cutting-edge technologies like blockchain, big data analytics, and artificial intelligence (AI). Artificial intelligence (AI) and machine learning are being used to automate repetitive jobs, improve decision-making processes, and improve customer service via chatbots and virtual assistants. AI-driven chatbots, for instance, may aid with complicated financial transactions, respond to often-asked queries, and provide consumers with immediate assistance. Large datasets are analyzed, patterns are found, and forecasts are made using machine learning algorithms, all of which help with strategic decision-making. The potential of blockchain technology to improve financial transaction efficiency, security, and transparency is being investigated. Blockchain has the potential to simplify settlement procedures, lower the risk of fraud, and open the door to new kinds of digital assets by producing a decentralized and unchangeable log of

transactions. On the other hand, banks may provide more specialized and focused services by using big data analytics to get insights into consumer behavior, preferences, and risk profiles.

DISCUSSION

The networks and systems that facilitate financial inclusion and provide underprivileged and unbanked people access to banking services are also included in the digital banking infrastructure. Important elements of this infrastructure include digital wallets, agent banking models, and mobile banking, which provide people in rural or underdeveloped regions accessibility and reasonably priced financial services. Particularly, mobile banking services have been essential in increasing financial inclusion since they let people use their phones to create accounts, send money, and get credit. With digital wallets, users may handle and keep money online, sometimes doing so without a regular bank account.

By forming alliances with neighborhood agents or companies, agent banking models provide more avenues for customers to receive banking services, hence expanding the reach of financial institutions into underprivileged areas.

Cloud computing has a revolutionary role in digital banking, completely changing the way financial institutions function and provide services. Unlike conventional on-premises IT infrastructure, cloud computing is by definition the delivery of computer services such as networking, processing power, and storage over the internet. Cloud computing is a key enabler of contemporary financial services because it provides previously unheard-of levels of scalability, flexibility, and cost-efficiency in the context of digital banking.

Scalable resources are among cloud computing's most important advantages for digital banking. The capacity of traditional banking infrastructure is limited by the physical resources available, and it often requires large financial investments in hardware and software. On the other hand, banks can scale their IT resources up or down in response to demand thanks to cloud computing. Because transaction volumes in the digital banking environment may vary greatly, scalability is especially crucial.

For example, transaction volumes may spike during busy shopping seasons or financial crises, necessitating a rapid boost in processing capacity from banks to sustain service levels. This flexibility is made possible by cloud computing, which spares banks from having to invest in extra physical equipment and allows them to satisfy consumer needs without going over budget.

The cloud's ability to reduce costs is yet another significant benefit for digital banks. Pay-as-you-go cloud service models allow banks to only pay for the resources they utilize. The conventional method, which requires banks to invest in and maintain IT infrastructure that may be idle for a large portion of the year, is drastically different from this model. Banks may drastically cut their capital expenditure and switch to a more predictable operational cost model by being cloud-based. By making this change, expenses are not only decreased but also available funds that may be allocated to other divisions of the company, such as customer support or innovation.

Cloud computing also helps digital banks become more innovative and agile. One of the most important competitive advantages in the ever-changing financial scene is the capacity to design, test, and implement new services fast. This agility is supported by cloud computing, which offers an adaptable and quick-to-respond IT environment. The software development lifecycle, from initial coding to deployment, may be accelerated by development teams by using cloud-based platforms and technologies. Furthermore, the adoption of cutting-edge technologies like

blockchain, machine learning, and artificial intelligence (AI) is made possible by cloud computing. These technologies call for substantial processing power and data processing skills. Banks may more readily explore and integrate new technologies via the use of cloud infrastructure, spurring innovation and improving the client experience.

Digital banking places a high priority on security, and cloud computing provides reliable solutions to meet this problem. Cloud service providers make significant investments in security measures, sometimes going above and beyond what individual banks can do. These precautions include identity and access control, encryption, and ongoing threat detection. Furthermore, cloud service providers usually adhere to industry rules and guidelines, such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR). By adhering to these regulations, banks can fulfill their legal requirements and take advantage of the cutting-edge security features provided by cloud platforms. It's crucial to remember that even if cloud providers provide robust security, the bank and the provider share responsibility for protecting data in the cloud. To completely safeguard the information of their clients, financial institutions must put in place their security policies and procedures, including data encryption, access restrictions, and recurring security audits.

Additional domains in digital banking where cloud computing is essential include disaster recovery and business continuity. Conventional disaster recovery plans sometimes include replicating IT infrastructure in many places, which may be costly and difficult to maintain. By enabling banks to duplicate their data and apps across geographically separated data centers, cloud computing streamlines this procedure. Cloud-based disaster recovery solutions allow banks to promptly restore services with the least amount of disturbance in the event of a system breakdown or natural catastrophe. In digital banking, where downtime may have serious consequences for finances and reputation, this capacity is crucial.

Cloud computing facilitates the internationalization of online financial services. Cloud computing offers the infrastructure required to continuously provide the smooth cross-border financial services that clients are increasingly demanding. Banks can give their clients quick and dependable services regardless of where they are because of cloud platforms' worldwide reach and data centers spread across many countries. For digital-only banks and fintech businesses, which often operate internationally and need a flexible infrastructure that can adjust to various regulatory contexts and client demands, this global reach is especially crucial.

Within the digital banking ecosystem, cloud computing also improves cooperation and data exchange. Banks may break down departmental and functional walls thanks to the cloud, which promotes more information exchange and cooperation. For instance, the product development team may quickly access and evaluate consumer data gathered by the marketing division to provide customized financial solutions. Through APIs and other integration tools, cloud computing also makes it easier to collaborate with other partners, including finance businesses. In order to develop and provide new services, banks must work together in order to take use of third parties' technology and knowledge.

While cloud computing offers many benefits for digital banking, institutions need to take certain precautions and overcome certain obstacles before using cloud solutions. Data privacy and sovereignty are two main issues. Sensitive consumer data is handled by financial organizations, and many nations' laws mandate that this data be kept domestically. Cloud providers need to guarantee that their services adhere to these requirements. This may include providing choices for data localization or collaborating with local partners to create data centers in designated locations.

The possibility of vendor lock-in, in which a bank becomes too reliant on the infrastructure and services of a single cloud provider, is another difficulty. If the supplier hikes pricing or modifies its service offerings, this reliance may reduce the bank's flexibility and increase expenses. Banks should think about multi-cloud options to lessen this risk. These include using various cloud providers for different services or keeping a hybrid cloud architecture that blends on-premises and cloud technology. This strategy lowers the possibility of vendor lock-in while offering more freedom. For financial organizations to utilize cloud computing, a cultural transformation is also necessary. Traditional banks in particular may have legacy systems and ingrained procedures that make it difficult to move them to the cloud. Adopting cloud computing successfully requires not just having the appropriate technology but also a dedication to change management, which includes personnel training, process updates, and promoting an innovative and flexible culture.

With the emergence of new technologies and business models, cloud computing is projected to play an even larger role in digital banking in the future. Cloud computing will probably be complemented by the further development of edge computing, which processes data closer to the source (such as Internet of Things devices) and offers even quicker and more effective services. Furthermore, by providing previously unheard-of processing power and capabilities, the combination of quantum computing with cloud services has the potential to completely transform industries like financial modeling, risk analysis, and encryption. The foundation of the digital banking infrastructure is made up of data centers, which are essential for handling, processing, and storing the enormous volumes of data produced by banking activities. The need for reliable and secure data centers has increased dramatically as the banking sector moves more and more towards digital platforms. These facilities facilitate everything from online transactions and mobile banking applications to sophisticated financial analytics and regulatory compliance. They guarantee the seamless operation of digital banking services.

The capacity of a data center to provide safe, dependable processing and storage for the massive amounts of data that banks handle on a daily basis is the fundamental component of a data center's significance. Sensitive financial data, such as customer information, transaction histories, and other private information, are constantly exchanged in digital banking. High-security mechanisms, including encryption, multi-factor authentication, and physical security controls, are built into data centers to guard against unwanted access and data breaches. The availability and integrity of this data are essential since any loss or interruption may have detrimental effects on a bank's finances and reputation. Data centers are necessary to guarantee the dependability and availability of digital financial services in addition to security. Customers nowadays expect to be able to use their banking services around the clock, so any interruption may result in serious complaints and perhaps even loss of business. To guarantee ongoing operation even in the case of hardware failures, power outages, or other disturbances, data centers are outfitted with redundant systems and failover methods. Maintaining consumer confidence and guaranteeing that financial services are always available when required depends heavily on this high availability.

CONCLUSION

The development of contemporary financial services has been greatly aided by digital banking infrastructure, which offers the framework required for safe, effective, and scalable banking operations. Core banking systems, data centers, cloud computing, cybersecurity protocols, and digital payment technologies interact to provide a unified framework that facilitates smooth client interactions and strong operating capacities. The need for a flexible and well-integrated infrastructure grows as financial institutions negotiate the challenges of the digital revolution. The future of digital banking will be shaped by continual technological breakthroughs and

changing regulatory requirements, which will need constant infrastructure investment to guarantee resilience and creativity. Financial institutions may improve their capacity to fulfill the demands of a digital economy that is evolving quickly and keep their competitive advantage in the market by comprehending and improving each component of the infrastructure supporting digital banking.

REFERENCES:

[1] J. Lee, L. Wewege, and M. C. Thomsett, "Disruptions and Digital Banking Trends," *J. Appl. Financ. Bank.*, 2020.

[2] C. Louw and C. Nieuwenhuizen, "Digitalisation strategies in a South African banking context: A consumer services analysis," *SA J. Inf. Manag.*, 2020, doi: 10.4102/sajim.v22i1.1153.

[3] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature," *Journal of Financial Crime*. 2020. doi: 10.1108/JFC-03-2020-0037.

[4] L. Wewege, J. Lee, and Michael C. Thomsett, "The Digital Banking Transformation : Disruption, Synergy toward Fintech Frontier," *Cent. Financ. Manag. Stud.*, 2020.

[5] D. B. S. Hada*, "Impact of Internet Banking on the Customer Satisfaction: Evidence from the Indian Banking Sector," *Int. J. Recent Technol. Eng.*, 2020, doi: 10.35940/ijrte.f8198.038620.

[6] E. O. Onah, A. I. Ujunwa, A. Ujunwa, and O. S. Ogundele, "Effect of financial technology on cash holding in Nigeria," *African J. Econ. Manag. Stud.*, 2020, doi: 10.1108/AJEMS-04-2020-0190.

[7] B. Lavanya and D. D. S. Selvakumar*, "Digital Infrastructure of Commercial Banks with Special Reference to Vellore District," *Int. J. Recent Technol. Eng.*, 2020, doi: 10.35940/ijrte.e6941.038620.

[8] I. Ramadhan, "Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)," *J. Soc. Polit. Sci.*, 2020, doi: 10.31014/aior.1991.03.04.230.

[9] E. Gorian, "Critical information infrastructure of the People's Republic of China: peculiarities of legal regulation in the area of ensuring information security of the financial-banking sector," *Административное и муниципальное право*, 2020, doi: 10.7256/2454-0595.2020.4.32878.

[10] T. Moenjak, A. Kongprajya, and C. Monchaitrakul, "ADBI Working Paper Series Fintech, Financial Literacy, And Consumer Saving And Borrowing: The Case Of Thailand Asian Development Bank Institute," *ADBI Work. Pap. Ser.*, 2020.

CHAPTER 3

ANALYSIS OF DIGITAL BANKING CHANNELS AND PLATFORMS

Prof. Bhargavi Deshpande, Assistant Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- bhargavi.deshpande@atlasuniversity.edu.in

ABSTRACT:

The financial services sector has seen a substantial transformation because of digital banking channels and platforms, which provide more effective, convenient, and customized banking experiences. The influence of several digital banking channels such as digital wallets, mobile banking applications, and Internet banking on customer behavior and banking operations is examined in this report. With the development of web-based systems, online banking now offers consumers extensive services like account management, money transfers, and access to financial services from anywhere. These functionalities are extended to smartphones via mobile banking applications, which further improve convenience with features like integrated financial management tools, biometric verification, and immediate alerts. Digital wallets that enable contactless payments and secure payment information storage include Apple Pay and Google Wallet. As a result of the spread of these platforms, banks, and other financial institutions are now more competitive, which encourages innovation and enhances service delivery. But the rise of online banking also brings up issues with data privacy, cybersecurity, and the digital divide. To safeguard users and maintain confidence, this research also takes regulatory issues into account and emphasizes the need for strong security measures. The results show that even while digital banking channels have many advantages, such as increased accessibility and user involvement, security and regulatory frameworks must always be upgraded to handle new threats.

KEYWORDS:

Digital Banking, Digital Wallets, Mobile Banking, Online Banking, User Experience.

INTRODUCTION

Modern financial services rely heavily on digital banking channels and platforms, which have completely changed how banks communicate with their clients and provide banking services. The creation of several channels and platforms that provide accessibility, efficiency, and ease of use has resulted from the spread of digital technology, changing the way that banking activities are conducted. Gaining an appreciation of these channels and platforms' subtleties and implications is essential to understanding their place in the financial ecosystem. Customers may access and control their banking services using a variety of platforms and tools found in digital banking channels [1], [2]. These channels enable consumers to conduct transactions and get information without having to physically visit bank offices since they are designed to be flexible and convenient. The three main digital banking channels are digital wallets, internet banking, and mobile banking. Each channel has a distinct purpose and works together to provide a seamless digital banking experience.

Online Banking: The foundation of digital banking is online banking, also referred to as internet banking. Through a web-based interface, clients may access their accounts, complete transactions, and manage their money [3], [4]. Web browsers on PCs or laptops are usually used to access online banking systems, which include several features including financial transfers, bill payments, investment management, and account monitoring. Online banking has several benefits, such as being accessible from any place with an Internet connection, handling

complicated transactions, and offering extensive account management capabilities. Sophisticated online banking systems often include strong security features, such as encryption and multi-factor authentication, to shield private financial data from internet dangers.

Using mobile devices, including smartphones and tablets, to access financial services is known as mobile banking. For managing funds while on the road, mobile banking programs, sometimes referred to as banking apps, provide a practical and easy-to-use interface. These applications include features including bill payment, transaction processing, and account access that are comparable to those found in online banking. To improve the user experience, mobile banking applications often include push notifications, location-based services, and biometric identification (such as fingerprint or face recognition). Mobile banking has been more popular due to the widespread usage of smartphones and the rising demand for mobile internet services. In today's fast-paced, digital world, mobile banking is an essential means of connecting with clients and providing services.

Applications that store payment data and enable electronic transactions are referred to as digital wallets or e-wallets. Customers may make payments easily online and in-store by connecting their digital wallets to their bank accounts, credit cards, or debit cards. Services for digital wallets that are well-known include Samsung Pay, Google Pay, and Apple Pay [5], [6]. With the use of these wallets, consumers may make contactless purchases at payment terminals by only touching their mobile devices, which increases convenience and eliminates the need for actual cash or credit cards. To provide a complete financial transaction management solution, digital wallets often include other features like budgeting tools, loyalty programs, and transaction history monitoring.

Although they are not fully digital, self-service kiosks and automated teller machines (ATMs) have developed to include further digital features. In addition to the usual cash withdrawal and deposit functions, contemporary ATMs often include account transfers, bill payments, and mini-statements. Similar to this, self-service kiosks in bank branches enable users to use digital interfaces to do a variety of banking operations, such as applying for loans or updating account information. These channels provide a better client experience with more automation and efficiency by bridging the gap between conventional and digital banking.

The underlying systems and technology that combine and support different digital banking channels are known as digital banking platforms. Core banking systems, customer relationship management (CRM) systems, and digital payment infrastructure are just a few of the components that make up these platforms. To provide a smooth and successful digital banking experience, these systems must be managed and integrated effectively. Managing account administration, transaction processing, and financial reporting, core banking systems are the foundation of digital banking platforms [7], [8]. These systems are in charge of processing transactions instantly, keeping correct records of client accounts, and producing reports for both internal and external use. To ensure that online and mobile banking transactions are synced with the bank's central database, modern core banking systems are built to accommodate digital channels. Scalability and flexibility have been further improved by the move to cloud-based core banking systems, which enables banks to swiftly adjust to shifting client demands and technological improvements.

By tracking customer interactions and information throughout the banking relationship, CRM systems are essential to digital banking. By giving banks access to information on consumer behavior, preferences, and transaction history, these systems allow for more specialized marketing and individualized customer care. CRM systems assist banks in better understanding the demands of their clients, providing specialized financial solutions, and raising client

satisfaction levels. Long-term connections are fostered and the customer experience is improved via seamless communication and interaction made possible by integration with digital banking channels [9], [10]. This refers to the systems and technology used to make electronic payments possible. This comprises networks, processors, and payment gateways that provide quick and safe payment processing. Many payment methods, such as bank transfers, electronic funds transfers (EFTs), credit and debit cards, are supported by digital payment infrastructure. Payment systems are integrated with digital banking channels to provide quick and safe transaction processing, giving consumers a smooth and easy way to make payments. Figure 1 shows the digital banking channels.

Figure 1: Represents the digital banking channels.

API Integration: By facilitating integration across many platforms and systems, Application Programming Interfaces (APIs) are essential to digital banking. APIs make it easier for third-party services, core banking systems, and digital banking channels to communicate information and functions. To improve the breadth of services offered to clients, banks may interact with fintech platforms, payment processors, and financial data aggregators, for instance, thanks to APIs. To swiftly adapt to changing consumer demands and market trends, banks may provide new products and services thanks to API integration, which fosters innovation.

DISCUSSION

Digital banking systems and channels provide many advantages, but there are drawbacks as well that institutions need to consider. These include the need for seamless integration across many systems and platforms, security issues, and regulatory compliance. Because banking channels are digital, there is a higher chance of cyber threats including malware, phishing scams, and data breaches. Strong security measures must be put in place by banks to safeguard private financial data and guarantee transaction integrity. This entails using multi-factor authentication, sophisticated encryption, and ongoing activity monitoring to spot suspect activities. Sustaining security is essential for maintaining client confidence and guaranteeing the secure functioning of online banking services.

Several regulations, such as those about financial reporting standards, data protection, and privacy, apply to digital banking. These rules, which differ according to the area and jurisdiction, must be complied with by banks via their digital channels and platforms. Maintaining compliance requires constant observation, adjustment to changing legal requirements, and implementation of safeguards for client information and transactional openness. It might be difficult to integrate digital banking channels with other platforms and core banking systems. Banks are required to provide efficient communication between various systems and cross-channel data synchronization. Careful planning, testing, and continuous maintenance are necessary to guarantee a flawless client experience and avoid any interruptions. Additionally, for banks to remain competitive and satisfy changing client expectations, they must constantly update and enhance their digital infrastructure due to the quick speed of technological progress.

Data centers are essential to the flexibility and scalability of digital banking processes. Data centers provide the platforms required to scale operations effectively as banks expand and the need for digital services rises. Specifically, cloud-based data centers provide on-demand scalability, which enables banks to promptly adjust to evolving requirements without requiring a substantial initial investment in physical infrastructure. The financial business is dynamic, with fast-changing market circumstances, regulatory regulations, and client expectations. This flexibility is crucial for adapting to these changes.

Data centers provide banks with the ability to improve their digital banking services by using cutting-edge technology and analytics. Data centers provide the processing capacity required to handle and analyze enormous datasets in real-time, which is becoming more important in the financial services industry due to the rise of big data and artificial intelligence. Banks may use this capacity to identify fraud, acquire insights into client behavior, improve operations, and create customized financial products. Effective data exploitation is turning into a competitive advantage in the world of digital banking.

Data centers are also essential for regulatory compliance. Banks must adhere to strict regulations governing data security, privacy, and reporting in their operations. By offering safe storage, audit trails, and reporting tools that guarantee adherence to laws like the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR), data centers assist banks in fulfilling these responsibilities. Data centers also assist with business continuity and disaster recovery planning, which are essential elements of regulatory compliance. Data centers assist banks in reducing the risk of fines from regulators and preserving operational resilience by making sure that data is backed up and can be promptly restored in the case of an emergency.

Data center administration and architecture have also changed to accommodate the unique requirements of online banking. To lessen their influence on the environment, modern data centers are progressively using sustainable technology and energy-efficient procedures. This is especially crucial since data centers use a lot of energy, and banks are coming under more and more pressure to show that they are committed to sustainability. Data centers are becoming more eco-friendly and efficient because of innovations like liquid cooling, renewable energy integration, and AI-driven energy management. Modularity and flexibility are being included in data center architecture more and more, giving banks the ability to optimize and tailor their infrastructure to meet their unique requirements. Banks can deploy and expand resources more effectively with this modular strategy, which lowers costs and increases agility. Furthermore, by putting processing capacity closer to the source of data production, edge computing is enhancing conventional data centers. This is especially helpful for applications that need low latency, such as real-time payments and fraud detection.

The nexus between data management and customer engagement has become a critical aspect impacting the total customer experience in the modern digital banking world. Digital banking uses cutting-edge technology to improve service delivery and operational efficiency. It is characterized by the provision of financial services via electronic channels as opposed to customary in-person encounters. In this context, customer engagement plays a complex function that includes a range of touchpoints where clients communicate with their banks via digital channels. Conversely, data management serves as the foundation for these exchanges by giving banks the tools they need to gather, handle, and evaluate client data, allowing them to provide individualized and effective services.

Digital banking mostly uses online channels including websites, chatbots, and mobile applications for customer contact. Numerous services, such as account administration, transaction processing, and customer assistance, are made possible by these digital channels. Since these encounters have a direct influence on consumer happiness and loyalty, their efficacy is vital. Positive client relationships need a smooth user experience that is defined by easy-to-navigate, fast response times, and dependable service. Personalization of services is an important part of consumer contact. Digital banking systems often use algorithms to customize offers and suggestions according to the unique behavior and interests of each client. For example, if a user regularly checks their account balances and transfers money using the banking app, the system may recommend related financial items or send them reminders when they have payments due. The customer experience is improved by this degree of customization, which makes interactions more interesting and relevant.

Real-time contact via a variety of channels, including as live chat and video help, is made possible by digital banking systems. In addition to answering consumer questions more quickly, this instantaneous communication fosters confidence in the bank's promptness and capacity to help. Sophisticated features like predictive analytics and automated answers are made possible by the integration of machine learning (ML) and artificial intelligence (AI) in customer support systems. By anticipating their demands and streamlining support procedures, these technologies improve the user experience in general

The foundation of digital banking is data management, which offers the framework needed to manage the enormous volumes of consumer data produced by online transactions. Several essential elements are required for effective data management, including data processing, analysis, storage, and gathering. Every one of these elements is essential in determining how the client experience is shaped.

Digital banking systems are always gathering information on the habits, past transactions, and interactions of its users. The comprehension of client demands and preferences is greatly aided by this data. For instance, transaction data might disclose spending patterns, while interaction data can show preferred times and channels for communication. Banking institutions may provide more individualized and relevant services by gathering and evaluating this data to get insights into the behavior and preferences of their customers. Preserving client confidence requires effective and safe data storage. To prevent breaches and unauthorized access to sensitive information, banks need to put strong security measures in place. To guarantee that client data is handled properly, compliance with data protection laws is also essential. Examples of these laws are the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR).

Data collection, processing, and analysis are necessary steps to get valuable insights from the data. Banks can spot patterns and trends in the behavior of their customers by using sophisticated analytics tools and strategies like data mining and predictive modeling. Predictive

analytics, for example, enables proactive service delivery by using previous data to estimate future client demands. Furthermore, the creation of customized product offers and focused marketing strategies is facilitated by data-driven decision-making. Banks may divide their clientele into discrete categories according to a range of factors, including financial demands, transactional patterns, and demographics, thanks to data management. This segmentation makes it possible to create personalized financial solutions and target marketing campaigns more precisely. For instance, depending on their salary and savings habits, a bank may create customized savings programs for young professionals.

The customer experience is greatly impacted by the combination of efficient data management and client engagement strategies. A well-thought-out digital platform that uses data to tailor communications and provide prompt assistance adds to a satisfying user experience. Important facets of this effect consist of one of the main factors influencing consumer happiness is personalized experiences. Banks can customize their services to match individual demands by using data to understand individual preferences and behaviors. In addition to product suggestions, targeted discounts, and tailored financial advice, this customization also includes other services that make the user experience more relevant and engaging.

Faster and more efficient transactions and interactions are made possible by digital banking systems with good data management. Services are delivered faster and more reliably when automated procedures, such as real-time fraud detection and rapid account changes, are used. Effective data management facilitates the expeditious handling of client inquiries and problems, hence augmenting the seamless and gratifying experience. Banks can anticipate client demands and provide proactive service thanks to data-driven insights. For instance, the system may provide a warning or recommend an appropriate overdraft protection plan to a client who often overdrafts their account.

In addition to averting any problems, this proactive strategy shows the bank's dedication to anticipating and meeting client demands. Establishing and preserving consumer trust is greatly aided by effective data management procedures. Strong security measures combined with open data processing procedures ensure clients that their data is secure. Long-term, enduring relationships are more likely to be fostered by banks that emphasize data security since trust is a vital aspect of the customer experience. Consistency across several digital channels is guaranteed by efficient data management. Whether a customer interacts with their bank via a website, mobile app, or other digital touchpoint, they anticipate a frictionless experience. Regardless of the platform being utilized, data integration across channels enables consistent service delivery and a seamless customer experience.

When compared to conventional methods, digital payment systems provide an unparalleled degree of convenience, speed, and security, completely revolutionizing the financial transaction process. Digital payment systems, at its foundation, use technology to facilitate electronic transactions between parties, doing away with the need for actual currency or checks. The growth of digital wallets, mobile payments, and blockchain-based solutions has led to a considerable expansion of this shift, which started with the introduction of online banking and credit card payments. The capacity of digital payment systems to instantly transact across geographical borders is one of its main benefits; this has had a significant influence on global trade and e-commerce in particular.

The convenience of sending and receiving payments devoid of time and geographical restrictions benefits both consumers and enterprises. For example, millions of users' payment procedures have been made easier by online platforms like Square, PayPal, and Stripe, which have made it possible for smooth transactions for products and services. Furthermore, by giving

people in isolated or underserved areas access to banking services, digital payment systems have improved financial inclusion. This trend is further shown by mobile payment systems like Apple Pay, Google Wallet, and Samsung Pay, which enable consumers to securely keep payment information on their devices and complete purchases with a single touch. Quick Response (QR) and Near Field Communication (NFC) code integration has significantly streamlined and accelerated the payment process while maintaining security.

Digital payment systems continue to prioritize security, and several safeguards are put in place to protect transactions. Tokenization, biometric identification, and encryption technology are a few of the major advancements that assist shield private financial information from unwanted access. Tokenization, on the other hand, substitutes unique identifiers that are worthless outside of the particular transaction context for sensitive information, while encryption guarantees that data communicated during a transaction is unintelligible to possible interceptors. Before completing a payment, biometric authentication which includes fingerprint and face recognition adds an extra degree of protection by confirming the user's identification. Digital payment systems still face certain difficulties even with these improvements. The integrity of digital transactions is significantly at risk from cybersecurity threats like phishing and hacking. Furthermore, both service providers and consumers need to continue paying attention to concerns about data privacy and regulatory compliance. To preserve confidence and protect user data, digital payment systems must comply with applicable laws, such as the Payment Card Industry Data Security Standard (PCI DSS) or the General Data Protection Regulation (GDPR) in Europe. The development of blockchain technology and cryptocurrencies is a direct result of the advancement of digital payment systems.

With the use of decentralized ledger systems for transaction recording, cryptocurrencies like Bitcoin and Ethereum provide an alternative to conventional fiat currencies. The visible and unchangeable transaction record provided by blockchain technology, the foundation of cryptocurrencies, improves security and lowers the possibility of fraud. Beyond cryptocurrencies, blockchain technology has applications in supply chain management, smart contracts, and decentralized finance (DeFi). It is anticipated that as digital payment systems advance, they will include cutting-edge technology like machine learning and artificial intelligence (ML) to further expand their functionalities. While machine learning (ML) models can forecast user behavior and customize payment experiences, artificial intelligence (AI)--driven algorithms can evaluate transaction patterns to identify and stop fraudulent actions in real-time. Furthermore, by presenting novel encryption techniques and testing established security mechanisms, developments in quantum computing may potentially have an influence on the domain of digital payments. More integration between digital payment systems and Internet of Things (IoT) devices is probably in store for the future. This will allow for smooth transactions with commonplace items like wearables and smart appliances. Maintaining a unified and effective global payment ecosystem will depend on assuring interoperability and standardization across many platforms and geographical areas as these systems become more commonplace.

CONCLUSION

The financial environment has seen a significant transformation due to the emergence of digital banking channels and platforms, which provide users with unparalleled ease and accessibility. Digital wallets, mobile banking applications, and online banking all provide special benefits, such as instantaneous mobile transactions, secure payment storage, and extensive web-based services. Along with improving customer experiences, these advances have encouraged financial institutions to compete more, which has advanced technology and raised service standards. However, there are drawbacks to the growth of digital banking, namely in the areas

of cybersecurity, data privacy, and regulatory compliance. For financial institutions, maintaining the security of digital transactions and protecting personal data is still of utmost importance. In addition, it is imperative to tackle the digital gap to guarantee that all users, irrespective of their technical aptitude or availability, get the benefits of these developments. In order to mitigate risks and maintain development, continuous investment in security measures, user education, and regulatory frameworks is important for digital banking. More innovation in digital banking is anticipated in the future; possible advancements include improved AI, blockchain integration, and smooth cross-platform interactions.

REFERENCES:

[1] M. Putica, "Influence of digital banking channels on the number of branches in European Union countries and Serbia," *Anal. Ekon. Fak. u Subotici*, 2020, doi: 10.5937/aneksub 2001067p.

[2] M. Yazbeck, "Customer satisfaction with digital banking channels: The case of the Lebanese banking sector," *Notre Dame Univ.*, 2020.

[3] Y. Son, H. E. Kwon, G. K. Tayi, and W. Oh, "Impact of customers' digital banking adoption on hidden defection: A combined analytical–empirical approach," *J. Oper. Manag.*, 2020, doi: 10.1002/joom.1066.

[4] S. Kozak and B. Golnik, "Migration of the Banking Sector to Digital Banking in Poland," *Econ. Reg. Stud. / Stud. Ekon. i Reg.*, 2020, doi: 10.2478/ers-2020-0021.

[5] S. Valero, F. Climent, and R. Esteban, "Future Banking Scenarios. Evolution of Digitalisation in Spanish Banking," *J. Bus. Account. Financ. Perspect.*, 2020, doi: 10.35995/jbafp2020013.

[6] J. Shifa Fathima, "Digital Revolution in the Indian Banking Sector," *Shanlax Int. J. Commer.*, 2020, doi: 10.34293/commerce.v8i1.1619.

[7] I. Y. Dalbah, "Management of Financial Technology and Its Impact on the Banking Services: Palestine," *Bus. Manag. Res.*, 2020, doi: 10.5430/bmr.v9n2p9.

[8] T. Boobier, *AI and the Future of Banking*. 2020. doi: 10.1002/9781119596165.

[9] S. Chandra Sekhar, "A Study on Effectiveness of Electronic Banking System," *Sanshodhan*, 2020, doi: 10.53957/sanshodhan/2020/v9i1/152472.

[10] L. B. Dam and K. Deshpande, "Relationship Between Demographic Variables and Awareness on Cybersecurity Threats: An Empirical Analysis," *Orissa J. Commer.*, 2020.

CHAPTER 4

AN OVERVIEW OF THE CONCEPT OF INFORMATION TECHNOLOGY IN BANKING SYSTEM

Meena Desai, Assistant Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- meena.desai@atlasuniversity.edu.in

ABSTRACT:

The financial sector has seen a fundamental transformation with the introduction of Information Technology (IT) into banking systems, which has improved data management, customer service, and operational efficiency. This overview looks at the use of IT in banking, with a particular emphasis on important technologies including automated teller machines (ATMs), online and mobile banking platforms, and core banking systems. With the use of core banking systems, banks may streamline procedures and save expenses by managing transactions, client accounts, and financial activities in real time. Online banking services give users convenience and accessibility by enabling them to conduct transactions, retrieve account information, and oversee financial activity from a distance. These features are expanded to smartphones via mobile banking apps, which provide real-time banking services and individualized financial management tools. Furthermore, technology-driven advancements like blockchain and artificial intelligence (AI) are having a bigger impact on banking procedures, boosting transaction transparency, and strengthening fraud detection. Notwithstanding these developments, there are still issues with integrating IT into banking systems, including the requirement for regulatory compliance, cybersecurity risks, and data privacy issues. This summary emphasizes how crucial it is to have strong security protocols and legal frameworks in place to deal with these issues. The constant growth of IT in banking emphasizes how important it is to keep up with technical developments and adapt to the ever-increasing needs of the digital era.

KEYWORDS:

Artificial Intelligence (AI), Automated Teller Machines (ATMs), Blockchain, Core Banking Systems, Mobile Banking.

INTRODUCTION

Computers have completely changed the way people arrange their time, jobs, communities, relationships with one another, and living spaces. The development of computers has been impacted by people's demands for processing information. In this quickly changing environment, banks have been digitizing their operations to provide services that are comparable to those provided by the most forward-thinking banks in other nations. This is done to stay up with technology advancements and client expectations. A lot of business elements have been impacted by information technology [1], [2]. A lot of improvements have been made possible by the advancement of information technology. As information becomes more digitally accessible, more companies are using digital technologies to improve their chances. Banks are now able to turn this procedure into a successful and long-lasting business thanks to information technology. Modern banking technology has been used by the Indian banking sector to transform bookkeeping, customer service, and management information system (MIS) reporting. Since then, the Indian banking sector has embraced computerization and automation, mostly as a result of regulations that have been put in place [3], [4]. The broad use of digital technology has facilitated the expansion and advancement of core banking systems, alternative

delivery channels, and many electronic payment methods, all of which enhance the general standard and ease of use of banking services. For clients, the ease of use of Internet banking has proved invaluable.

The banking industry in India has the potential to both gain from and contribute to the broad trend of widespread digitalization. Financial institutions' customer bases are fluctuating, but digitalization offers chances to enhance offerings, save expenses, and foster more devotion and loyalty. That being said, this is not only an Indian occurrence. In light of the fast-growing digital economy in India and the mounting demand from the government to assist the growing digital community, banks that have not yet made significant investments in digitization stand to earn much from doing so. In an attempt to safeguard themselves against the possibility of disruption in today's linked global markets, many multinational bankers are resorting to measures that would have been unthinkable in the banking industry even ten years ago. The Indian economy has seen a lot of activity recently in the area of new financial services. Numerous new fintech startups have appeared in the banking and financial markets industry.

Popular fintechs are starting to permeate every aspect of everyday life. In 1966, the Exchange Banks Association and the Indian Banks Association signed the first wage agreement with the unions. The agreement covered several items, including the use of IBM or ICT accounting machines for agency accounts, salary and provident fund accounts, inter-branch reconciliation, and other purposes. Indian banks came to the realization toward the close of the 1980s that they needed to employ computers to enhance MIS reporting, accounting, and customer service [5], [6]. Association on the placement of one mainframe computer per bank, minicomputers at zonal and regional headquarters, and Advanced Electronic Ledger Posting Machines (AELPMs) at branches. Signed in 1987, the second computerization agreement outlined the conditions for branches where AELPMs may be placed, as well as the extent of the computers and their configuration.

The primary objectives of computerization at the branch level are to enhance housekeeping standards, customer service, and data production for improved management control. The goal of computerization at the regional and head office levels is to quickly generate information by storing, analyzing, and retrieving data received from branches. This strengthens internal control over branches for the creation of policies. Banks were among the first to embrace personal computers when they were initially offered. These machines are now part of a Local Area Network (LAN) thanks to modifications [7], [8]. Banks began to use Core Banking technologies as technology developed. As a result, branch banking was superseded by bank banking. Core Banking Solution (CBS) has allowed financial institutions to provide improved customer convenience. This was a sensible step in providing clients with more convenient banking alternatives. Many Core Banking solutions gained more traction.

To remain competitive in the market and business, a large number of financial and commercial institutions have begun to provide digital client service. The computerization trend accelerated in 1991 and 1992 once the economy became more liberalized. A significant contributing aspect to this change was competition from international and private banks. Banks have benefited greatly from using modern technology. Significant savings have been made, and new sources of income have become available. Many thanks to the introduction of Internet banking, which made "Anywhere Banking" possible and contributed to the extraordinary expansion of the clientele. Its ability to access and analyze data continuously makes it a useful reporting system. Due to digitalization, human error rates have been reduced.

The convenience of anytime banking has been made possible by commercial banks in India moving toward technology through bank automation and mechanization, the introduction of

MICR-based check processing, electronic funds transfers, interconnectivity between bank branches, and the installation of ATM (Automated Teller Machine) channels. The Reserve Bank of India has made significant strides in bolstering and expanding the Payment and Settlement networks of banks [9], [10]. The process of moving specific activities from analog to digital forms is referred to as "digitization". Think about how ATMs have changed in comparison to the more conventional way of taking out cash from a bank branch, which requires speaking with a human teller.

The integration of various digital components such as digital functions, processes, and other digitally enabled activities into a potentially cohesive, enterprise-wide whole is known as digital transformation. Having a 360-degree view of the consumer and striving for a consistent cross-channel experience are two examples. Digital reinvention is pushing digitalization to unprecedented levels even as it advances. Historically, a lot of banks have made sporadic, piecemeal investments in technology, as was the case when they initially started offering online banking in addition to conventional banking sites. Customers were using just mobile devices more and more. Digital mobility has to be included in a cohesive omnichannel experience. The emergence of a more complete and systematic approach to technology investments and business transformation by several important conventional banking incumbents, along with competition from customer-centric born-digital banks, is pushing banks' technical and experience standards higher. The financial industry is undergoing another major change, which is mostly being caused by consumer expectations for easier, more convenient, and more relevant. Because of the industry's fast technological advancement, banking is changing fundamentally. Today's consumers want highly personalized content from their physical and online encounters.

DISCUSSION

They would rather remain silent and wait for someone else to speak first. Clients anticipate that their banks will notify them of any potential problems and keep them updated on their accounts. The Indian banking and financial sector has to be technologically ready to foresee and manage the upcoming problems as it grows and interacts with the world's financial markets. Banks in India are embracing computer-assisted contemporary systems and processes in place of their antiquated practices, as has been the case everywhere else in the globe.

During the early phases of bank computerization, banks primarily used stand-alone computer systems. In essence, they are single-user computers, which are used by only one person at a time, as the name suggests. The decision-making process including the processing and analysis of data was best suited for stand-alone systems; managers and executives in charge of making management choices made use of these systems. Although stand-alone systems aren't meant to be used in multi-user environments, they may be seamlessly integrated with current multi-user systems to get access to shared resources and corporate databases.

A stand-alone system in these situations is often referred to as a workstation or a node. Modern stand-alone systems are also capable of handling fax communications, multimedia, the Internet, and high-quality graphics. Installing single-user systems has many benefits, including cheaper hardware, simpler software, easier operational training for bank employees, and increased security. The single-user system can only be used by one person at a time and has restrictions due to its limited data storage capacity and sluggish processing speed. It is best suited for front-office branch computerization at bank branches with light workloads. During the first stage of computerization, banks used Branch-level automation, using standalone systems to manage transactions for certain products like as Current, Savings, and Loan accounts. These devices, referred to as Automatic Ledger Posting Machines, or ALPMs, were not networked. Since not

every product was automated, the General Ledger was created by hand. There were two main reasons why branch-level computerization was prioritized. First, at the branch level, the customer interface was optimized.

Increased use of computers and cutting-edge technology shortened wait times, improved account statement accuracy, and speed up money transfers. Each of these results in better customer support. Because branches were not connected to the Internet or used online banking, security was not a top priority when it came to computerization.

The majority of security features, including variable access permissions to the system, data locking capabilities, and password provisioning at multiple levels, were pre-installed in the hardware and operating system. Features like transaction tracking systems, disk duplexing, disk mirroring, frequent backups, and uninterruptible power supplies assist avoid system failures and facilitate recovery. The correct operation of the computerized systems was guaranteed by the creation of audit trails and extraordinary transaction reports.

Computers that allow several users to access them at once are known as multi-user systems. This category includes minicomputers, mainframe computers, microcomputers, supercomputers, virtual computers, and cloud computers. A central computer or server that can process information centrally is the hub of a multi-user computer networking system, to which numerous users from different terminals may connect via a network. Every piece of information is processed and kept on central servers. Online application development is a good fit for these time-sharing-based platforms.

The notion of centralized computing is used in the development of most financial systems. This is because such a processing system is made possible by the widespread use of operating systems (like Unix). The Unix platform is used by the majority of Database Management Systems (DBMSs), including Relational Database Management Systems (RDBMSs). The terminals in this method are power-constrained and unable to handle the data locally. The more users there are, the more work the central computer has to do. Indian banks began implementing total branch automation and mechanization in a multi-user computer system in the middle of the 1990s. Most banking goods were available in digitized form. Every client and company transaction is completed using a computer when a branch is fully computerized.

A transaction is logged each time it is entered via a terminal. Following verification and authentication, all related modifications are immediately reflected. The individual modules, or activities, are connected to create an integrated system that makes changes instantly. To guarantee data security and integrity, several security measures are put into place It is possible to generate a variety of outputs online, including client account statements, passbooks, vouchers, and ledger extracts.

The "single window" concept where clients may conduct and finish all of their transactions at any counter was made possible by total branch computerization. The systems may be configured to grow from a single window transaction to a partial or universal window transaction, based on the demands of the branch and the clients' convenience.

Additionally, it made it easier to use EFT (Electronic Fund Transfer) by processing and sending messages and money automatically between branches and banks. At point-of-sale terminals, EFT permits. A centralized branch computerization approach is known as core banking. The branches are linked to a central host that houses online various delivery channels, including ATMs, debit cards, telebanking/mobile banking, internet banking, and more, along with branch automation modules. The Bank uses a wide area network (WAN) to run a single banking software across all of its locations. CBS and contemporary financial services are merged. Core

banking solutions include real-time online transaction processing systems that process transactions in all sub-systems, such as client account ledgers, general ledgers, and other account books, while concurrently performing the required debits and credits.

Technology has been used to offer new items. Both the banks and their clients benefited greatly from the use of CBS in banks. However, this has also presented additional difficulties in stopping cyber fraud and dishonest people from abusing the system. To guarantee that appropriate checks, controls, and procedures are put in place to avoid or reduce abuse of computerization, the RBI has provided thorough instructions to the banks As a result, all Banks have provided personnel with operating guidelines. Operational controls in CBS operations include regular audits at the Branch and Data Center, regular verification of extraordinary transactions, observance of strong password policies, and data consistency checks. The Bank as a whole might be severely impacted by any errors in data center operations, hence caution should be used in their execution. Many laborious batch procedures are involved in day-end and day-begin activities, and their prompt completion is essential to the start of branch operations.

The Segregation of Duties, the Rotation of Duties, the Four Eye Principle / Maker Checker, and Ownership of systems for providing access rights are a few operational controls in Core Banking activities. Strong password access control techniques are supported by core banking technologies that enforce password standards such as length, encryption, and expiration. By integrating CBS with various payment systems, third-party service providers, billers, and e-commerce suppliers, banks have gone beyond Core Banking. The Internet, mobile devices, and ATMs are just a few of the service delivery channels that have been connected to core banking. Customers are happy and business has risen as a consequence of their ability to bank whenever and wherever they want.

For many purposes, banks may benefit from centralized data cleansing, holding, and analysis. Since ADC channels were made accessible for transactions outside of the Branch, the dangers and threats have grown. Customers who use phone banking may access their bank accounts and conduct financial transactions over the phone. Calling a designated phone number and following the instructions to get account information or carry out certain operations is the standard procedure for phone banking. Consumers may pay bills, transfer funds, check the balance of their accounts, and more via phone banking. Customers who don't have access to the Internet or who would rather do their banking over the phone might find this service extremely helpful. When a customer's internet or mobile banking service is experiencing technical difficulties, phone banking might be a helpful fallback alternative. The advent of smartphones marked the beginning of the next major revolution in banking. The development of mobile banking has made it possible for consumers to manage their finances at any time or place. It is now possible for users to create new accounts, check balances, make transfers, and do much more while managing their money on the move. Customers' desire to visit a physical branch has started to decline as mobile banking has grown in popularity.

Customers may use a smartphone or other mobile device for mobile banking, which enables them to access their bank accounts and conduct financial transactions. Usually accessible via a mobile app that can be downloaded to a device, mobile banking offers functions including checking account balances, transferring funds, paying bills, and locating local ATMs. Customers who may not have easy access to conventional banking channels or who prefer the ease of doing banking duties on the fly may find that mobile banking is a handy and secure method to handle their financial affairs. With a mobile wallet service provider, customers may preload money into their accounts and use those funds to make purchases at both online and offline stores that have been added to the provider's list. A mobile wallet is a virtual container

that operates on mobile devices. For example, a user may use their phone to pay for coffee at coffee shop A which is part of the XYZ mobile wallet. One may pay via an app, text message, social media account, or website, depending on the service provider. For example, companies like Paytm, MobiKwik, Freecharge, and others have collaborated with several stores to enable customers to pay using their mobile wallets.

Consumers may use mobile wallets for a variety of transactions, such as offline purchases, internet shopping, and utility payments. Mobile wallet ownership might be bank or non-bank. The non-bank supplier of mobile wallets must get a PPI license from the RBI before launching the product. A computerized cash register that uses both software and hardware is called a POS (Point-of-Sale) terminal. Retail businesses often use point-of-sale (POS) terminals that let consumers make purchases and pay using credit or debit cards. Modern point-of-sale (POS) terminals are capable of processing credit and debit cards, managing inventory, connecting to other systems via a network, and recording and tracking consumer orders and transactions.

Retailers will manage pricing lists, special promotional circumstances, customer loyalty data, inventory, and invoicing with a fully functional point of sale (POS). This model was created many years ago. They typically include a printer and a barcode reader. A card reader that accepts credit or debit card payments and a connection that extends outside a store's local area network (LAN) would enhance this approach. A point-of-sale (POS) machine is a compact, internet-enabled payment terminal that has a card reader, related software, a printer, and connection to banks and payment systems.

The terms "online banking," "e-banking," "virtual banking," and "internet banking" all refer to a particular kind of digital payment system that enables clients of banks or other financial institutions to carry out a range of financial transactions via the bank's website. Through a bank's website or mobile app, customers may utilize online banking to access their accounts and complete banking operations. Banks were able to lower transaction costs, more quickly and easily incorporate new services, and start focused marketing initiatives thanks to the convenience of online banking. The ability of CBS to provide online banking via digital channels such as ATMs, internet and mobile banking, etc., is one of its key characteristics. Additionally, it speeds up the clearance of checks. As a consequence of CBS, money leaks have been stopped and housekeeping has improved. Interbranch reconciliations are now automated, more precise, and quicker. The goal of the Banks' customer-centric innovations was to draw in and bring on board additional consumers. Customers have benefited from several advances and conveniences brought about by online banking via a variety of devices. The government increases risk in the monetary market as a consequence of laws, taxation, globalization, liberalization, and privatization.

Systems for payment and settlement are designed to make financial transaction clearing and settlement easier. Payment systems and services that are safe, affordable, and widely available promote growth, bolster financial stability, and broaden financial inclusion. Payment systems facilitate financial inclusion while fostering financial stability and economic growth. The Reserve Bank of India (RBI) has made ensuring safe, secure, dependable, accessible, inexpensive, and efficient payment systems a top priority. To accomplish this, India has developed one of the most sophisticated payment systems in the world, suitable for large, small, or quick money. Over the last decade, a plethora of diverse payment systems have emerged to simplify everyday life and bolster the trust of the general public by implementing safety and security protocols.

The RBI's function has evolved from that of regulator, operator, and facilitator to one of establishing the framework necessary for the planned growth of India's payments industry.

Since 2001, the strategic direction and execution strategy for this development has been given by the RBI's payments Vision publications. The systems that enable people, companies, and other organizations to transfer money that is normally kept in a bank account to one another are referred to as the "payments system." ensuring prompt transaction processing and the availability of financial services. It has a standard Online Transaction Processing (OLTP) environment, meaning that minor data additions, modifications, and deletions are possible inside a database. OLTP is intended for users with a high volume of transactions.

When databases are searched for analytical reasons in OLAP (online analytical processing) settings, data warehouses perform better. To assist banks, make better judgments, OLAP lets them see trends in their transaction data. Central A data warehouse stores historical banking data in a format that facilitates analysis and questioning. Data warehouses are designed to hold many types of data so decision support systems may get relevant information from them. A method for handling data across an entire company is a data warehouse. Analytics and business intelligence are built upon it. A data warehouse stores information from several sources, such as transactional programs and log files. Large volumes of information, particularly historical information, may be found in data warehouses.

CONCLUSION

Information technology usage in banking systems has completely changed the sector and brought about significant improvements in operational management, customer service, and efficiency. Financial activities have been concentrated by core banking systems, allowing for real-time processing and cost savings. Customers now have unparalleled access to their accounts and financial services from almost anywhere thanks to online and mobile banking systems. Some of the most important issues facing the business are addressed as cutting-edge technology like blockchain and artificial intelligence are integrated to further improve the security and transparency of financial transactions. But there are also a lot of difficulties associated with IT's quick development, especially when it comes to data protection and cybersecurity. Maintaining regulatory compliance and protecting sensitive data is essential for maintaining confidence and averting security breaches. To successfully manage possible risks, financial institutions must continue to embrace technological innovations invest in a strong security infrastructure, and keep up with developing trends. With possible advancements in fields like biometric identification and quantum computing, the future of IT in banking seems promising. In the end, maintaining operational effectiveness and customer trust will require striking a balance between technological advancement and a dedication to security and regulatory compliance, which will be necessary for the successful integration of IT in banking.

REFERENCES:

[1] A. V. Kolesnikov, L. E. Zernova, V. V. Degtyareva, I. V. Panko, and Y. I. Sigidov, “Global trends of the digital economy development,” *Opcion*, 2020.

[2] A. Annarelli, F. Nonino, and G. Palombi, “Understanding the management of cyber resilient systems,” *Comput. Ind. Eng.*, 2020, doi: 10.1016/j.cie.2020.106829.

[3] M. T. G. M. Naidu and D. P. S. Rani, “Role of Technology in Financial Services of Commercial Banks in Visakhapatnam,” *Int. J. Recent Technol. Eng.*, 2020, doi: 10.35940/ijrte.e5636.059120.

[4] C. Flavián *et al.*, “Evidence Of Digital Financial Services Impacting Women’s Economic Empowerment What Explains The Impacts And What Is Left To Learn The authors are grateful to,” *Int. J. E-bus. Res.*, 2020.

[5] S. G. Magomedov, P. V. Kolyasnikov, and E. V. Nikulchev, "Development of technology for controlling access to digital portals and platforms based on estimates of user reaction time built into the interface," *Russ. Technol. J.*, 2020, doi: 10.32362/2500-316x-2020-8-6-34-46.

[6] F. Bharucha, R. K. Kothadiya, and T. Y. J. N. Malleswari, "Securing medical records for insurance claims using blockchain technology," *Int. J. Adv. Sci. Technol.*, 2020.

[7] Sukirwan, "Pembelajaran dari Rumah: dari Klasikal ke Digital," *Hum. Relations*, 2020.

[8] S. Kharel, "Tourism entrepreneurs awareness level of knowledge management for promoting visit Nepal 2020 in Kathmandu, Nepal," *Hum. Relations*, 2020.

[9] C. Jiang and Z. Li, *Mobile Information Service for Networks*. 2020. doi: 10.1007/978-981-15-4569-6.

[10] ODCE, "Aid by DAC members increases in 2019 with more aid to the poorest countries," *Human Relations*. 2020.

CHAPTER 5

EXPLAIN THE ROLE OF RESERVE BANK OF INDIA IN DIGITAL BANKING AND TECHNOLOGY

Dr. Varsha Agarwal, Associate Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- varsha.agarwal@atlasuniversity.edu.in

ABSTRACT:

The Reserve Bank of India (RBI) has a significant influence on how digital banking and technology are developed in India. It encourages innovation in the industry while maintaining consumer protection and financial stability. The main responsibilities of the RBI in the area of digital banking are examined in this synopsis, which includes financial inclusion promotion, regulatory framework creation, and supervision of digital payment systems. The National Payments Corporation of India (NPCI) was established, and frameworks for digital lending and mobile banking were introduced as some of the measures the RBI has put in place to support the expansion of digital banking. The efficiency, security, and accessibility of financial services are the goals of these initiatives. By addressing concerns like cybersecurity and data privacy, the RBI's regulatory rules make sure that digital banking systems follow standards of operational integrity and client safety.

The RBI's programs to promote digital financial inclusion and literacy also contribute to the larger goal of bringing marginalized groups into the formal financial system. In spite of these developments, the RBI is still working to reconcile innovation with the preservation of financial stability by addressing issues including technology disruptions and regulatory compliance. This summary emphasizes how important the RBI has been in steering the development of digital banking in India, making sure that innovations in technology meet legal requirements and support a diverse financial sector.

KEYWORDS:

Digital Banking, Financial Inclusion, National Payments Corporation of India (NPCI), Reserve Bank of India (RBI), Regulatory Frameworks.

INTRODUCTION

The goal of today's banks is to provide customers with a seamless, accurate, and fast banking experience. The RBI has acted as a mentor for the banks, offering advice and rules to help them accomplish a range of goals. For all Indian banks, digitalization is now their top focus. and settlement mechanisms used by Indian banks. Through the introduction of MICR-based check processing, electronic fund transfers, branch interconnectivity, and ATM (automated teller machine) channels, Indian commercial banks have embraced technology to provide their customers with the flexibility to bank whenever they choose [1], [2]. To assist the banking sector, get closer to its objectives, the Reserve Bank of India (RBI) has shaped laws and offered guidance.

Technology advancements in banking have focused on using digital technologies to promote the adoption of new payment methods and change customer perceptions of a society that uses "less cash." The Digital Payments Index (DPI), designed to show how much payment processing is becoming digital nationwide, showed growth in the use and sophistication of digital payments. To promote innovation in an institutional and sustainable manner, the Reserve Bank Innovation Hub (RBIH) was founded as a fully owned subsidiary [3], [4]. In

order to build an ecosystem that facilitates access to financial services and products and advances financial inclusion, the Hub collaborates with banks, financial institutions, technology, businesses, and academic institutions. It also helps individuals exchange ideas and create prototypes linked to financial innovations.

It would provide the organizational framework needed to support FinTech research and make working with entrepreneurs and innovators easier. The Hub has its headquarters in Bengaluru and is run by an independent Board made up of distinguished business and academic leaders. The Reserve Bank of India (RBI) launched the Regulatory Sandbox program, which exempts financial technology (Fintech) businesses from certain regulatory restrictions and lets them test their products and services in a real-world setting [5], [6]. The goal of the Regulatory Sandbox is to provide fintech businesses a secure, regulated environment in which they may develop and experiment without putting customers at unnecessary risk. Using application programming interfaces (APIs), open banking allows banks and other financial organizations that are not banks to exchange transaction and customer data with outside financial service providers. Another name for open banking is "open bank data.

Open banking facilitates the management and access of consumer banking and financial accounts by third-party applications. It may change user experience and banking competitiveness. Due to the extensive sharing of client data, "open banking" presents both significant threats and many possibilities. With open banking, online financial service providers have access to and control over customer data. In order for the banks to provide access to outside service providers, customers must agree.

Open banking will facilitate the sharing of accounts and data between financial institutions, customers, and third-party service providers. Third-party APIs may look into a customer's accounts and transaction history and provide them a range of financial services using consumer and financial counterparty data. Additionally, they may compile information from customers and partner financial institutions to create marketing profiles, as well as carry out new transactions and account adjustments on their behalf. Open banking is emerging as a significant source of innovation that has the potential to revolutionize the financial sector. Third-party applications may access and control customers' banking and financial accounts thanks to open banking [7], [8]. The banking industry may see more competition as a result of open banking, and consumer interactions with banks may alter. Neo Banks are online-only virtual financial institutions (FFIs) that provide digital banking services to its clientele. Neo Banks promises a seamless online experience by overlaying an immersive digital layer on top of conventional banking. Because of the focus on technology, customers enjoy how easy it is to create accounts and start utilizing the services without help. Neo Banks in the nation depend on their partnerships with conventional banks to provide some of its essential services since they are not yet permitted to run fully digital banking facilities.

Neo Banks function independently of physical financial institutions and are fully online. In contrast to conventional banks, they don't have any physical locations. They only provide a range of specialized services online, in contrast to more traditional banks that have both an online and physical presence. NeoBanks, in contrast to traditional banks, often focus on a small range of services, but they also commonly use cutting edge technology, such as artificial intelligence, to provide highly personalized services to each individual client. Neo Banks may provide its services to clients at a far lower cost than traditional banks.

While Indian authorities applaud fintech advancements, Neo Banks still have a lot of security and regulatory hurdles to overcome. Like any other kind of financial institution, they have benefits and downsides.Expenses may be minimized since no office building or other

infrastructure is required. Customers gain from this in part because interest rates are made more appealing and fees for different transactions and services are decreased or eliminated. Enhanced operational efficiency: Neo Banks are open twenty-four hours a day [9], [10]. Daily tasks, including paying bills, are simple to do anytime and wherever the consumer wants. They also use AI to promptly address customer concerns, further personalizing their support offerings.

Neo Banks take additional care to guarantee the privacy of their clients' personal information and the security of their transactions since they do not operate on outdated technology. Ensuring total protection of consumer data becomes paramount. Aid is not provided one-on-one: The inability of most customers to get in-person assistance with complex financial transactions or processes may cause them frustration. This is the reason why some individuals could feel uncomfortable use Neo Banks for certain transactions, especially the elderly or those who are not tech-savvy. Neo-banking is a modern alternative to traditional banking, but since it lacks the same experience as traditional banks, it lacks credibility and confidence. Neo Banks are not capable of running on their own. Because they lack clear policies and a clear legal framework, they are unable to take deposits or provide lending products from their books. In the worst-case situation, as these banks lack any explicit policies or legal safeguards to protect them, the money of their clients may be at risk when they file for bankruptcy.

DISCUSSION

Neo-banks and digital banks are undoubtedly growing in popularity, but many of these establishments still need to demonstrate that they can turn a profit on a regular basis. They might, nonetheless, significantly upset the banking and financial services industries. Convincing existing banks to re-engineer processes and invest in state-of-the-art technology in order to provide easy and expedient client service would be essential to their success. Technology breakthroughs and shifting consumer tastes have caused a major revolution in India's banking industry in recent years. Customers may now more easily access financial services via their smartphones and other devices thanks to the growth of digital banking. As a result, there has been a rise in the availability of online and mobile banking services, including contactless payment options such UPI Artificial intelligence (AI) and machine learning are being used by Indian banks to increase the accuracy and efficiency of their operations. AI-enabled chatbots, for instance, may respond to consumer inquiries, and machine learning algorithms can assist banks in identifying and preventing fraud.

In order to get access to cutting-edge technology and provide their clients with cutting-edge financial goods and services, several banks in India are collaborating with fintech businesses. New business models, like Neo Banks, which are exclusively digital banks without a physical location, are the result of this. Artificial Intelligence (AI) and Business Analytics have changed dramatically. Robotics with AI capabilities is predicted to be the next big thing in the banking sector. In an effort to enhance services and save expenses over time, a number of private banks plan to use robots for loan approval, financial advice, and customer support. Digital banking is going to be the most common kind of banking in the next years.

For all banks to promote innovation, operational effectiveness, and commercial expansion, they must discover the benefits of the digital age. Artificial intelligence (AI) and cognitive computing, bots, drones, the Internet of Things (IoT), smartphones, social media, and new security-related technologies like blockchain are just a few of the developing technologies that have impacted banking. Furthermore, the cloud is a universal technology that serves as a platform for everything. By combining this technology with reworked procedures, firms may progress a fundamental reimagining of their operations. Additionally, firms may begin a

significant redesign of their strategies, processes, and operations from a customer-centric viewpoint by putting consumers at the start or center of strategic processes rather than at the conclusion, where they have historically been placed.

In order to remain competitive and support the digital economy, banks should consider collaborating with FinTechs and huge tech companies to build specialty products that provide superior customer experiences and ease. This will help them compete with Neo banks. The few issues that still plague the banking sector include data breaches or leaks, customers' lack of experience with online banking, and the rapidly changing nature of technology. Banks are required to safeguard the confidentiality of their customers, provide them better services, and maintain the security of their financial data. The government, business specialists, and other financial organizations may come up with practical solutions to the aforementioned problems together.

The digital era and highly interconnected surroundings of today necessitate that banks continuously reengineer their business procedures. The adoption of constantly changing technology, transaction costs, employee retention, privacy and security, partnering with fintechs, standardization, and capacity building are some of the issues facing the Indian banking industry. With the medium-term objectives of lowering operating costs, improving customer services, and raising overall efficiency, the banking sector has been more quickly computerized thanks to the financial sector reforms of the 1990s, as well as the opening of the economy and its integration with global markets. Global banking and other financial institutions now operate differently as a result of information technology and communication networking technologies. Every financial institution in highly developed countries may be accessed online. Banks and other financial organizations in India have begun using computer networking and information technology. It will take time for banks to integrate cutting-edge technology into their regular business processes.

In India, computerization does not aim to replace people with technology. Rather, the objective is to provide consumers and staff compelling reasons to come to work. The banking sector is dependent on technology as it consumes a lot of information and data. It should go without saying that in order to properly use new technology, the banking industry's structure, organization, processes, and attitudes will need to change. Mobility that offers anywhere, anytime banking, high service availability, quickness and efficiency in transactions, account aggregation, relationship banking, and data and money security and privacy are only a few of the needs of the customers. Bankers want to increase revenue growth, workforce productivity, financial inclusion, and consumer engagement and experience all at the same time. Banks have always used technology to enhance their offerings and operational effectiveness. Technology of today is altering client relationships in addition to the environment. Along with breaking down numerous barriers, technology has also resulted in better goods and channels. As a result, consumer connections are now receiving more attention. It is also seen as a means of saving expenses and effectively connecting with individuals and organizations in the banking industry.

To stay competitive and remain among the top global suppliers of complex services, banks have made significant investments in digital technology. The nation's banks must use best worldwide practices and develop cutting-edge new goods, services, and business models in response to the demands of India's digital customers. By creating creative plans that combine digital transformation with quick adoption of cutting-edge technologies like artificial intelligence (AI) and cognitive computing, India's financial institutions can compete with the finest in the world. A computer network is made up of many linked computers or other devices that cooperate to share information and services offered by different network "nodes." Network-connected computers may exchange data using conventional protocols delivered

across digital connections. These connected computers and gadgets are supported by telecommunication networks, which may take many different shapes based on the intended network architecture.

Nodes in a computer network might include standalone PCs, servers, networking devices, and other specific or all-purpose hosts. These gadgets sometimes feature hostnames in addition to IP addresses. Once hostnames are created as memorable labels for the nodes, they are assigned initially and are seldom modified. Network addresses are used by data exchange protocols, such as the Internet Protocol, to locate and identify the nodes participating in a particular transmission. Information sent between devices is referred to as "transmission mode" or "communication mode." Every communication channel has an orientation depending on the transmission medium. The direction in which the signal is conveyed is referred to as the "transmission mode" in this context. Simplex mode allows for unidirectional communication, meaning that data only flows in one way. Devices operating in simplex mode can only transmit or receive data; they cannot send and receive data at the same time. Since most network interactions need data flow in both directions, the simplex mode is not particularly common. In enterprises where a comparable reply is not necessary, the simplex method is used. The direction of data flow in Half-duplex mode may be reversed, meaning that data can be sent in both ways, but not concurrently, unlike in Simplex mode. The channel's whole bandwidth may be utilized in one way at a time while in half-suplex mode.

Half-duplex mode allows for error detection and allows the recipient to resend the data in the event of a transmission fault. One useful example of the half-duplex mode, in which one person may only listen while the other talks, is a walkie-talkie. They are unable to talk at the same time, however. Signals from numerous communication lines are received by a multiplexer device, which then forwards them to one communication line and vice versa. A multiplexer groups together many low-speed lines into a particular group on a single high-speed line by combining their separate data transmission capacities. Several input lines are fed into a multiplexer (MUX), which merges them into a single output line. The many-to-one rule, which has n input lines and one output line, is used in multiplexing. Effective communication between two linked pieces of equipment can only happen when they can "talk" and "understand" the same language. Stated otherwise, a common protocol for communication need to exist. Every kind of communication connection, such as cables, connectors, and software on linked devices that manages data transfer across a network, has its own set of protocols. A protocol is a convention or standard used in computing that manages and makes it easier for computer end points to connect, communicate, and transfer data. In its most basic form, a protocol is a set of rules that govern the synchronization, syntax, and semantics of communication.

Protocols may be implemented using hardware, software, or a mix of the two. At its most basic level, a protocol explains how a hardware connection behaves. The guidelines for communication between related process modules, often located on separate nodes, are known as protocols. Message formats and the guidelines for exchanging messages are specified by protocols. It manages transmission faults, transmission priority and order, as well as the start and finish of conversion. A fiber-optic cable, often referred to as an optical fiber cable, is a kind of cable that transmits data using optical fibers as opposed to electrical wires. The optical fiber components may be separately plastic-coated and enclosed in a protective tube, depending on the working circumstances. Among the applications for optical fiber cables are high-speed data transfer and long-distance communication.

Due to their numerous benefits over copper lines, fibre optic cables are becoming more and more popular. Increased bandwidth and higher transmission rates are two of these benefits. Data may be sent quickly and across long distances using fiber fiber optics. Additionally, since

optical fiber connections transfer data using light rather than electronic signals, they are impervious to electrical blockage. Because of this, situations with high levels of electrical interference are best suited for optical fibres. Because it links local area network (LAN) devices that employ the same protocols, a hub is the most fundamental network connecting device. A hub's only purpose is to transmit electrical signals that are received on one port to every other port that is connected. Hubs function at the Physical layer of the Open Systems Interconnection (OSI) paradigm and lack the ability to filter or address packets. In addition to connecting different computer networking devices, a network hub also acts as a repeater by boosting signals that travel great distances. Hubs are applicable to digital and analog data types. When data is received in digital format, the hub transmits it as packets; when data is received in analog form, the hub transmits it as signals.

These days, switches are preferred over hubs because they are more cost-effective, more efficient, and provide more features. Since messages are not broadcast and all communication takes place directly between the source and destination systems, switching has a very low packet collision risk. Every networking gadget is assigned a distinct MAC address. The switch wraps an IP packet into a Frame containing the source and destination MAC addresses when it is transmitted from one device or computer to another. Then, it delivers the Frame to the intended recipient. At the destination, the frame is stripped and transmitted to the device whose MAC address corresponds to the target MAC address of the IP packet recipient. Data packets are routed from one network to another by use of a network router. Links between various Internet Protocol (IP) networks are made using routers. A router controls the direction in which data flows between several networks. These two networks could be either public or private.

The first line of defense is the router, which has to be set up to only let approved traffic through. As smart devices, routers save data about the networks to which they are linked. With the use of access control lists (ACLs), the majority of routers may be set up to operate as firewalls that filter packets. Firewalls, packet inspection, network address translation (NAT), access control lists (ACLs), and other features are supported by routers. Routers use a variety of network topologies to intelligently send packets to the addresses they have been assigned. Routers use the Routing Information Protocol (RIP), the Border Gateway Protocol (BGP), and the Open Shortest Path First (OSPF) protocol to exchange information.

A router may be either dynamic or static. While dynamic routers generate their routing tables by learning about other routers in their network, static routers are manually setup. Routers link two or more networks and are useful for a wide range of applications. An interface of a router is linked to its Address Resolution Protocol (ARP) module, LAN address (network card address), and Internet Protocol (IP) address. The router uses an internally maintained routing table to direct a packet to its intended destination.

A device that directs packets to and from the Internet and perimeter networks is called an external router. Packets will be ignored or routed to the right destination if the routes are set up correctly. Additionally, we may set up the external router to only let a certain set of protocols to connect from the Internet into the perimeter network. The firewall policy alone includes Two or more hosts or network segments are connected via bridges. Bridges' main function is to store and forward frames between the segments they link. Bridges transport data frames by using the hardware's Media Access Control (MAC) addresses. Bridges have the ability to either permit or prohibit data transfer, depending on the MAC address of the linked devices in each segment. Bridges may be used to link two real Gateways usually function at the Transport and Session levels in the OSI model. Above the Transport layer, there are several protocols and standards from numerous vendors; they are translated between by means of gateways.

Gateways may translate two networking protocols: Transmission Control Protocol/Internet Protocol (TCP/IP) and Open System Interconnection (OSI). For this reason, networks that run independently and use various routing protocols, topologies, domain name systems, and administrative procedures may communicate with one another thanks to gateways. Before allowing a data packet to get through, a physical firewall, also known as a hardware firewall, inspects it. It functions similarly to a main entry metal detector door in a building. It determines whether a data packet should pass through by examining the source and destination addresses following predetermined guidelines. A software firewall filters traffic and decides whether to grant or deny access to certain ports and programs on a computer system when a data packet reaches the network. Better security and control against insider threats are made possible by this.

Access control lists are used to record Internet Protocol (IP) addresses that are untrustworthy. Any data packets coming from such IP addresses will be rejected by the firewall. As an alternative, the firewall may only let traffic from IPs that are listed as coming from reliable sources in the access control list. A firewall may be configured in a variety of ways. Generally speaking, the kind of firewall and its configuration have an impact on the amount of protection they provide. The interconnection of all the parts that make up a network is referred to as its topology. Physical topology and logical topology are the two main categories of topologies. The way the devices are physically linked using cables is described by a physical topology. A logical topology explains to the user how devices seem to be linked.

CONCLUSION

By striking a balance between innovation and regulatory monitoring, the Reserve Bank of India (RBI) has played a significant role in the development of digital banking and technology in the Indian financial industry. The National Payments Corporation of India (NPCI) and other regulatory frameworks and efforts of the RBI have made a substantial contribution to the growth and development of digital banking services. The Reserve Bank of India (RBI) establishes guidelines for cybersecurity, operational integrity, and client safety to guarantee that digital banking systems function in a controlled and safe environment. The financial inclusion and digital literacy initiatives of the RBI have been crucial in facilitating the integration of marginalized communities into the financial system and augmenting their availability of banking services. However, there are constant obstacles brought about by the quickening rate of technology advancement, such as the have to constantly modify regulatory measures in order to handle new dangers and disruptions. The RBI will continue to play a critical role in leading the digital banking industry through these changes as it develops, making sure that technology innovations comply with legal requirements and support a safe, stable, and inclusive financial environment. The continued expansion and prosperity of digital banking in India will depend heavily on the RBI's proactive approach to resolving these issues and encouraging innovation.

REFERENCES:

[1] M. H. Adil and N. R. Hatekar, “Demonetisation, Banking and Trust in ‘Bricks’ Or ‘Clicks,’” *South Asia Res.*, 2020, doi: 10.1177/0262728020915566.

[2] J. Shifa Fathima, “Digital Revolution in the Indian Banking Sector,” *Shanlax Int. J. Commer.*, 2020, doi: 10.34293/commerce.v8i1.1619.

[3] B. R. and P. S. Aithal, “RBI Distributed Ledger Technology and Blockchain - A Future of Decentralized India,” *Int. J. Manag. Technol. Soc. Sci.*, 2020, doi: 10.47992/ijmts.2581.6012.0091.

[4] M. C. Arthi and K. Shanmugam, "Financial Inclusion via Mobile Banking – A Comparison Between Kenya and India," in *IFIP Advances in Information and Communication Technology*, 2020. doi: 10.1007/978-3-030-64849-7_50.

[5] A. Perwej, "The Impact of Pandemic Covid-19 on the Indian Banking System," *Int. J. Recent Sci. Res.*, 2020.

[6] J. Saini, "The Future of Blockchain and Whether India Should Have a Specific Law on This Aspect?," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3562306.

[7] D. D. R. Srivastava, S. Pandey, and A. K. Sinha, "Role of digital banking in increasing financial inclusion in India," *Indian J. Econ. Bus.*, 2019.

[8] K. K. Das and R. Mahapatra, "Customer perception towards payment bank: A case study of cuttack city," *Int. J. Manag.*, 2019, doi: 10.34218/IJM.10.4.2019.001.

[9] R. Agrawal, "Review of Initiatives taken by the Government and the Banking Regulator for Successful Transition to a Financially Inclusive Economy: An Empirical Study of India," *Econ. Anal.*, 2019, doi: 10.28934/ea.19.52.12.pp81-96.

[10] D. Sengupta and N. Shastri, "Digital payments through PFMS - Facilitating digital inclusion and accelerating transformation to a 'Digital Economy,'" in *ACM International Conference Proceeding Series*, 2019. doi: 10.1145/3326365.3326391.

CHAPTER 6

ANALYSIS OF NETWORK OPERATING SYSTEM IN DIGITAL BANKING SYSTEM

Hansika Disawala, Assistant Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- hansika.disawala@atlasuniversity.edu.in

ABSTRACT:

Network operating systems (NOS) must be integrated into digital banking systems in order to manage the complex IT infrastructure that underpins contemporary banking activities. This investigation looks at how NOS might improve digital banking services' dependability, efficiency, and security. Network operating systems, including Windows Server, Linux, and UNIX, provide the foundational infrastructure needed to manage network resources, facilitate server-to-client communication, and guarantee error-free data processing. Digital payment systems, online and mobile banking platforms, and core banking applications all depend on these technologies. Banks may maintain high levels of service availability and performance by using NOS, which facilitates effective network management, load balancing, and resource allocation. Furthermore, NOS helps to keep digital banking systems secure by enforcing strict access rules, keeping an eye on network activity, and defending against online attacks. The significance of NOS's scalability and flexibility in enabling banks to adjust to shifting client expectations and technological demands is further highlighted by this investigation. The dependence on NOS does, however, come with drawbacks, including the need for frequent upgrades, vulnerability management, and compatibility with cutting-edge technology. All things considered, Network Operating Systems are essential to the backbone of digital banking systems because they provide security, agility, and operational effectiveness in a financial environment that is changing quickly.

KEYWORDS:

Cybersecurity, Load Balancing, Network Operating Systems (NOS), Scalability, Security.

INTRODUCTION

Centralized control and distributed control are the two fundamental types of local area network architectures utilized in information transfer. While distributed controls are based on ring and bus topologies, popular centralized control networks are based on star and tree topologies. Every topology has benefits and drawbacks. Every device in a network with a bus topology is linked to a single, continuous connection called the "backbone cable." There are two ways that nodes may connect to the backbone cable: directly or via a drop cable. Whether or whether the message is addressed, it will be transmitted to every station in the network. Every other workstation receives transmissions from any workstation that traverse the full wire length in both directions. Bus topology is quite simple to set up, and if one LAN workstation node fails, the network as a whole remains unaffected [1], [2].

Bus topology, on the other hand, provides little room for modification and restricts geographical expansion. A local area network (LAN) consists of two or more computers connected by a server. Networked computers share a common space and interact with one another. The two most significant components of this network are Ethernet and Wi-Fi. LANs are used to link computers in a variety of locations, including companies, laboratories, universities, schools, and libraries.

Every node in a local area network has the ability to function independently and interact with other systems. Therefore, a computer network is a data communication network that is primarily used to exchange hardware, software, and data resources in order to enhance the flow of information inside and outside of an organization. In general, Cat5e cables have a 100-meter maximum LAN wire length [3], [4]. The network's establishment medium affects both the supported node count and distance. Any autonomous system is referred to as a node in a local area network (LAN), and a node that is linked to other nodes is called a LAN. Typically, all network services are provided and controlled by a single central node, or server. The client nodes ask the server for the services they need, and the server responds. The server in charge of these services is determined by the protocols and topology.

The essential components of LAN functioning are sharing common cabling and pooling resources within a workgroup. In contrast, a local area network (LAN) makes use of network adapters that utilize unique methods to share a common medium such as a cable, radio, or light wave among the linked nodes. Software is also used by a LAN to handle many client stations' simultaneous service requests [5], [6]. A Wide Area Network (WAN) is a large computer network that is dispersed across a considerable amount of land and often makes use of the telecommunications network. WANs are often used in the banking industry to link branches to regional offices, regional/zonal offices to head offices, etc. In general, WANs have far lower data transfer rates than LANs due to their constrained transmission speeds and capacities. Computers can communicate with one another even if they are located in distant locations thanks to WAN.

It occurs in several locations rather than just one. Another way to think about WAN is as a collection of linked local area networks. The most well-known example of a WAN is the Internet. WLANs are computer networks that use wireless network technologies, such Wi-Fi, yet operate similarly to local area networks. This network, in contrast to a local area network (LAN), allows objects to connect wirelessly rather than via physical lines. One excellent example of a WLAN is Wi-Fi. WLAN is a wireless data transmission method that may be used with two or more devices. WLANs often include Internet access points and use high-frequency radio waves. WLANs allow users to roam freely within the coverage area, which is usually a home or small business, all the while maintaining a network connection [7], [8]. When utilizing public networks, users may create a secure network connection with the use of a VPN, or "Virtual Private Network". With a VPN, a user's online identity is concealed and internet traffic is encrypted. Real-time encryption takes place. This makes it far more difficult for unauthorized users to keep an eye on someone's online activity and steal information from them.

Improved functionality, security, and network management are among the benefits of a VPN. It gives remote workers access to resources that are not available via a public network. Although often used, encryption is not a requirement for a VPN connection. Dedicated circuits or tunnelling methods are used to create a virtual point-to-point connection via pre-existing networks in order to construct a VPN. Some of the benefits of a wide area network (WAN) may be obtained via a VPN that is available over the public Internet. The resources of the private network are seen from a distance by the user.

Network operating systems are the programs and related protocols that enable efficient and economical network communication between independent computers. It permits the sharing of hardware like disks, printers, and the between computers. UNIX, Windows, and MS-DOS are a few types of network operating systems. A network operating system's job is to configure certain PCs/servers as hosts and other PCs as clients of those hosts. The hosts are in charge of their customers' file sharing, printer sharing, and communications connection sharing. These services might be dispersed among several servers or they could operate on a single server [9],

[10]. Any common network may be used to run the network operating system software. Using Transmission Control Protocol/Internet Protocol (TCP/IP) connections, computers may send files to one another using the File Transfer Protocol, or FTP.

Transferring data across systems is simple, but it may sometimes lead to issues. For example, the file organization rules in two systems could vary. The methods in which text and data are displayed in two systems could vary. There might be differences in the two systems' directory structures. The FTP protocol avoids these issues by creating two connections between hosts. A single connection is made to the Secure File Transfer Protocol (SFTP), a network protocol designed to protect private information and facilitate the access, management, and transfer of large files. The Secure File Transfer Protocol allows file access, transfer, and management across a network. It was created by the Internet Engineering Task Force as an extension of the Secure Shell (SSH) protocol. Telnet is an application protocol that facilitates remote computer communication between users who are located in separate places. TELNET uses the Transmission Control Protocol/Internet Protocol (TCP/IP) combo to establish a connection with a distant system. The distant systems communicate as if they were locally linked.

DISCUSSION

Programs for terminal emulation enable users to connect to a remote computer and commonly utilize TELNET as a communication channel. However, TELNET may also be used to facilitate communication between processes and terminals. Other protocols, such as the File Transfer Protocol (FTP), which makes use of TELNET, may also be used to establish a protocol control channel. A switch is a component that connects several PCs and gadgets inside a local area network. In the OSI model, it functions at the data link layer. Devices are connected by a network switch so they may interact and exchange data packets. Switches are virtual devices that govern physical networks and may be either hardware or software-based.

In many data networks, a switch is a typical network equipment. Switches provide wired connections to a variety of Internet of Things devices, such as card entry systems, industrial machines, printers, and wireless access points (APs). They link real servers and a significant amount of the storage infrastructure to the PCs that house virtual machines (VMs) in data centers. Switches in telecoms provider networks handle enormous volumes of traffic. A network switch functions at the data-link layer of the Open Systems Interconnection (OSI) paradigm. In an Ethernet-based local area network (LAN), a network switch looks up the media access control (MAC) address to figure out where to transmit each incoming messageframe. Switches keep tables that link each MAC address to its matching port.

Messages are not transmitted by a switch. Rather, it guarantees that data is sent just to the intended device by using the destination address. Full duplex mode is used for switching, and no setting is needed. Switching prevents network packet collisions and allows for the best possible network bandwidth use. The acronym for "Open System Interconnection" is OSI. This refers to a reference model that illustrates the transfer of data across physical media from one computer's software program to another. The OSI model was created in 1984 by the International Organization for Standardization (ISO). These days, it serves as a paradigm for the architectural communication between computers. Computers may communicate with one another via a network using DNS. DNS maintains track of all internet hosts' names using a distributed database. DNS servers respond to queries from clients by sending replies back to the servers. Using a client request and a name, forward DNS lookups convert the request into an IP address. Reverse DNS lookups convert an IP address from a client request into a name. The DNS server resolves the IP address of the hostname when a client sends a request containing a hostname. A DNS server routes a request to an alternative DNS server if it is

unable to resolve the IP address associated with a hostname. The resolver uses the internet protocol to complete the request if the IP address reaches it. A "Uniform Resource Locator," or "URL," is required for users to access content on the Internet. Using a URL is a common method to locate any information on the Internet. HTTP makes use of the URL concept to make content easier to access.

A URL is made up of four components: the route, the host computer, the method, and the port. There are two components to a website address. The first is the domain name, which links the name and goals of the brand to the web address. The domain name extension, which expresses the nature and purpose of the website, is the second component. The letters that appear after the second dot in a URL are much more important in establishing the legitimacy of the website and its degree of brand alignment than the letters that appear between the two dots.

Websites may be categorized using domain extensions, also known as top-level domains (TLDs), based on their nature, location, or business plan. The most often used domain extensions on the Internet are ".org," ".com," and ".net," out of hundreds of options. Creating web apps. The notion of centralized computing is used in the development of most financial systems. This is because a processing system like this is made possible by the widely used Operating Systems (like Unix). The Unix platform is used by the majority of Database Management Systems (DBMSs), including Relational Database Management Systems (RDBMS). The terminals in this method are power-constrained and unable to handle the data locally. The more users there are, the more work the central computer has to do.

Services may also be offered via delivery channels, like as ATMs, the Internet, and mobile devices, in addition to branches. Nearly all computerized information systems process their data in a data center (DC). Every day, the DC must handle massive amounts of data, necessitating a significant infrastructure and upkeep budget. Any financial institution's network infrastructure is essential to the continued provision of services. A high-performance computer network that is scalable, secure, dependable, and designed for optimal speed and efficiency is necessary. Since wide area networks are built on top of telecommunication networks, the kind of network and the type of communication mechanism employed will vary. A network is referred to as leased line network when two or more computers are connected by independent dedicated data lines. Dial-up networks, which connect computers via regular phone lines, are another option. Other methods of establishing connectivity include satellite connections and microwave links. In a single network, all of these techniques may possibly be combined. Broadband transmission is possible using microwave technology. In a microwave system, signals are sent straight from a dish antenna to a receiving dish antenna at the next microwave station, which is situated no more than 25 miles distant in a direct line of sight. The data signals may be captured and 'boosted' by each relay station before being sent to other receiving stations.

An alternative to conventional telecommunications is a satellite communications network. Information such as text, data, speech, and video is transformed into radio waves at Earth stations and sent to a satellite via a broadband transmission channel. The satellite sends the information back across the nation or the globe to an Earth station or an antenna atop a tall structure at the receiving point. It only takes a few milliseconds for transmission. To guarantee data transmission and reception, any computer linked to a wide area network (WAN) needs access to a modem, a communications connection, and communication software. A choice of communications medium might be made based on the geographical location of the computers being linked. It makes sense that a modem is required at both ends of any telephone connection connecting two computers. At the sending end, these modems transform digital signals from the computer into analog signals, and at the receiving end, they reverse the conversion from analog to digital signals. All things considered, 5G promises to open up a plethora of new use

cases and enhance mobile network performance across a broad range of applications. While carriers have continued to roll out 5G, many businesses that had planned to move to 5G have opted to stick with 4G/LTE.

Unexpected and growing healthcare expenses put strain on government initiatives like telematics-based 5G smart city programs. All of the physical parts of the computer that store and execute the code included in the software are collectively referred to as hardware. This suggests that the term "hardware" refers to any component of a computer that is visible. Hardware includes the Motherboard, CPU, and screen. Software is the term used to describe the collection of programs and instructions that manage a computer's operations and allow it to carry out certain tasks. The phrases "software," "applications," and "scripts" are interchangeable when referring to the many kinds of computer code that may be loaded and executed on a computer or other electronic device. Hardware and software are used in the banking sector to support a range of functions, including Data and instructions for the computer's Central Processing Unit (CPU) to access are stored in computer memory, often referred to as computer RAM (Random Access Memory). A computer with greater memory is able to process and store more instructions at once. Since memory is volatile, it gets erased when the machine is turned off.

A computer loads the required information and instructions into memory when it launches an application or opens a file, enabling the CPU to access them fast. As a result, the CPU can work on tasks and processes more quickly since it is not continuously accessed by slower storage devices like solid-state or hard disks. A computer's or other electronic device's "brain" is the processor, also referred to as the central processing unit. It carries out the mathematical computations and instruction execution necessary for the gadget to work. Millions of small electrical switches, often known as transistors, make up a processor. These transistors may be switched on or off to represent binary data (0 or 1) and carry out operations. The clock speed of the CPU, expressed in gigahertz (GHz), dictates how many instructions it can perform in a second. There are many various kinds of processors; the most popular ones are made by Apple, AMD, Intel, ARM, and Qualcomm.

The performance of the device is also impacted by its particular architecture, which might include different core and thread counts and be x86, x64, ARM, etc. Machine code and programming languages are not the same thing. Only after it has been translated can the processor comprehend the software code. To interpret the program's instructions as needed, an "interpreter" is required.

A program created in a high-level programming language (such as Python or C++) is translated into machine code that a computer can comprehend and run by compiler software, also known as an interpreter or compiler. But they approach it in different ways. A compiler is a kind of software that instantly translates computer code into machine code, producing an executable file. After reading the whole program and making sure there are no mistakes, the compiler generates machine code that the computer can run. This makes the software run more quickly, but it requires more time to build and test. Compilers are used by the programming languages C, C++, and C#. Certain languages may be compiled and interpreted on their own, or with the assistance of certain frameworks and libraries. Some languages, such as Java, which can be read by the JVM (Java Virtual Machine) but requires a just-in-time compiler to convert byte code into machine code before it can be executed, combine the two approaches.

Hardware and other system resources are managed and controlled by system software on computers. The programs that control the system, including the operating system, file management tools, and the disk operating system (also known as DOS), are included in system

software. Function libraries, system services, printer and other device drivers, system preferences, and further configuration files are among the files that make up the system. Assemblers, compilers, file management tools, system utilities, and debuggers are examples of system software programs. On a gadget, such a computer, smartphone, or network, firmware comes pre-installed and controls 3.5 of its fundamental operations. It serves as a conduit for data between the operating system and hardware of the device, allowing lower-level software and hardware to interact.

The function of firmware is to regulate a device's low-level functions, including memory management, input/output control, and power management. It is in charge of setting up the hardware components of the device and maintaining a stable operating system environment. The firmware also gives the gadget its fundamental functions and gives it the ability to carry out certain tasks. Non-volatile memory, such ROM, flash memory, or EEPROM, is where firmware is often kept, enabling it to be kept even after the device is turned off. This enables the gadget to keep its setup and settings even after a reboot or power loss. Software that is made accessible to the public for free is known as freeware. It is free for users to download, use, and share the program. Freeware software authors usually do not charge for their creations, although they may still be entitled to certain rights including copyright. Certain freeware programs are open-source, meaning that anybody may alter and share the program's source code because it is made publicly accessible.

The fact that freeware is often accessible to everyone and is free of cost is one of its primary advantages. For those who cannot afford pricey commercial software, this may be helpful. Furthermore, a lot of freeware apps contain capabilities that are comparable to those of their paid versions, and some of them may even be used in place of paid software.

Nevertheless, there are drawbacks to utilizing freeware, such as the possibility that some of it contains malware such as spyware or adware that might steal personal data. In addition, it is difficult to get technical help for issues with Freeware since it is not commercially sponsored. Shareware is usually offered as a trial version so that consumers may test the program before deciding to purchase it. Shareware, in contrast to Freeware, is not free to use; instead, it is often offered at a discounted price or with restricted features, with the expectation that the user would pay to register and get the full version if they find the program to be helpful. Shareware is a kind of commercial software distribution in which the software provider grants customers access to the program for a constrained amount of time or with a restricted feature set. This enables the user to assess the program before deciding whether to buy it. A demo or trial version, which may have certain functionality disabled or expire after a set number of days, is often used to distribute shareware.

To use the full version of the program after that, the user must buy a license. The ability to test software before committing to a purchase is one of the primary advantages of shareware, since it enables consumers to make better informed judgments about whether or not to buy the program. Because consumers are often ready to share the program with others, shareware is also a useful strategy for software providers to promote their product and increase visibility. there are drawbacks to adopting shareware. For instance, shareware may include more problems or mistakes than commercial software since it is often offered as a trial version. Let's say, therefore, that a user wishes to keep using the program after the trial term has expired. In such scenario, they will have to pay a hefty fee for a license. A "programming language" is a language intended to specify a series of A formal language made up of a collection of instructions that may be used to write software is called a programming language. It enables programmers to convey their concepts in a form that a machine can comprehend and use. Database management, robot control, user interface creation, and many more jobs may be

created using programs written in programming languages. Specific syntax and grammar rules are employed in programming languages to produce code, which is then used to teach computers. The computer can comprehend and carry out these commands because they are converted into machine code.

Apple created Swift, a general-purpose compiled programming language. Applications for iOS, iPadOS, macOS, watchOS, and tvOS are often developed using it. Every language has advantages and disadvantages, and the choice of language is often based on the particular project or application. The benefits of a programming language are many. Compared to machine code, it is considerably easier to comprehend and provides for more portability that is, it can be readily modified to operate on a variety of computer types. This is the exact reason a bank is established, mostly because the banking sector is dominated by the services sector. In this sense, digital banking primarily focuses on offering a smooth, enjoyable client experience. A digital bank is required to use holistic CRM (which includes operational, analytical, and collaborative CRM) in order to achieve this. Based on a comprehensive knowledge of the client, customer-centric business models are used to develop a strong digital interaction that ultimately results in highly customized, collaboratively generated goods and services that make use of data and analytics.

CONCLUSION

Network operating systems, or NOS, are critical components of digital banking systems' security and effectiveness because they manage network resources and guarantee dependable, effective operations.

The foundation required for digital payment systems, online and mobile banking, and core banking applications is provided by NOS like UNIX, Linux, and Windows Server. They are essential for addressing the needs of contemporary banking because of their capacity to efficiently manage network traffic, balance loads, and distribute resources, all of which lead to excellent service availability and performance. Furthermore, NOS improve security by putting in place access restrictions, keeping an eye out for dangers, and fending off cyberattacks all of which are essential for securing sensitive financial data. Nevertheless, there are drawbacks to NOS integration in digital banking, such as the need for constant upkeep, upgrades, and interoperability with emerging technologies. In order to maintain the resilience and adaptability of their NOS infrastructure, banks need to consistently tackle these difficulties. The role of NOS in sustaining operational resilience and fostering new technologies will grow in importance as digital banking develops. In order for banks to provide safe, effective, and scalable digital services while negotiating the challenges of a rapidly evolving technology landscape, the effective management of NOS will be essential.

REFERENCES:

[1] O. Bayram, “Importance of Blockchain Use in Cross-Border Payments and Evaluation of the Progress in this Area,” *Doğuş Üniversitesi Derg.*, 2020, doi: 10.31671/dogus.2020.444.

[2] N. Anand and A. Kumar, “Efficiency mapping of private banks in India through II-stage network DEA efficiency scores,” *Int. J. Sci. Technol. Res.*, 2020.

[3] I. Aldasoro, C. Cabanilla, P. Disyatat, T. Ehlers, P. McGuire, and G. von Peter, “Central bank swap lines and cross- border bank flows,” *BIS Bull.*, 2020.

[4] B. S. Bhati and C. S. Rai, “Analysis of Support Vector Machine-based Intrusion Detection Techniques,” *Arab. J. Sci. Eng.*, 2020, doi: 10.1007/s13369-019-03970-z.

[5] N. Al-Milli and B. H. Hammo, "A Convolutional Neural Network Model to Detect Illegitimate URLs," in *2020 11th International Conference on Information and Communication Systems, ICICS 2020*, 2020. doi: 10.1109/ICICS49469.2020.239536.

[6] K. Ullah *et al.*, "Financial Reporting in the Oil and Gas Industry," *Rev. Account. Stud.*, 2020.

[7] B. R. Gaines, "From facilitating interactivity to managing hyperconnectivity: 50 years of human–computer studies," *Int. J. Hum. Comput. Stud.*, 2019, doi: 10.1016/j.ijhcs. 2019.05.007.

[8] K. Siva Nageswararao, M. Venkataramanaiah, and C. M. Latha, "Performance analysis of s&p bse bankex public sector banks," *J. Adv. Res. Dyn. Control Syst.*, 2019.

[9] D. N. K. J. Arachchilage, F. Jameel, and M. Qaraqe, "Secure RF Energy Harvesting Scheme for Future Wireless Networks," 2019. doi: 10.5339/qfarc.2018.ictpp179.

[10] S. Oduro, "Examining open Innovation practices in low-tech SMEs," *J. Bus. Res.*, 2019.

CHAPTER 7

INVESTIGATION OF THE CONCEPT AND SIGNIFICANCE OF DIGITAL BANKING ECOSYSTEM

Dr. Malcolm Homavazir, Associate Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- Malcolm.homavazir@atlasuniversity.edu.in

ABSTRACT:

The advent of fintech innovations and the integration of sophisticated technology have led to a revolutionary change in the financial services sector, which is reflected in the digital banking ecosystem. The notion and importance of the digital banking ecosystem are examined in this research, with a particular emphasis on its constituent parts traditional banks, fintech firms, authorities, and technology infrastructure. The study emphasizes how these components work together to provide a dynamic environment that improves customer satisfaction, financial inclusion, and operational effectiveness. The report examines the competitive and cooperative dynamics that exist between fintech companies and conventional banks, shedding light on how the digital banking ecosystem promotes innovation, propels digital transformation, and reimagines the financial services landscape. The results highlight how crucial technology developments, regulatory frameworks, and strategic alliances are to creating a flexible and resilient digital banking environment.

KEYWORDS:

Collaboration, Digital Banking, Ecosystem, Fintech, Innovation.

INTRODUCTION

The financial services sector has seen a paradigm change with the advent of digital banking ecosystem, which is defined by the incorporation of cutting-edge technologies that have revolutionized conventional banking operations into a model that is more customer-centric, accessible, and efficient. Digital banking refers to a broad variety of platforms and services that let companies and people use technology to manage accounts, carry out financial transactions, and get banking services often without having to visit physical branches. The contemporary banking experience is defined by the emergence of digital payment methods, mobile banking applications, and internet banking, which are the result of shifting consumer habits and technological advancements [1], [2]. Digital banking encompasses a wide range of services, from simple operations like moving money and checking account balances to more intricate ones like loan applications, investment management, and even cryptocurrency transactions. Digital banking encompasses more than just providing online banking services. It also entails fully digitizing all banking procedures so that clients may get services around the clock from any location in the globe [3], [4]. This is now feasible because of the widespread use of technologies like big data analytics, blockchain, cloud computing, and artificial intelligence, which allow banks to provide their clients with individualized, real-time services.

When banks first started providing basic internet services in the late 20th century, online banking took off and has since evolved from conventional to digital banking. Online banking was first restricted to basic functions like checking account balances and making money transfers between accounts. However, as more people used the internet and technology developed, more services were available, which prompted the creation of more complex online banking systems. The emergence of mobile banking during the early 21st century was a noteworthy turning point in this progression because smartphones were widely used and

enabled users to do financial transactions while on the move using mobile applications [5], [6]. Since then, mobile banking applications have developed to include a broad range of features, such as peer-to-peer payments, mobile check deposits, and individualized financial management tools that meet each user's unique requirements. These developments have improved consumer involvement as well as convenience since banks can now communicate with their clients via a variety of digital platforms, offering a streamlined and integrated banking experience.

New actors in the financial services sector have also emerged as a result of the growth of digital banking, including fintech firms that focus on offering digital financial services. These businesses use technology to provide cutting-edge goods and services, often more affordably and flexibly than conventional banks. Neobanks, or digital-only banks, provide consumers with a digital banking experience by operating only online and without any physical branches. These neobanks have become more well-known because of their simple onboarding procedures, inexpensive fees, and intuitive user interfaces. Fintech businesses have also brought in novel solutions like peer-to-peer lending platforms that link lenders and borrowers directly, doing away with conventional middlemen, and robo-advisors that utilize algorithms to give automated investing advice. The emergence of these new competitors has increased rivalry in the banking sector, forcing established institutions to step up their digital transformation initiatives to stay competitive.

Customers' growing expectations for quick, easy, and individualized financial services are one of the main factors driving the transition from conventional to digital banking. As a result, banks have shifted to a customer-centric strategy and started using data analytics to understand the preferences and behavior of their clients. This has made it possible for them to provide individualized goods and services that cater to the unique requirements of each client. Predictive analytics, for instance, enables banks to provide customized investment portfolios or pre-approved loans to customers based on their anticipated requirements [7], [8]. Digital banking has also made it possible for banks to improve client engagement by providing tailored and interactive experiences via digital channels like social media and mobile applications. This has raised customer loyalty as well as satisfaction since satisfied clients are more inclined to stick with a bank that provides them with a convenient and customized banking experience.

The ecology of digital banking is also defined by the growing significance of security and regulatory adherence. Banks must handle related risks, such as cybersecurity attacks and data breaches, as they use digital technology. Preserving sensitive financial data and upholding consumer confidence depend heavily on digital banking systems' security. To protect client data and stop illegal access, banks have put in place several security measures, such as encryption, multi-factor authentication, and biometric verification. Apart from addressing security issues, banks also need to adhere to regulatory mandates that differ geographically and may be rather complex and rigorous [9], [10]. To guarantee that digital banking services are offered in a safe and compliant way, regulatory agencies like the European Central Bank (ECB) and the Reserve Bank of India (RBI) have set rules and regulations. These rules address Know Your Customer (KYC) standards, data protection, and anti-money laundering (AML) measures, among other elements of digital banking. For banks to function lawfully and stay out of trouble, they must adhere to certain requirements.

Technological developments, notably in the fields of big data analytics, blockchain, and artificial intelligence (AI), have propelled the development of digital banking. AI has made it possible for banks to automate several tasks, including fraud detection, credit scoring, and customer support, which has improved productivity and decreased operating expenses. For instance, banks today often deploy AI-powered chatbots to provide immediate customer help,

responding to questions and resolving problems without the need for human participation. In a similar vein, AI-powered fraud detection systems can instantly examine vast amounts of transaction data to spot unusual behavior and stop fraudulent transactions. On the other hand, blockchain technology offers a transparent and safe means of recording transactions, which has the potential to completely transform the financial sector. Because blockchain technology is decentralized, transaction records are impenetrable, lowering the possibility of fraud and boosting confidence in the financial system. Furthermore, since blockchain decreases transaction processing times and does away with the need for middlemen, it may enable cross-border payments that are quicker and less expensive. Another technological advancement that has significantly impacted digital banking is big data analytics, which allows banks to examine enormous volumes of data to get insights into consumer behavior, industry trends, and operational efficiency. This has made it possible for banks to streamline their operations, make data-driven choices, and provide clients with more individualized goods and services.

DISCUSSION

The internal workings of banks have also changed as a result of the transition to digital banking. To adapt to the digital age, traditional banks have had to make considerable organizational and cultural adjustments. Rethinking their business models, reorganizing their operations, and taking a more flexible stance on innovation have all been necessary to achieve this. A lot of banks have set up teams specifically for digital transformation, to foster innovation and make sure the bank stays competitive in the quickly changing financial market. These groups often collaborate with fintech businesses, taking use of their knowledge to create and execute fresh approaches to digital banking. Furthermore, banks are putting the needs of their clients first and emphasizing providing value to them via digital channels. This has necessitated a change in the corporate culture, with banks now emphasizing innovation, continuous improvement, and the client experience more.

The importance of alliances and teamwork in the digital banking environment cannot be overstated. Banks have been forming strategic alliances with fintech startups, technology providers, and other financial institutions more and more to remain competitive in the digital era. Through these alliances, banks may better serve their customers, increase operational efficiency, and create cutting-edge goods and services by using the resources and knowledge of their partners. Peer-to-peer payment platforms and mobile wallets are two examples of the digital payment solutions that many banks have collaborated with fintech startups to provide. In a similar vein, banks have worked with IT companies to put cutting-edge cybersecurity protections in place, guaranteeing the security of their online banking systems. These alliances are advantageous to both parties as they provide fintech firms access to the resources and clientele of well-established banks, while banks can take advantage of the fintech businesses' creativity and adaptability.

Financial inclusion has been greatly impacted by the use of digital banking, especially in developing nations. Accessing financial services has become simpler for those living in distant and underserved locations thanks to digital banking systems, often for the first time. In this sense, mobile banking in particular has been very important as it enables people to do financial transactions using their phones instead of going via a real bank branch. Millions of individuals now have access to crucial financial services as a result of this helping to close the gap between the unbanked and the established financial system. Digital banking has not only made banking services more accessible, but it has also empowered people by giving them more financial autonomy. For instance, financial management capabilities are often included in digital banking systems, enabling users to better monitor their spending, create budgets, and save money. This has aided in fostering responsible financial behavior and raising financial literacy,

especially among younger generations. Another feature of the digital banking environment is the increasing significance of consumer data. Given its ability to give banks insights into the behavior, tastes, and demands of their customers, data has emerged as one of their most significant assets in the digital era. Data analytics is being used by banks more and more to understand their clients better and provide more individualized goods and services. For instance, banks may determine patterns and trends in transaction data that point to a customer's financial need and provide customized solutions, such as investment advice or individualized savings strategies. Furthermore, banks may use data analytics to target certain consumer demographics with tailored marketing efforts, like millennials or small business owners. Concerns about data security and privacy are also brought up by the expanding usage of client data. To prevent data breaches, banks must make sure that they manage consumer data responsibly, following all legal obligations and putting strong security measures in place.

Traditional banks, which have historically been distinguished by their physical branches, are undergoing a dramatic shift as they shift to digital platforms due to the quickening pace of technological innovation and the changing needs of their clientele. This change represents a significant departure from the traditional banking paradigm, which mostly depended on face-to-face communication, paper-based procedures, and a permanent infrastructure. In the past, banking services were provided via a chain of physical branches that clients would visit to complete a variety of tasks including making deposits or withdrawals, submitting loan applications, or getting financial advice. Customers have to follow branch hours and overcome bureaucratic procedures, which may be time-consuming processes. However, the emergence of digital technology has completely changed this environment, forcing established banks to adopt digital platforms to boost client satisfaction, increase operational effectiveness, and maintain their competitiveness in a world that is becoming more and more digital.

The shift to digital platforms includes the digitalization of essential banking functions, enabling clients to use online and mobile banking platforms for account access, financial transfers, bill payment, and investment management. This change has been mostly fueled by the increasing use of smartphones, the expansion of internet connectivity, and the need for more adaptable and convenient banking options. When rudimentary online services were introduced in the late 20th century, users could use their computers to check their account balances and conduct simple transactions. This marked the beginning of the development of online banking. These services developed to provide a wider variety of features, including financial transfers, account management, and bill payment, as technology and internet access increased. This shift was further expedited by the emergence of mobile banking applications, which allowed users to transact banking straight from their smartphones or tablets while they were out and about. Digital banking systems now provide a full range of services to meet a variety of financial demands, from simple transactions to sophisticated financial planning and investment management.

Traditional banks have several difficulties in the digital era, even with the notable advancements in the use of digital platforms. Modernizing legacy IT systems, many of which were constructed decades ago and are ill-suited to the needs of a digitally-first banking environment, is one of the main issues. The foundation of many conventional banks is these legacy systems, which are often expensive to operate, complicated, and rigid. The difficult process of upgrading or replacing ancient systems with contemporary, cloud-based infrastructure calls for significant financial outlay and meticulous planning. In addition, cautious management of the shift from traditional to digital platforms is necessary to prevent interruptions in financial services and guarantee the protection of private client information.

The growing rivalry between fintech firms and digital-only banks, or neobanks, is another big issue facing conventional banks. These recent arrivals in the financial services sector have benefited from their adaptability, cutting-edge technology, and customer-focused mindset to deliver banking services that are often quicker, less expensive, and more convenient than those offered by established banks. Neobanks, for instance, usually do not have physical branches, which enables them to save expenses and provide consumers with reduced rates. Peer-to-peer lending platforms, robo-advisors, and mobile payment solutions are just a few of the cutting-edge goods and services that fintech businesses have launched. These products and services are drawing in an increasing number of clients, especially among younger, tech-savvy consumers. Traditional banks need to reevaluate their business models and take a more customer-centric stance in addition to investing in digital technologies if they want to stay competitive in this quickly evolving market.

Another significant obstacle that conventional banks must overcome as they move to digital platforms is cybersecurity. The growing dependence of banks on digital technology has increased their susceptibility to cyber risks, including but not limited to hacking, data breaches, and online fraud. Preserving sensitive financial data and upholding consumer confidence depend heavily on digital banking systems' security. To protect themselves from these attacks, traditional institutions must invest in cutting-edge cybersecurity techniques like encryption, multi-factor authentication, and ongoing network activity monitoring. Furthermore, banks have to abide by an increasing amount of regionally specific, complicated, and strict regulations about cybersecurity and data protection. Serious fines and harm to one's reputation may arise from breaking these rules.

In the digital era, data privacy is a major problem for conventional banks and is directly linked to cybersecurity. Banks must make sure that the massive volumes of consumer data they gather and handle including financial and personal information—are managed sensibly and following applicable data protection regulations. The European Union's General Data Protection Regulation (GDPR) and other recent rules have raised the bar for data privacy standards, necessitating that banks establish stringent controls over the collection, storage, and use of consumer data. Conventional banks have to deal with client concerns about data privacy in addition to navigating these legislative obstacles as people become more conscious of the dangers of disclosing personal information online.

Despite these obstacles, conventional banks stand to gain greatly from the shift to digital channels. Enhancing the client experience via digital media is one of the biggest possibilities. Banks may provide easy, individualized services that are tailored to each customer's unique requirements and preferences by using digital technologies. Banks, for instance, may utilize data analytics to learn more about the behavior of their customers and provide customized financial solutions, such as pre-approved loan offers, personalized savings programs, and investment advice. Digital banking systems facilitate banks' provision of real-time services, allowing consumers rapid access to their accounts, money transfers, and payment processing from any location in the globe. Customer loyalty and happiness may be greatly increased with this degree of customization and convenience.

The capacity to automate processes and save expenses via digitization and streamlining presents conventional banks with additional opportunities in the digital age. Financial institutions may enhance their operational efficiency and minimize the need for human intervention by automating repetitive processes including transaction processing, account administration, and customer support. This decreases operating expenses while also lowering the possibility of mistakes and enhancing the accuracy and speed of financial services. To manage consumer queries, for instance, some banks have deployed AI-powered chatbots.

These chatbots provide prompt answers to frequently asked issues, freeing up human agents to concentrate on more intricate duties. Comparably, digital platforms let banks automate compliance procedures like anti-money laundering (AML) and Know Your Customer (KYC) checks, which lessens the risk of non-compliance and eases the cost of regulatory compliance.

Traditional banks may also benefit from the digital era by reaching new markets and growing their client base. Without having to open physical offices, digital banking systems have made it simpler for banks to provide their services to clients in rural or underserved regions. This has created new avenues for financial inclusion, especially in underdeveloped nations where there has historically been restricted access to banking services. In this sense, mobile banking in particular has been quite helpful, enabling people in remote locations to use their phones to access financial services. Traditional banks may reach a wider audience and open up new income streams by using digital technologies.

Conventional banks are now able to support innovation and create new goods and services that cater to the changing demands of their clientele thanks to the shift to digital platforms. For instance, the advent of open banking, fueled by legislative modifications like the European Union's Revised Payment Services Directive (PSD2), has given banks more chances to work with fintech firms and outside suppliers. Customers who use open banking may access a greater variety of financial goods and services by sharing their financial information with approved third parties. As a result, new solutions have been created, like account aggregation platforms that let users manage numerous bank accounts in one location and personalized financial management tools that offer recommendations based on the spending patterns and financial objectives of the user. Traditional banks may be at the forefront of innovation and provide their consumers with more options by adopting open banking.

In addition, the digital era gives conventional banks a chance to improve their sustainability initiatives and help create a more sustainable future. By eliminating paper-based procedures and lowering the energy used in physical branches, digital banking platforms may lessen the environmental effect of banking operations. For instance, digital banking eliminates the need for paper checks, statements, and other paperwork, saving trees and lowering the carbon footprint of printing and distributing these materials. Digital platforms also allow banks to provide eco-friendly solutions like digital investment alternatives and paperless loans that promote socially and ecologically conscious enterprises. Traditional banks may lessen their environmental effect and attract consumers who value sustainability while making financial choices by incorporating sustainability into their digital initiatives.

The explosive growth of financial technology, or fintech, has caused a seismic upheaval in the financial environment in recent years. As key participants in the financial ecosystem, fintech businesses are driving innovation that both challenges and enhances conventional banking practices. Their impact extends to a broad range of services, including loans, payments, insurance, and wealth management, and it has a profound impact on how companies and consumers engage with financial institutions. Fintech's capacity to use cutting-edge technology like blockchain, big data analytics, cloud computing, and artificial intelligence is at the core of its innovative function. Compared to their conventional competitors, fintech companies can now provide more individualized, effective, and easily accessible financial services because of this technology. Peer-to-peer lending sites, such as Lending Club and Prosper, for example, use advanced algorithms to connect lenders with borrowers instead of conventional credit evaluations, which saves time and money on loan approvals. In a similar vein, robo-advisors such as Wealth-front and Betterment use machine learning to provide automated and customized investing advice, opening up wealth management a formerly specialized field for high-net-worth individuals to a wider audience.

The customer experience has been greatly improved by fintech advancements by emphasizing user-friendly interfaces and frictionless digital interactions. Fintech has made financial transactions faster and easier. Examples of this include digital wallets, contactless payment methods, and mobile banking applications.

By offering scalable, simple-to-integrate payment processing solutions to companies of all sizes, companies like Square and Stripe have completely changed the payment environment, promoting greater financial inclusion and empowering small businesses to compete in the digital economy. blockchain technology which is supported by fintech companies like Chainalysis and Ripple has brought previously unheard-of levels of security and transparency to financial transactions, with the potential to lower fraud and expedite cross-border payments. These innovations provide new income streams and business models that were previously unreachable inside the inflexible frameworks of conventional banking, in addition to increasing operational efficiency.

The competitive dynamics between fintech startups and conventional banks have significantly changed as a result of the fintech industry's fast developments. Although fintech companies were once seen as disruptors that threatened traditional banks' hegemony, the connection between them has developed into a more complex dynamic of cooperation and rivalry. Fintech businesses compete with conventional banks on the one hand by providing better customer service, more affordable fees, and cutting-edge goods that appeal to younger, tech-savvy consumers. Fintech companies' agility and flexibility enable them to quickly adjust to shifting market conditions and technology developments, often surpassing the slower, more bureaucratic procedures that come with big banks. To maintain their market share, conventional banks have been compelled by this rivalry to step up their own digital transformation initiatives. They have upgraded their web and mobile platforms, invested in new technology, and embraced customer-centric strategies.

CONCLUSION

The examination of the digital banking ecosystem emphasizes how crucial a role it has played in transforming the financial services sector. The interaction of fintech businesses, conventional banks, regulators, and technology infrastructure has created an ecosystem that has greatly improved financial services' efficiency, accessibility, and customization. The research indicates that the digital banking environment promotes cooperation as well as competition, allowing fintech companies and conventional banks to capitalize on their unique advantages. To drive innovation and guarantee the smooth integration of cutting-edge technologies like big data analytics, blockchain, and artificial intelligence (AI) into financial services, cooperation is essential. Furthermore, the study emphasizes how crucial regulatory frameworks are to preserving the ecosystem's security and stability as well as fostering innovation and consumer protection. The results highlight the need for constant adaptation and strategic alliances as the digital banking environment changes further to take advantage of the possibilities and difficulties brought about by quick technical progress. In the end, the financial services industry is about to transform thanks to the digital banking ecosystem, which will provide a more accessible, effective, and customer-focused banking experience.

REFERENCES:

[1] N. Gupta and D. Jhamb, “How india can develop its payments fraud prevention model: A study of emerging best practices,” *J. Payments Strateg. Syst.*, 2020.

[2] V. Lizovskaya, I. Salikhova, and E. Khalina, “Marketing in Banking Sector and Digital Ecosystems,” 2020. doi: 10.2991/aebmr.k.200324.146.

[3] Y. G. Shvetsov, "Genesis of the Digital Bank," *Vestn. NSUEM*, 2020, doi: 10.34020/2073-6495-2020-1-076-090.

[4] P. M. Rubanov, "Transformation of the Banking Sector in the Digital Era," *Mech. an Econ. Regul.*, 2020, doi: 10.21272/mer.2019.86.11.

[5] A. Gandolfo, "Content shared between banks and users on the social ecosystem: an inductive exploratory inquiry," *Electron. Commer. Res.*, 2020, doi: 10.1007/s10660-019-09340-z.

[6] J. Gorzala, "PayTechs im Open Banking," *Zeitschrift für das gesamte Bank- und Börsenwes.*, 2020, doi: 10.47782/oeba202001004601.

[7] P. K. Singh and A. Dutta, "Socio-metrics of digital payments in demographic dividend: Descriptive analysis of dichotomous preferences," *Applied Innovative Research (AIR)*. 2020.

[8] D. W. Arner, D. A. Zetzsche, R. P. Buckley, and R. H. Weber, "The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II.," *Stanford J. Law, Bus. Financ.*, 2020.

[9] P. Dintrans, A. Anand, M. Ponnuveetil, A. Acharya, A. Chardukian, and C. Technology Solutions, "How Banking as a Service Will Keep Banks Digitally Relevant and Growing," 2020.

[10] K. Ullah *et al.*, "Financial Reporting in the Oil and Gas Industry," *Rev. Account. Stud.*, 2020.

CHAPTER 8

ANALYSIS OF TECHNOLOGICAL FOUNDATIONS IN DIGITAL BANKING

Parag Amin, Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- parag.amin@atlasuniversity.edu.in

ABSTRACT:

Digital banking is built on a variety of technical advancements that have completely changed the financial services industry by improving client satisfaction and operational effectiveness. Online banking platforms that make use of web technologies to provide easily available financial services are examples of core technologies, as are Core Banking Systems (CBS), which serve as the foundation for account administration and transaction processing. Through the use of mobile development frameworks and APIs, mobile banking brings these services to smartphones with improved functionality and security. Blockchain technology offers decentralized and secure transaction recording, while cloud computing affords scalable and adaptable IT infrastructure. In customer service and risk management, artificial intelligence (AI) and machine learning (ML) are essential. While chatbots and virtual assistants improve client interactions, ML algorithms improve fraud detection and predictive analytics. Operational insights and tailored financial services are further enhanced by big data analytics. Together, these technologies handle the benefits and difficulties that come with living in the digital era and help to form a financial environment that is more efficient, safe, and focused on the needs of the client.

KEYWORDS:

Artificial Intelligence (AI), Blockchain, Cloud Computing, Core Banking Systems (CBS), Machine Learning (ML).

INTRODUCTION

The technical underpinnings of digital banking are an amalgam of many cutting-edge technologies that have completely changed the financial services sector and the way banks function and engage with their clientele. The integration of information technology systems that enable scalable, safe, and effective financial operations is the foundation of digital banking. Core banking systems (CBS), which replaced manual procedures with automated ones to manage account information and financial transactions, marked the beginning of this change. Many digital banking services rely on CBS as its backbone since it allows for real-time transaction processing and cross-channel access to consumer data [1], [2]. Relational databases, which handle and store vast amounts of financial data, and middleware, which unifies different services and apps within the banking ecosystem, are the foundations upon which these systems are constructed.

The introduction of the internet and the growth of online banking platforms expedited the development of digital banking even further. Through safe online portals, online banking systems provide users access to their accounts by using web technology. These platforms are designed with a responsive and user-friendly interface thanks to the integration of client-side technologies like HTML, CSS, and JavaScript with server-side technologies like PHP, Java, .NET, and PHP. To protect sensitive information from unwanted access, the bank uses Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols to encrypt data being sent between its servers and clients' devices.

The growing popularity of smartphones led to the emergence of mobile banking, which further broadened the range of digital banking services. From simple transactions to sophisticated financial management tools, mobile banking applications are designed to provide a variety of features that customers may access via their mobile devices [3], [4]. These applications are created with the aid of mobile development frameworks, including Kotlin for Android and Swift for iOS, and they are integrated with application programming interfaces (APIs) that facilitate communication between the bank's backend systems and the mobile application. Features like push notifications, biometric authentication, and geolocation services may improve the security and usability of mobile banking applications.

Technological developments in cloud computing have also contributed to the growth of digital banking by enabling banks to extend their infrastructure and services effectively. By allowing banks to install and manage their data and apps on a scalable infrastructure, cloud computing eliminates the need for expensive on-premises hardware and speeds up the rollout of new services. Banks may improve their digital capabilities by using a variety of solutions provided by cloud service providers, such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Utilizing cloud computing also makes data processing and storage easier, allowing banks to manage high transaction volumes and consumer data availability and dependability.

With its decentralized and secure transaction recording mechanism, blockchain technology has become a major revolution in digital banking. The distributed ledger technology of blockchain makes sure that every member of the network has an identical picture of the transaction history, which lowers the possibility of fraud and increases transparency. Smart contracts further improve the efficiency of financial operations by enabling automated and trustless transactions [5], [6]. Smart contracts are self-executing contracts that have the conditions of the agreement directly encoded into code. Banks are investigating the potential of blockchain technology for a range of purposes, such as identity verification, trade financing, and international payments.

Digital banking now relies heavily on artificial intelligence (AI) and machine learning (ML), which are driving advancements in fields like fraud detection, customized financial advising, and customer care. Chatbots and virtual assistants driven by artificial intelligence (AI) provide consumers real-time help and support by managing standard queries and transactions without requiring human participation. Large volumes of transaction data are analyzed by machine learning algorithms to find trends and abnormalities, which helps banks discover and stop fraud in real time. Personalized financial insights and suggestions are another benefit of AI-driven analytics solutions, which assist users in making wise choices about their spending, savings, and investments.

Big data analytics is essential to digital banking because it allows banks to make use of the enormous volumes of data produced by many types of digital transactions. To get insights into consumer behavior, tastes, and trends, data analytics technologies process and analyze client data. This enables banks to provide tailored goods and services. By using predictive analytics, for instance, banks may proactively provide pertinent solutions, like customized loan offers or investment possibilities, by anticipating consumer wants and behaviors. Big data and sophisticated analytics technologies together improve banks' understanding of and capacity to predict client demands, resulting in more effective and efficient financial services.

In the context of digital banking, cybersecurity is crucial as banks are more vulnerable to data breaches and cyberattacks. Banks use various security measures, such as intrusion detection systems, encryption, and multi-factor authentication (MFA), to safeguard confidential financial data and uphold client confidence [7], [8]. MFA adds an extra degree of protection by requiring

users to give many kinds of authentication before being able to access their accounts. Data exchanged between consumers and banks is safe and impenetrable to nefarious actors thanks to encryption. By keeping an eye out for unusual activity on a network, intrusion detection systems may warn banks of possible security risks before they can do a lot of harm.

Another crucial component of digital banking is regulatory compliance, as banks have to go by a wide range of intricate rules and guidelines about cybersecurity, financial transactions, and data protection. Strict guidelines for data security, client permission, and transparency are required by laws like the General Data security Regulation (GDPR) and the Payment Services Directive 2 (PSD2). For banks to stay out of trouble and keep their regulatory approval, they need to have strong [9], [10]. Compliance plans and systems in place. Banks may better handle the increasing complexity of regulatory requirements by integrating regulatory technology (RegTech) solutions, which leverage automation and artificial intelligence (AI) to expedite compliance operations.

DISCUSSION

Open banking, an idea that encourages banks and third-party suppliers to share financial data via APIs, has also grown as a result of digital banking. By enabling outside developers to provide fresh financial services and products that interface with bank systems, open banking promotes innovation. Customers have more options and competition because of this ecosystem, which makes a greater variety of financial services available from different suppliers. By using these alliances, banks that support open banking may provide their clients with more complete and integrated solutions, thereby improving their value offerings. Consumer expectations and behavior have significantly changed as a result of the banking industry's use of digital technology. Consumers today expect accessible, customized, and smooth banking experiences, so banks must constantly develop and modify their digital services. Banks have had to reconsider their branch strategy in light of the trend toward digital-first engagements. They now prioritize digital channels while maximizing the use of physical branches for customer service and relationship management.

The foundation of contemporary financial services is formed by core technologies in digital banking, which allow banks to provide their clients with innovative, safe, and effective services. The Core Banking System (CBS), which provides the essential framework for handling and processing financial transactions, is at the center of these technologies. Real-time transaction processing, including loan administration, transfers, withdrawals, and deposits, is made easier by CBS. It is based on a strong IT foundation that incorporates middleware to connect different banking apps and services and relational databases to manage massive amounts of transaction data. Regardless of where consumers access their accounts, this system guarantees smooth functioning across several branches and channels, giving them access to the most recent information and consistent service.

The introduction of online banking as a key technical innovation with the development of the internet has greatly influenced the progress of digital banking. Through safe online portals, online banking platforms provide banking services by utilizing web technology. These platforms are built using client-side technologies like HTML, CSS, and JavaScript that provide an interactive and user-friendly interface, and server-side technologies like Java,.NET, and PHP that manage backend activities. Online banking requires security protocols like Secure Socket Layer (SSL) and Transport Layer Security (TLS), which encrypt data being sent between the bank's servers and clients' devices to guard against data breaches and unauthorized access.

With the rise of smartphones and other mobile devices, mobile banking has become a game-changing technology in the world of digital banking. Customers may use mobile banking apps to access a variety of services straight from their devices, including managing investments, conducting transactions, and checking account balances. Application Programming Interfaces (APIs) that facilitate communication between the mobile app and the bank's backend systems are included in these apps, which are created with the help of mobile development frameworks like Kotlin for Android and Swift for iOS. The usefulness and security of mobile banking applications are improved by features like push notifications, biometric authentication, and geolocation services, which provide users with a simple and safe banking experience while on the move.

Because cloud computing offers a scalable and adaptable environment for implementing and administering digital banking services, it has completely changed the way banks manage their IT infrastructure. Cloud services provide banks with the ability to use virtualized resources and lessen their need for hardware housed on-site. These services include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Banks can now grow their operations effectively, roll out new services quickly, and handle data with high availability and dependability thanks to this move to the cloud. Cloud computing facilitates the creation of data-intensive apps and services by supporting the processing and storing of massive amounts of transaction and customer data.

With its decentralized and secure approach to documenting financial transactions, blockchain technology is a major revolution in digital banking. The distributed ledger technology of blockchain makes sure that every member of the network has an identical picture of the transaction history, which lowers the possibility of fraud and increases transparency. Smart contracts simplify a variety of financial processes by enabling automated and trustless transactions. Smart contracts are self-executing contracts with the contents of the agreement encoded into code. To improve the speed and security of these procedures, banks are investigating the use of blockchain technology for applications including trade finance, digital identity verification, and international payments.

Digital banking now relies heavily on artificial intelligence (AI) and machine learning (ML), which are advancing fraud detection, client service, and financial management. Artificial intelligence (AI)-driven chatbots and virtual assistants provide consumers immediate assistance by managing standard questions and tasks with little assistance from humans. Large databases are analyzed by machine learning algorithms to find trends and abnormalities, giving banks the ability to detect and stop fraud in real time. AI-driven analytics also provide individualized financial insights and guidance, assisting clients in making wise spending, saving, and investing choices.

Because it allows banks to use the massive volumes of data created by digital transactions, big data analytics is essential to digital banking. To get insights into consumer behavior, tastes, and trends, data analytics technologies process and analyze customer data. This enables banks to customize their offerings to meet the specific demands of their customers. For example, predictive analytics makes predictions about the wants and habits of customers, allowing banks to proactively provide relevant solutions like customized loan offers or investment possibilities. By combining big data with cutting-edge analytics technologies, banks may better understand and anticipate the demands of their clients, resulting in financial services that are more effective and efficient.

In the context of digital banking, cybersecurity is a critical issue since cyber-attacks and data breaches are becoming more common. Banks use a variety of security measures, such as

intrusion detection systems, encryption, and multi-factor authentication (MFA), to protect sensitive financial data. MFA adds degree of protection by requiring users to give several forms of authentication before being able to access their accounts. Data that is sent between users and banks is shielded from interception via encryption. By keeping an eye on network traffic for unusual activity, intrusion detection systems may identify any security problems and notify banks promptly so they can take appropriate action to reduce risks.

Since banks are required to abide by a complicated structure of rules controlling data privacy, financial transactions, and cybersecurity, regulatory compliance is a crucial component of digital banking. Strict guidelines for data security, user permission, and transparency are mandated by laws like the General Data security Regulation (GDPR) and the Payment Services Directive 2 (PSD2). To comply with these regulations, banks must put in place thorough compliance procedures and systems to stay in compliance and retain regulatory approval. Banks can handle the growing complexity of regulatory duties via the use of Regulatory Technology (RegTech) solutions, which employ automation and artificial intelligence to expedite compliance procedures.

By enabling banks to exchange financial data with third-party providers via APIs, open banking is a game-changing idea that promotes innovation. By integrating new financial services and products with bank systems, this strategy fosters competition and increases client choice. Open banking fosters cooperation between fintech and banks, leading to creative solutions like customized financial management tools and account aggregation platforms. Banks that support open banking may take advantage of these alliances to increase the range of services they provide and give their clients a more seamless, all-inclusive banking experience.

With the introduction of chatbots and virtual assistants, artificial intelligence (AI) has completely changed the banking industry's customer care environment, and machine learning (ML) has greatly improved predictive analytics and risk management capabilities. The delivery of effective, customized, and safe banking services now depends heavily on these technologies, which represents a significant change in the way financial institutions engage with their clientele and control operational risks.

AI in Customer Support: Virtual Assistants and Chatbots

Artificial intelligence (AI)-driven chatbots and virtual assistants are transforming customer service by providing prompt, round-the-clock support and streamlining repetitive chores. Chatbots are artificial intelligence (AI) powered programs that converse with users via text or voice in an attempt to mimic human interaction and provide assistance and knowledge. Because they are built using natural language processing (NLP) methods, they can comprehend and interpret user inputs in a way that is similar to that of a person. To enable the chatbot to properly answer a broad variety of client requests, this entails training it on big datasets that include diverse language patterns and contextual information.

compared to standard chatbots, virtual assistants are more complex and often use advanced AI features to provide a wider range of services. To complete duties like making appointments, carrying out transactions, and making tailored suggestions, they may interact with other systems and apps, manage complicated requests, and conduct multi-turn discussions. Virtual assistants employ a mix of natural language processing (NLP), machine learning, and contextual awareness to provide more intelligent and flexible replies that improve the user experience in general.

There are several advantages to using chatbots and virtual assistants in banking. By addressing basic questions and automating repeated operations, they drastically lessen the strain of human

customer care workers. This increases productivity while freeing up human agents to concentrate on more intricate and valuable interactions. Furthermore, consistent and correct replies are provided by chatbots and virtual assistants, reducing the possibility of human mistake and guaranteeing that clients get precise information. Their round-the-clock operation also improves accessibility, enabling clients to get help whenever they need it, no matter where they are in the world.

Customer engagement and satisfaction are also impacted by the use of AI in customer service. Chatbots and virtual assistants increase customer satisfaction by improving the entire customer experience via tailored interactions and instantaneous replies. A more individualized banking connection may be fostered by them by analyzing consumer data and behavior to customize interactions, provide pertinent product suggestions, and attend to particular requirements. Furthermore, they may continuously enhance their effectiveness and provide more complex help over time because of their capacity to learn from and adapt to encounters.

In the banking industry, machine learning has become a potent instrument for risk management and predictive analytics since it provides sophisticated forecasting, decision-making, and fraud detection skills. With the use of statistical algorithms and historical data, predictive analytics helps banks forecast future occurrences with confidence by spotting patterns and trends. By continuously increasing their accuracy and learning from data, machine learning algorithms improve predictive analytics. To enable models to provide more accurate predictions and insights, this entails training them on huge datasets to identify patterns and linkages.

Machine learning algorithms evaluate transaction data, demographic data, and interaction patterns about client behavior to forecast the requirements and preferences of the customer. For instance, banks may determine which consumers are most likely to need a loan or investment product shortly by looking at past spending trends.

By using predictive models to segment clients based on their behavior, banks can target certain groups with customized offers and marketing campaigns. This degree of customization raises the possibility of cross-selling and up-selling financial items while also improving consumer engagement.

Because machine learning offers sophisticated instruments for detecting and reducing possible dangers, it is also essential to risk management. Machine learning models examine a variety of variables, such as income, spending patterns, and credit history, to assess credit risk and determine the probability of default. More precise risk evaluations are produced as a consequence of these algorithms' ability to spot patterns and correlations that more conventional credit scoring techniques could overlook. Machine learning algorithms adjust to shifting risk variables and increase their forecast accuracy by continually learning from fresh data.

Another area where machine learning is very influential is fraud detection. Real-time transaction data is analyzed by machine learning algorithms to look for irregularities and questionable activity that could point to fraud. These models look for patterns that differ from typical behavior using methods including classification, anomaly detection, and clustering. Banks may minimize losses and safeguard consumer accounts by taking proactive steps to detect possibly fraudulent activities. Rapid identification and reaction to new fraud risks are made possible by the capacity to continually monitor and analyze transactions.

By revealing possible hazards and weaknesses in banking processes, machine learning also improves operational risk management. Predictive models, for example, might use past data and trends to anticipate operational interruptions, such as system failures or security breaches.

Banks may lessen the effect of operational risks by taking preventative action and recognizing any problems before they arise. Furthermore, machine learning algorithms may improve operational procedures and resource allocation, enhancing resilience and overall efficiency.

Digital banking is changing as a result of the incorporation of AI and machine learning technologies, which are also spurring innovation and enhancing the client experience. With more advanced features and customization available, chatbots and virtual assistants are growing in sophistication. Predictive analytics and risk management are being advanced by machine learning, giving banks more effective tools for fraud detection, operational efficiency, and forecasting. There will probably be more opportunities for synergy between AI-driven customer service and machine learning-based analytics as these technologies develop further since they will become more integrated and interoperable. For instance, predictive analytics may influence the functioning and design of virtual assistants, and AI-powered chatbots can use machine learning models to provide more precise and context-aware replies. These technologies' continued growth will spur more developments in digital banking, opening up fresh avenues for creativity and client interaction.

CONCLUSION

The scene has been profoundly altered by technological breakthroughs, according to a review of the underlying underpinnings of digital banking. While online and mobile banking platforms have increased accessibility and convenience, core banking systems continue to be essential for managing banking operations and transactions. Scalability and flexibility brought about by cloud computing have made it possible for banks to effectively manage expanding data and service requirements. Blockchain technology solves important issues in transaction processing by providing increased security and transparency. With their advanced capabilities for fraud detection, customization, and predictive analytics, artificial intelligence and machine learning have emerged as critical components in the improvement of risk management and customer service. As these technologies develop further, their integration will spur further innovation in digital banking, increasing client happiness, efficiency, and security. However, to handle new issues and guarantee a safe and responsive banking environment, the quick speed of technological advancement also calls for constant adaptation and attention.

REFERENCES:

[1] O. T. Nguyen, “Factors affecting the intention to use digital banking in Vietnam,” *J. Asian Financ. Econ. Bus.*, 2020, doi: 10.13106/jafeb.2020.vol7.no3.303.

[2] T. T. Nguyen, H. T. Nguyen, H. T. Mai, and T. T. M. Tran, “Determinants of digital banking services in Vietnam: Applying utaut2 model,” *Asian Econ. Financ. Rev.*, 2020, doi: 10.18488/journal.aefr.2020.106.680.697.

[3] D. N. Nguyen, D. D. Nguyen, and D. Van Nguyen, “Distribution information safety and factors affecting the intention to use digital banking in Vietnam,” *J. Distrib. Sci.*, 2020, doi: 10.15722/jds.18.6.202006.83.

[4] S. Melnychenko, S. Volosovych, and Y. Baraniuk, “Dominant Ideas Of Financial Technologies In Digital Banking,” *Balt. J. Econ. Stud.*, 2020, doi: 10.30525/2256-0742/2020-6-1-92-99.

[5] Z. F. Mamedov and A. Azer, “The development of digital banking in modern russia,” *Econ. Soc. Dev. B. Proc.*, 2020.

[6] K. D. Melubo and S. Musau, "Digital Banking and Financial Inclusion of Women Enterprises in Narok County, Kenya," *Int. J. Curr. Asp. Financ. Bank. Account.*, 2020, doi: 10.35942/ijcfa.v2i1.104.

[7] S. A. Husseini and S. F. Fam, "Integrating TQM practices and knowledge management to enhance Malaysian digital banking," *Opcion*, 2019.

[8] O. O. Oni, "Effect of Digital Banking on Customer Satisfaction Within the Federal Capital Territory, Nigeria," *Accountability, Transpar. Nation-Building*, 2019.

[9] S. Lumpkin and S. Schich, "Banks, Digital Banking Initiatives and the Financial Safety Net: Theory and Analytical Framework," *J. Econ. Sci. Res.*, 2019, doi: 10.30564/jesr.v3i1.1113.

[10] A. Nikolic and D. Nikolic, "Digital Banking Transformation - Development and Use of Electronic Banking Serbia," *41st International Scientific Conference on Economic and Social Development*. 2019.

CHAPTER 9

AN OVERVIEW ON THE RISE OF MOBILE WALLETS AND CONTACTLESS PAYMENTS

Kshipra Jain, Assistant Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- kshipra.jain@atlasuniversity.edu.in

ABSTRACT:

Driven by technology breakthroughs and evolving customer tastes, the financial services industry has seen considerable change with the emergence of mobile wallets and contactless payments. This review looks at the creation and uptake of contactless payment systems that make use of NFC and RFID technology, as well as mobile wallets like Apple Pay and Google Pay. When compared to conventional payment methods, these technologies provide improved speed, convenience, and security. The report evaluates the advantages, such as increased transaction efficiency and decreased fraud risk, and looks at the main competitors in the industry, including important technology suppliers and payment networks. It also draws attention to difficulties with privacy, security, and regulatory compliance. The review also explores the implications for the financial ecosystem, the adoption patterns that are already in place, and potential future paths that might include new business models and developing technology. The report emphasizes these payment technologies' revolutionary importance in updating payment systems and influencing the direction of financial transactions by offering a thorough examination of them.

KEYWORDS:

Adoption, Contactless Payments, Mobile Wallets, Security, Technology.

INTRODUCTION

Due to shifting consumer tastes and technological improvements, financial transactions have undergone a considerable evolution with the introduction of mobile wallets and contactless payments. Applications that enable users to store and manage their payment information on their mobile devices are called mobile wallets, also known as digital wallets or e-wallets. This makes it possible for customers to conduct safe and easy transactions both online and in physical shops [1], [2]. Alternatively, contactless payments employ technologies like Near Field Communication (NFC) and Radio Frequency Identification (RFID) to allow consumers to make purchases by only touching their payment card or mobile device near a contactless payment terminal.

Mobile wallets provide a quick and safe way to make payments by using a variety of technologies. These apps essentially record the payment information of users, including bank account information, credit and debit card information, and even information on virtual currencies. To safeguard consumers' sensitive data, mobile wallet technology combines tokenization, encryption, and security components. To guarantee that payment information is safely sent between the mobile device and the payment processing system, mobile wallets utilize encryption, a key security technique [3], [4]. The mobile wallet encrypts the payment information when a transaction is started, making it unreadable by other parties. Information is encrypted using sophisticated algorithms in this process, and only authorized parties with the right encryption keys may decode it.

Tokenization substitutes distinct tokens for sensitive payment data, adding an extra degree of protection. Tokens that reflect the payment data are generated by mobile wallets, rather than sending real credit card numbers. While the real card information is stored safely within the mobile wallet's secure element, these tokens are used for transaction processing. Given that tokens are worthless outside of the designated transaction environment, tokenization lowers the risk of fraud and data breaches [5], [6]. A mobile wallet's secure element (SE) is a specific hardware part intended to safeguard credit card details. Cryptographic keys and encrypted data are stored in the SE, guaranteeing that private data is safe even if the device is hacked. Mobile wallets sometimes make use of Trusted Execution Environments (TEEs), which are safe zones within the processor of the device that provides extra security for private activities and data.

Mobile wallets may be used for more than just making and receiving payments. Features including transaction history, digital receipts, and loyalty card administration are often included. Within the wallet application, users may monitor their spending habits, see their recent transactions, and access digital discounts and rewards programs. Peer-to-peer (P2P) payments are supported by some mobile wallets, making it simple for users to send money to friends and family. The usefulness and convenience of mobile wallets are further enhanced by integration with different payment systems and financial institutions.

By allowing transactions to be completed with only a touch of a card or mobile device, contactless payments have completely changed the way people make purchases. NFC and RFID, two wireless communication technologies that work across short distances, are the main foundations of this technology. NFC is a radio communication technology that enables data interchange between devices by bringing them close together, usually within a few millimeters. NFC-enabled payment cards and mobile devices interact with contactless payment terminals using NFC in contactless payment systems [7], [8]. The NFC technology uses wireless transmission to send payment information to a terminal when a user taps their card or device close to it to complete the transaction. The short-range transmission of NFC lowers the possibility of unwanted access and guarantees the security of transactions.

Although RFID functions are often used in a wider variety of applications, such as contactless payment cards. When brought near an RFID reader, the unique identifiers found in RFID tags implanted in payment cards or mobile devices are read. Contactless payments are made possible by RFID technology, which makes it simple and fast for the payment card or device to communicate with the payment terminal. There are a few essential elements involved in the contactless payment implementation. NFC and RFID communication is made possible by integrated chips and antennae found in contactless payment cards. Readers that can recognize and handle contactless transactions are placed in payment terminals. The procedures for transaction authorization and settlement are facilitated by payment processors and financial institutions. Compared to conventional payment methods, contactless payments have several benefits. By cutting down on transaction times and eliminating the need for direct physical touch with payment terminals, they provide a quicker and more convenient payment experience. This is especially helpful in places with a lot of traffic, including vending machines, retail businesses, and transportation systems [9], [10]. The use of digital payment methods is encouraged by the ease of contactless payments, which also improves the entire consumer experience.

When it comes to contactless payments and mobile wallets, security and privacy are major considerations. Even with the most sophisticated security measures in place, there are still dangers and vulnerabilities associated with these technologies. To preserve user confidence and guarantee the further expansion of digital payment systems, these issues must be resolved. Payment information is protected in mobile wallets by security features including tokenization,

encryption, and secure components. To protect their devices and private information, users must, nonetheless, also adopt security measures. This entails protecting their mobile wallets with the most recent security updates, employing strong passwords or biometric authentication techniques to unlock their devices, and being watchful for malware or phishing efforts that might compromise their data. To safeguard payment data during transmission, contactless payments also include security elements like tokenization and encryption. However, consumers should be aware of the possible hazards connected with illegal scanning or skimming of payment information since NFC and RFID technologies are proximity-based. Payment cards and mobile devices often have built-in security mechanisms that restrict the amount of data transferred and demand verification for higher-value transactions to reduce these dangers.

DISCUSSION

Contactless payments and mobile wallets are both governed by industry standards and governmental regulations that aim to safeguard consumer interests and improve security. Guidelines for safe payment processing and data security are established by organizations like the Payment Card Industry Data Security Standard (PCI DSS) and the EMVCo standards for contactless payments. Adherence to these guidelines contributes to the security of payment systems and the sufficient protection of users' sensitive data Mobile wallets and contactless payments will continue to evolve due to constant technology developments and innovation. The use of blockchain technology, the incorporation of biometric verification, and the growth of virtual currencies are examples of emerging trends. Mobile wallets are increasingly using biometric identification, such as face and fingerprint recognition. These techniques offer another degree of protection by confirming the user's identification before approving transactions. Mobile wallet security is improved, and users may enjoy a more simple and user-friendly experience with biometric identification. Blockchain technology has the potential to improve digital payments' security and transparency. A safe and verifiable record of transactions may be provided via blockchain's decentralized and immutable ledger, lowering the possibility of fraud and enhancing transaction integrity. Although blockchain technology is still being used by payment systems in its infancy, researchers are looking at how it may be used in contactless payments and mobile wallets.

The future of mobile payments is expected to be impacted by digital currencies, particularly cryptocurrencies and central bank digital currencies (CBDCs). Central bank-issued digital copies of national currencies, or CBDCs, provide a safe and effective way to make payments. Alternative payment options are offered by cryptocurrencies like Bitcoin and Ethereum, which are also being accepted by banks and retailers. Digital currency integration with contactless payment methods and mobile wallets has the potential to completely change the payment environment and open up new avenues for creativity. Modern contactless payment and communication systems are based on two essential technologies, Near Field Communication (NFC) and Radio-Frequency Identification (RFID), each having unique uses and features. A type of RFID technology called NFC allows flawless data transmission between devices across short distances. Radio waves are used by both NFC and RFID to transfer data, although their applications, frequencies, and ranges are different.

Short-range communication, usually occurring within a few millimeters, is the focus of NFC technology. The ISO/IEC 14443 standard, which outlines the communication protocol for contactless smart cards, serves as its foundation. High-frequency (13.56 MHz) radio waves are used by NFC devices to connect and exchange data. Three primary modes of operation are supported by the technology: card emulation, peer-to-peer, and reader/writer modes. An NFC-capable device can read data from and write data to NFC tags or cards while it is in reader/writer mode. Applications like electronic ticketing, where customers may attend events or

transportation services by tapping their NFC-enabled smartphone against a ticket scanner, are often used in this way. Peer-to-peer mode allows two NFC-capable devices to immediately exchange data, making it easier to do tasks like file transfers and contact sharing. An NFC-enabled device may operate at NFC-compatible payment terminals by imitating a contactless payment card in card emulation mode.

RFID covers a wider spectrum of technologies that operate in other frequency bands, such as ultra-high-frequency (UHF), high-frequency (HF), and low-frequency (LF). RFID systems are made up of readers and tags. RFID tags have an antenna and a microchip that allow them to communicate with an RFID reader when they are close enough to do so. RFID tags may be classified as semi-passive, active, or passive based on how they communicate and get power. Passive RFID tags depend on the energy sent by the RFID reader to power them and send data instead of a battery. These tags provide an affordable way to track and manage products, which is why they are often employed in asset tracking and inventory management. On the other hand, active RFID tags include a battery that powers the electronics within the tag, enabling greater scan ranges and more frequent data updates. These tags are often utilized in real-time tracking applications including high-value asset management and vehicle monitoring. Semi-passive RFID tags, often referred to as battery-assisted passive (BAP) tags, depend on the signal from the reader to communicate while having a battery powering their electronics.

NFC and RFID applications are used in a wide range of sectors, including logistics, retail, healthcare, and transportation. Mobile payments and digital wallets, which allow users to conduct transactions by tapping their cellphones against NFC-enabled payment terminals, are two common applications of NFC technology. When scanned, NFC tags placed in retail items provide customers access to extra information and promotions. NFC is used in healthcare to monitor medications and identify patients, increasing precision and lowering mistakes. RFID technology is widely used in logistics and supply chain management for inventory tracking and management. Real-time insight into stock levels and movement is provided by RFID tags affixed to goods or pallets, which increases productivity and lowers losses. RFID is used in transportation to enable electronic toll collection systems, which eliminate the need for cars to stop at toll booths. RFID tags are used in animal monitoring and identification as a means of managing and keeping an eye on animals. Modern payment systems are not complete without digital tokens, which provide increased security and anonymity for financial transactions. Digital tokens are distinct identifiers that substitute non-sensitive counterparts for sensitive payment data, such as credit card numbers. Tokenization ensures that real payment information is hidden from view during transactions, lowering the risk of fraud and data breaches.

Tokenization entails assigning a unique token, created by a tokenization service provider, to each piece of sensitive data. The token is used instead of the real payment details when a transaction is started. Potential attackers cannot benefit from the token since it is meaningless outside of the particular transaction environment and has no inherent value. Tokens can only be resolved back to their original value by the tokenization service provider, who maintains a secure mapping between tokens and sensitive data. Tokenization is a commonly used security measure in contactless payment systems and mobile wallets. The supplier of the mobile wallet is a token for the credit card number when a user saves their credit card information in it. To resolve the token and finish the transaction, the mobile wallet sends the token to the payment terminal, which then gets in touch with the payment processor. By using this method, the real card information is protected and isn't sent across the payment network. Another essential technology that supports the security of digital tokens and payment systems is encryption. Using an encryption key and an algorithm, plain text data is transformed into an unintelligible format called ciphertext during the encryption process. The only person who can decode the

encrypted data back into its original format is the one who has the necessary decryption key. Sensitive data is shielded from unwanted access and kept secret thanks to encryption.

Encryption is used in digital payment systems throughout the transaction process. Encryption technologies like Transport Layer Security (TLS) and Secure Socket Layer (SSL) are used during data transfer to protect communication between the payment processor and the payment device. Data sent over the internet is shielded from interception and manipulation thanks to the encrypted connections created by the SSL and TLS protocols. Another important factor in protecting saved payment data is encryption. For instance, payment data is encrypted to thwart unwanted access whether kept on a payment server or in a mobile wallet. To protect data when it's at rest, encryption techniques like the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are often used. While RSA is an asymmetric encryption technique that employs a pair of keys public and private for safe data transmission, AES is a symmetric encryption system that uses the same key for both encryption and decryption.

Secure key management procedures are crucial for preserving the integrity of digital payment systems, in addition to encryption and tokenization. Encryption key production, distribution, storage, and protection are all included in key management. Access to sensitive data is restricted and encryption keys are managed securely when key management is done well. Regular key rotation, safe key storage, and access restrictions to stop unwanted usage are examples of key management procedures. Innovation in digital payments is being driven by the integration of NFC, RFID, digital tokens, and encryption technologies, which also improve security across a range of applications. The combination of these technologies improves user experience and lowers fraud risks by enabling safe and effective payment processing. Future developments and trends in digital payment systems are influencing the direction of NFC and RFID technology. For example, the growing number of wearables with NFC capabilities, such fitness trackers and smartwatches, is increasing the number of devices that can accept contactless payments. Wearable technology offers a safe and practical way for consumers to make payments without needing to carry a real wallet.

Inventory control and supply chain monitoring are becoming more efficient thanks to the introduction of ultra-high-frequency (UHF) RFID tags with better read ranges and data transmission speeds. Longer read ranges and quicker data transmission are provided by UHF RFID tags, allowing for more effective asset management and real-time visibility. The future of NFC and RFID applications is also being influenced by the trend of integrating blockchain technology with digital payments. The decentralized and unchangeable ledger of blockchain technology may improve payment transaction security and transparency by offering a safe transaction history and lowering the possibility of fraud. To guarantee the security of digital payment systems, key management procedures and encryption technology development will need to continue. Encryption algorithms and key management strategies will need to change as cyber threats do to handle emerging vulnerabilities and preserve the integrity of payment data.

he innovative efforts of payment solution providers and major credit card networks, contactless payments have become a standard feature of contemporary financial transactions. With their extensive networks and creative solutions, the three main participants in the contactless payment market—Visa, Mastercard, and American Express—have each contributed to the development and widespread use of contactless payment technology. Payment solution providers work in tandem with these big credit card networks to continuously push the limits of contactless payment capabilities and integrate cutting-edge technology to provide safe, easy, and convenient payment experiences. Visa, a pioneer in digital payments globally, is renowned for both its wide network and its dedication to developing payment technology. Near Field Communication (NFC) technology is used by Visa's contactless payment solution, Visa

Contactless, to facilitate quick and safe transactions. Simply swiping a Visa card or mobile device near a contactless payment terminal is how customers can make purchases using Visa Contactless payments, which stand out for their quickness and ease of use. The foundation of Visa's contactless technology is the EMV (Europay, MasterCard, and Visa) standard, which guarantees security and compatibility amongst various payment methods. Visa's worldwide reach and broad merchant acceptance network make it a popular option for both consumers and companies, helping to drive the widespread adoption of contactless payments.

In terms of contactless payment technologies, Visa has also been a leader. The organization has implemented other improvements aimed at enhancing the user experience, including the introduction of biometric authentication capabilities and the ability to enable larger transaction limits. By working with mobile wallet providers, Visa has increased the acceptance of contactless payments. Users can now safely keep their Visa card details on their smartphones and use mobile wallets like Apple Pay, Google Pay, and Samsung Pay to make purchases. Furthermore, by substituting distinct tokens for sensitive payment data during transaction processing, Visa's investment in tokenization technology improves the security of contactless transactions.

Offering its Mastercard Contactless solution to enable quick and safe payments, Mastercard is another significant competitor in the contactless payment market. NFC technology is used by Mastercard Contactless payments to facilitate transactions with a single touch of the card or mobile device. The goal of Mastercard's contactless payment technology is to provide customers with a smooth and convenient payment experience by speeding up transaction times. Because Mastercard's contactless cards and mobile wallets work with a variety of payment terminals, they are widely accepted and simple to use. Through several inventions, Mastercard has advanced contactless payment technology significantly. The business has started offering contactless payment cards with improved security features, such as dynamic CVV (Card Verification Value) codes and biometric verification. By forcing customers to utilize face recognition or fingerprint authentication to confirm their identity before approving transactions, biometric authentication provides an additional degree of protection. Due to their frequent changes, dynamic CVV codes provide a unique security code for every transaction, hence aiding in the prevention of card-not-present fraud. By working with tech partners, Mastercard has also been able to build contactless payment solutions for wearables, such as fitness trackers and smartwatches, which has increased the number of devices that can accept contactless payments. Offering its American Express Contactless solution to improve the payment experience, American Express is a well-known participant in the contactless payment market. With only a touch of the card or smartphone, American Express Contactless payments use NFC technology to provide speedy and safe transactions. By eliminating the need for direct physical touch with payment terminals and expediting transaction times, American Express's contactless payment solution is intended to provide a seamless and effective payment experience.

To enhance contactless payment security and functionality, American Express has made several enhancements. To secure payment information during transactions, the business has used tokenization technology, which substitutes distinct tokens for sensitive card information while processing payments. To increase security by forcing customers to validate their identities before completing transactions, American Express has also investigated the use of biometric authentication for contactless payments. The company's attempts to provide contactless payment solutions that put cardholder convenience and security first are clear indications of its emphasis on security and user experience.

Payment solution providers have been instrumental in pushing innovation, developing contactless payment technologies, and enhancing the potential of digital payments. These businesses have brought in a range of innovations and technology that improve contactless payment ease, security, and usefulness. Among the biggest advancements in contactless payments are mobile wallets. using the help of mobile wallet solutions like Apple Pay, Google Pay, and Samsung Pay, consumers can safely keep their credit card information on their smartphones and conduct contactless payments using NFC technology. Numerous credit cards, loyalty cards, and transport passes may all be stored in mobile wallets, among other capabilities. Additionally, they use biometric authentication—like fingerprint or face recognition—to improve security and provide a smooth payment process.

Wearable technology has become a major advance in contactless payments. Payment solution providers have created contactless payment options for fitness trackers, smartwatches, and rings, among other wearables. These gadgets include NFC technology, allowing consumers to touch and pay with ease, making payments easy and hands-free. Wearable payment systems with features like biometric identification and security components to safeguard payment information are designed to be both user-friendly and safe. The increasing popularity of contactless payments has led to the evolution of contactless payment terminals. Payment solution providers have created cutting-edge payment terminals that work with RFID and NFC technologies, allowing retailers to take contactless payments with a variety of cards and devices. These terminals are equipped with technologies like tokenization and dynamic encryption to safeguard payment information, making them ideal for quick and safe transaction processing. The acceptance of contactless payments in several sectors, including retail, transportation, and hospitality, has been made easier by the widespread installation of contactless payment terminals.

Payment solution providers provide tokenization services that improve contactless payment security by substituting distinct tokens for sensitive payment data. To safeguard card information during transactions, these services are linked to payment processing systems and mobile wallets. By ensuring that real payment information is not sent across the payment network, tokenization services lower the possibility of fraud and data breaches. Tokenization services are provided by payment solution firms to banks, retailers, and technology suppliers, enhancing the ecosystem's overall security for contactless payments. Technologies for Fraud Detection and Prevention are essential advancements that improve contactless payment security. Payment solution providers have created sophisticated systems for preventing and detecting fraud, using machine learning (ML) and artificial intelligence (AI) algorithms to detect and stop fraudulent activity. These systems look for abnormalities and stop fraudulent transactions by analyzing user behavior, transaction patterns, and other data. Payment solution providers can provide real-time monitoring and protection against new risks by incorporating AI and ML into fraud detection systems.

Contactless payments are also impacted by innovations in the field of blockchain technology. The decentralized and unchangeable ledger of blockchain technology offers a safe and transparent transaction record, lowering the possibility of fraud and improving transaction integrity. To increase security, expedite transaction processing, and support new payment patterns, payment solution providers are investigating the possibility of integrating blockchain technology into existing payment systems. Digital currencies, smart contracts, and decentralized payment networks are among the contactless payment applications that blockchain may be used for. Future contactless payment innovations will be characterized by ongoing technical development and innovation. The use of biometric verification, the growth of virtual currencies, and the creation of sophisticated payment methods are examples of

emerging trends. With its improved security and ease, biometric identification is predicted to be used in contactless payments more and more. The payment process will be expedited and further levels of security added by integrating biometric capabilities like voice authentication, face recognition, and fingerprint identification. With the development of biometric technology, contactless payments will become safer and more convenient. The use of digital currencies in contactless payments is expected to change in the future. These include cryptocurrencies and central bank digital currencies (CBDCs).

Digital copies of national currencies that are issued by central banks are known as CBDCs, and they provide a safe and effective way to make payments. Alternative payment options are provided by cryptocurrencies like Bitcoin and Ethereum, which are becoming more and more popular with both customers and retailers. Digital currency integration with contactless payment systems will spur more innovation and change the payment environment. The future of contactless payments will be shaped by advanced payment technologies including Internet of Things (IoT) integration and autonomous payment systems. AI and IoT-powered autonomous payment systems will make it possible for transactions to be completed automatically and seamlessly across a range of platforms and devices. Contactless payments will be made easier by IoT integration in smart settings like linked homes and smart cities, opening up new possibilities for convenience and creativity.

CONCLUSION

Technology breakthroughs and changing customer expectations have led to a revolutionary change in the payment environment with the emergence of mobile wallets and contactless payments. NFC and RFID technologies are used by mobile wallets, which include well-known systems like Apple Pay and Google Pay, to provide quick, safe transactions that improve convenience for customers and businesses. With advantages including faster checkout times, more transaction security, and better financial management tools, the integration of different payment systems has drastically upended conventional payment methods. Adoption of these technologies is not without its difficulties, however, since privacy issues, security flaws, and strict regulatory compliance are all important considerations. Resolving these issues is essential to preserving customer confidence and guaranteeing the expansion of contactless and mobile payment systems.

In the future, payments will probably be further shaped by developments like the incorporation of cryptocurrencies, improvements in biometric identification, and the growth of contactless payment possibilities into wearables and Internet of Things devices. All things considered, contactless payments and mobile wallets have the potential to completely change the way people transact money by providing a window into a more effective, safe, and user-friendly payment environment.

REFERENCES:

[1] M. Aljawder and A. Abdulrazzaq, “The effect of awareness, trust, and privacy and security on students’ adoption of contactless payments: An empirical study,” *Int. J. Comput. Digit. Syst.*, 2019, doi: 10.12785/ijcds/080614.

[2] Y. M. Wang and W. C. Lin, “Understanding consumer intention to pay by contactless credit cards in Taiwan,” in *International Journal of Mobile Communications*, 2019. doi: 10.1504/IJMC.2019.096507.

[3] A. J. Conneely *et al.*, “Laser micromachining of contactless RF antenna modules for payment cards and wearable objects,” 2019. doi: 10.2351/1.5118613.

[4] R. Paavola, "Adopting Emerging Technology In Public Sector: A Case Of The Contactless Payment System For Pupils In Elementary Schools," in *10th Scandinavian Conference on Information Systems, SCIS 2019*, 2019.

[5] A. Debant and S. Delaune, "Symbolic Verification of Distance Bounding Protocols," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019. doi: 10.1007/978-3-030-17138-4_7.

[6] V. Jain, Y. Khurana, M. Kharbanda, and K. Mehta, "BeaTicket - Beacon Based Ticketing System," *Recent Adv. Comput. Sci. Commun.*, 2019, doi: 10.2174/2213275912666190307163422.

[7] J. de D. B. Mugiraneza, Y. Sugita, K. Kida, T. Maruyama, and S. Yamagishi, "Enhancing the Performance of Display-Integrated NFC Antenna by Magnetic Resonance Coupling for Secure Contactless Payment Transactions and for IOT," in *Digest of Technical Papers - SID International Symposium*, 2018. doi: 10.1002/SDTP.12114.

[8] L. Grustniy, "Secure Element — securing contactless payments in smartphones | Kaspersky official blog," kaspersky daily.

[9] W. Kaewratsameekul, "An examination of behavioral intention to use contactless mobile payment: Rapid transit system in Thailand," *Sci. Eng. Heal. Stud.*, 2018, doi: 10.14456/sehs.2018.2.

[10] Ł. Zakonnik, P. Czerwonka, and R. Zajdel, "Contactless payments in Poland - advantages and disadvantages based on surveys of a selected group of users over the years 2011-2018," *SHS Web Conf.*, 2018, doi: 10.1051/shsconf/20185701033.

CHAPTER 10

INVESTIGATION OF CUSTOMER EXPERIENCE IN DIGITAL BANKING

Prof. Ameya Ambulkar, Assistant Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- ameya.ambulkar@atlasuniversity.edu.in

ABSTRACT:

The study of the customer experience in digital banking looks at how consumers' interactions with financial institutions are affected by developments in technology and digital transformation. This research looks at many important aspects of digital banking, such as multichannel assistance, customization, and user interface design. It emphasizes how crucial user-friendly online and mobile banking systems, strong security protocols, and efficient customer service are to creating satisfying customer experiences. The study also examines how data analytics, future technology, and consumer input might improve service delivery. The research seeks to provide insights into how digital banking may be adjusted to meet changing consumer expectations and enhance overall satisfaction by examining existing trends and best practices.

KEYWORDS:

Customer Feedback, Digital Banking, Personalization, Security, User Experience.

INTRODUCTION

The success and advancement of contemporary financial services heavily depend on the quality of the customer experience in digital banking. Understanding and improving the customer experience has become crucial for preserving competitive advantage and encouraging client loyalty as banks and other financial institutions continue to embrace digital transformation. Convenience, accessibility, and efficiency are just a few advantages of digital banking, which includes online and mobile banking services [1], [2]. Nonetheless, providing a smooth and satisfying customer experience in this domain requires a thorough comprehension of client requirements, habits, and anticipations in addition to the tactical use of cutting-edge technologies and procedures.

Technological developments and shifting customer demands have been the main forces behind the rise of digital banking. The shift to digital platforms from conventional banking techniques, such as in-branch visits and paper-based transactions, has drastically changed how clients communicate with their financial institutions. Early attempts at digital banking concentrated on offering fundamental web services like transaction processing, account access, and balance inquiries. With time, a vast range of features and services have been added to digital banking to better serve the varied demands of users. Examples of these include mobile applications, online account management, individualized financial insights, and cutting-edge security measures.

The increasing use of smartphones and the internet has accelerated the transition to digital banking by allowing users to access and manage their accounts at any time and from almost anywhere. The banking sector is changing as a result of the emergence of fintech firms and digital-only banks, which puts pressure on established banks to improve and develop their online services. Because of this, digital banking has grown to be an essential part of the whole customer experience, with banks working to provide an intuitive and effective digital platform

that works in tandem with their physical locations and customer support lines [3], [4] In digital banking, usability and accessibility are essential components of the consumer experience. A well-crafted digital banking platform needs to be user-friendly, intuitive, and accessible to a variety of users, including those with impairments. Clearness of the user interface, simplicity in completing routine actions (such as paying bills and transferring money), and general platform responsiveness are all examples of usability. Ensuring the digital banking platform is useable by people with different abilities, including those who use assistive technology, is part of accessibility.

Banks should invest in user experience (UX) design concepts to improve usability. They should also regularly undertake usability testing to find and fix any problems that might degrade the user experience. This entails maximizing the platform's functionality, layout, and style to make sure it satisfies the demands of various clientele groups. Features like keyboard navigation, screen reader compatibility, and adjustable font sizes should be taken into account when designing an accessible system for those with disabilities or visual impairments [5], [6]. In digital banking, personalization and Customization are important factors in improving the user experience. Consumers anticipate individualized service and customized interactions that take into account their unique financial objectives, interests, and habits. Digital banking systems can use artificial intelligence (AI) and data analytics to deliver tailored suggestions, insights, and offers to consumers based on their financial goals, past transactions, and spending habits.

Banks, for instance, may use AI-driven algorithms to examine the spending patterns of their clients and provide customized suggestions for savings or budgeting. Customers may be informed about critical account actions, such as impending bill payments or possible overdrafts, with the use of personalized notifications and alerts. Customers may also customize features like transaction categorizations and bespoke dashboards to fit their requirements and preferences while using digital banking. In Digital Banking, security and privacy are essential elements of the user experience. Customers are becoming more worried about the security of their financial information and the possibility of cyber-attacks as digital transactions and data interchange grow more widespread. Strong security measures must be a top priority for banks to safeguard sensitive consumer data and maintain confidence.

Multi-factor authentication (MFA), which requires users to submit several forms of verification before accessing their accounts, is one of the key security features. Technologies for data encryption protect sensitive data both during transmission and storage, keeping it secure from unwanted access. Frequent vulnerability analyses and security upgrades assist in identifying and addressing any possible flaws in the online banking system [7], [8]. Transparent data practices and adherence to data protection laws, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR), are further privacy factors. Banks should provide consumers opportunities to control their privacy settings and be transparent about how their data is gathered, utilized, and shared.

To provide customers with a great digital banking experience, customer support and assistance are essential. Even while digital platforms are convenient, users could still run into problems or have inquiries that need to be answered by a person. In order to respond to questions from customers, handle issues, and give advice, banks need to have readily available and efficient customer service channels. To accommodate a range of consumer preferences, digital banking systems may include many support channels, such as live chat, email assistance, and phone help. While human support workers may handle more complicated problems and give individualized help, Chatbots and Virtual Assistants powered by artificial intelligence can handle regular requests and deliver instantaneous replies. Ensuring a smooth transition between automated and human assistance guarantees that clients have the assistance they want quickly

[9], [10]. Creating a consistent client experience across digital banking channels requires integration and smoothness. Whether engaging with physical branches, smartphone apps, or internet banking portals, customers need a consistent experience. The user experience is improved overall when digital banking platforms are integrated with other banking services and channels, including third-party apps, financial planning tools, and customer support.

DISCUSSION

Customers may monitor and evaluate their financial data in one location by combining digital banking with financial management solutions, for instance. Customers may undertake activities online and finish them in person if necessary thanks to seamless transitions between digital and physical channels. Financial institutions must allocate resources towards technologies that promote seamless integration and guarantee that clients may get their account details and conduct transactions with ease on various platforms. Technology and innovation are the main factors influencing how the consumer experience has changed in digital banking. Banks may provide new and improved services that enhance the client experience as technology develops. Blockchain, AI, and machine learning are examples of emerging technologies that are changing the face of digital banking and opening up new avenues for client engagement.

Blockchain Technology offers a decentralized and unchangeable record that might improve financial transaction security and transparency. The client experience may be further enhanced by using AI and machine learning to power predictive analytics, automate procedures, and provide tailored suggestions. Banks have to keep up with technology advancements and look into creative solutions that suit the requirements and tastes of their clients. An invaluable source of information for enhancing the online banking experience is customer feedback. Through questionnaires, evaluations, and face-to-face conversations, banks should aggressively seek out and gather consumer input. Consumer pain points, places for improvement, and new trends in consumer preferences may all be found by analyzing customer feedback.

Digital banking systems adapt to shifting demands and expectations via continuous development based on client input. Banks should have procedures in place for routinely assessing and upgrading their online banking services, adding client feedback, and resolving any problems that may come up. Building relationships with clients and showcasing your dedication to their needs encourages trust and loyalty. Numerous banks and financial establishments have effectively executed tactics aimed at augmenting the consumer experience inside digital banking. For instance, Erica, the virtual assistant driven by artificial intelligence on Bank of America's digital banking platform, offers individualized financial counseling, transaction notifications, and budgeting assistance. Customers' interaction with the platform is improved by Erica's smooth and interactive integration with the bank's mobile app.

A Digital-only bank that emphasizes the client experience with its intuitive mobile app and cutting-edge features. Monzo's app gives users a thorough understanding of their money with real-time transaction alerts, budgeting tools, and tailored insights. The bank's excellent reputation and large client base are a result of its emphasis on openness, simplicity, and consumer input. Future developments in client expectations, new trends, and continuous technological breakthroughs will all influence the digital banking customer experience. Financial institutions will persistently investigate novel approaches to boost the digital banking encounter by using advancements like voice banking, augmented reality (AR), and sophisticated data analytics Speech-activated virtual assistants facilitate speech banking, enabling users to conduct banking operations and retrieve account details via spoken prompts. Visualizing financial data or replicating branch interactions are just two examples of the rich and engaging experiences that AR technology provides. The client experience will be further

enhanced by advanced data analytics, which will lead to more precise forecasts and customized suggestions. To remain ahead of new trends and satisfy client expectations, banks will need to emphasize agility and adaptation as the digital banking market continues to grow. In the realm of digital banking, banks may achieve sustained profitability and provide outstanding client experiences by adopting new technologies, emphasizing customization and usability, and sticking to security and customer service.

The success and advancement of contemporary financial services heavily depend on the quality of the customer experience in digital banking. Understanding and improving the customer experience has become crucial for preserving competitive advantage and encouraging client loyalty as banks and other financial institutions continue to embrace digital transformation. Convenience, accessibility, and efficiency are just a few advantages of digital banking, which includes online and mobile banking services. Nonetheless, providing a smooth and satisfying customer experience in this domain requires a thorough comprehension of client requirements, habits, and anticipations in addition to the tactical use of cutting-edge technologies and procedures.

Technological developments and shifting customer demands have been the main forces behind the rise of digital banking. The shift to digital platforms from conventional banking techniques, such in-branch visits and paper-based transactions, has drastically changed how clients communicate with their financial institutions. Early attempts at digital banking concentrated on offering fundamental web services like transaction processing, account access, and balance inquiries. With time, a vast range of features and services have been added to digital banking to better serve the varied demands of users. Examples of these include mobile applications, online account management, individualized financial insights, and cutting-edge security measures.

The increasing use of smartphones and the internet has accelerated the transition to digital banking by allowing users to access and manage their accounts at any time and from almost anywhere. The banking sector is changing as a result of the emergence of fintech firms and digital-only banks, which puts pressure on established banks to improve and develop their online services. Because of this, digital banking has grown to be an essential part of the whole customer experience, with banks working to provide an intuitive and effective digital platform that works in tandem with their physical locations and customer support lines.

In digital banking, usability and accessibility are essential components of the consumer experience. A well-crafted digital banking platform needs to be user-friendly, intuitive, and accessible to a variety of users, including those with impairments. Clearness of the user interface, simplicity in completing routine actions (such as paying bills and transferring money), and general platform responsiveness are all examples of usability. Ensuring the digital banking platform is useable by people with different abilities, including those who use assistive technology, is part of accessibility.

Banks should invest in user experience (UX) design concepts to improve usability. They should also regularly undertake usability testing to find and fix any problems that might degrade the user experience. This entails maximizing the platform's functionality, layout, and style to make sure it satisfies the demands of various clientele groups. Features like keyboard navigation, screen reader compatibility, and adjustable font sizes should be taken into account when designing an accessible system for those with disabilities or visual impairments.

In digital banking, personalization and customization are important factors in improving the user experience. Consumers anticipate individualized service and customized interactions that take into account their unique financial objectives, interests, and habits. Digital banking

systems can use artificial intelligence (AI) and data analytics to deliver tailored suggestions, insights, and offers to consumers based on their financial goals, past transactions, and spending habits. Banks, for instance, may use AI-driven algorithms to examine the spending patterns of their clients and provide customized suggestions for savings or budgeting. Customers may be informed about critical account actions, such as impending bill payments or possible overdrafts, with the use of personalized notifications and alerts. Customers may also customize features like transaction categorizations and bespoke dashboards to fit their requirements and preferences while using digital banking. In digital banking, security and privacy are essential elements of the user experience. Customers are becoming more worried about the security of their financial information and the possibility of cyber-attacks as digital transactions and data interchange grow more widespread. Strong security measures must be a top priority for banks to safeguard sensitive consumer data and maintain confidence.

Multi-factor authentication (MFA), which requires users to submit several forms of verification before accessing their accounts, is one of the key security features. Technologies for data encryption protect sensitive data both during transmission and storage, keeping it secure from unwanted access. Frequent vulnerability analyses and security upgrades assist in identifying and addressing any possible flaws in the online banking system. Transparent data practices and adherence to data protection laws, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR), are further privacy factors. Banks should provide consumers opportunities to control their privacy settings and be transparent about how their data is gathered, utilized, and shared. To provide customers with a great digital banking experience, customer support and assistance are essential. Even while digital platforms are convenient, users could still run into problems or have inquiries that need to be answered by a person. To respond to questions from customers, handle issues, and give advice, banks need to have readily available and efficient customer service channels.

To accommodate a range of consumer preferences, digital banking systems may include many support channels, such as live chat, email assistance, and phone help. While human support workers may handle more complicated problems and give individualized help, chatbots and virtual assistants powered by artificial intelligence can handle regular requests and deliver instantaneous replies. Ensuring a smooth transition between automated and human assistance guarantees that clients have the assistance they want quickly. Creating a consistent client experience across digital banking channels requires integration and smoothness. Whether engaging with physical branches, smartphone apps, or internet banking portals, customers need a consistent experience.

The user experience is improved overall when digital banking platforms are integrated with other banking services and channels, including third-party apps, financial planning tools, and customer support.

Customers may monitor and evaluate their financial data in one location by combining digital banking with financial management solutions, for instance. Customers may undertake activities online and finish them in person if necessary thanks to seamless transitions between digital and physical channels. Financial institutions must allocate resources towards technologies that promote seamless integration and guarantee that clients may get their account details and conduct transactions with ease on various platforms. Technology and innovation are the main factors influencing how the consumer experience has changed in digital banking. Banks may provide new and improved services that enhance the client experience as technology develops. Blockchain, AI, and machine learning are examples of emerging technologies that are changing the face of digital banking and opening up new avenues for client engagement. Blockchain technology, for instance, offers a decentralized and unchangeable record that might improve

financial transaction security and transparency. The client experience may be further enhanced by using AI and machine learning to power predictive analytics, automate procedures, and provide tailored suggestions. Banks have to keep up with technology advancements and look into creative solutions that suit the requirements and tastes of their clients. An invaluable source of information for enhancing the online banking experience is customer feedback.

Through questionnaires, evaluations, and face-to-face conversations, banks should aggressively seek out and gather consumer input. consumer pain points, places for improvement, and new trends in consumer preferences may all be found by analyzing customer feedback. Digital banking systems adapt to shifting demands and expectations via continuous development based on client input. Banks should have procedures in place for routinely assessing and upgrading their online banking services, adding client feedback, and resolving any problems that may come up. Building relationships with clients and showcasing your dedication to their needs encourages trust and loyalty.

Numerous banks and financial establishments have effectively executed tactics aimed at augmenting the consumer experience inside digital banking. For instance, Erica, the virtual assistant driven by artificial intelligence on Bank of America's digital banking platform, offers individualized financial counseling, transaction notifications, and budgeting assistance. Customers' interaction with the platform is improved by Erica's smooth and interactive integration with the bank's mobile app.

Another example is Monzo, a digital-only bank that emphasizes the client experience with its intuitive mobile app and cutting-edge features. Monzo's app gives users a thorough understanding of their money with real-time transaction alerts, budgeting tools, and tailored insights.

The bank's excellent reputation and large client base are a result of its emphasis on openness, simplicity, and consumer input. Future developments in client expectations, new trends, and continuous technological breakthroughs will all influence the digital banking customer experience. Financial institutions will persistently investigate novel approaches to boost the digital banking encounter by using advancements like voice banking, augmented reality (AR), and sophisticated data analytics.

Speech-activated virtual assistants facilitate speech banking, enabling users to conduct banking operations and retrieve account details via spoken prompts. Visualizing financial data or replicating branch interactions are just two examples of the rich and engaging experiences that AR technology provides.

The client experience will be further enhanced by advanced data analytics, which will lead to more precise forecasts and customized suggestions. In order to remain ahead of new trends and satisfy client expectations, banks will need to emphasize agility and adaptation as the digital banking market continues to grow.

In the realm of digital banking, banks may achieve sustained profitability and provide outstanding client experiences by adopting new technologies, emphasizing customization and usability, and sticking to security and customer service.

User interface (UI) and user experience (UX) design elements are crucial in determining the efficacy and level of pleasure that digital banking systems provide. The banking industry is rapidly shifting to digital channels, and as a result, platforms for banking must be designed with both functionality and the user experience including easy navigation and visually pleasing design at the forefront. For digital banking services to be user-friendly, effective, and engaging

and to increase client satisfaction and long-term loyalty well-designed user interfaces and user experiences are crucial. This in-depth examination explores the fundamental design ideas that support successful digital banking systems, highlighting the importance of aesthetics and user-friendly navigation in achieving the best possible user experience.

CONCLUSION

Customer pleasure and loyalty can only be sustained by a smooth, user-friendly, and safe digital contact, according to research on the subject of customer experience in digital banking. The research emphasizes the value of user interface (UI) and user experience (UX) concepts being given top priority in well-designed mobile and online banking services. Data analytics-driven personalization is crucial for adjusting services to each client's unique demands and increasing consumer engagement. Resolving difficulties quickly and effectively requires effective customer care, which includes the use of AI-driven chatbots and multichannel communication. Concerns about security and privacy are still crucial, necessitating strong safeguards to preserve client information and foster confidence.

The research focuses on cutting-edge developments in technology and trends like blockchain and artificial intelligence that provide chances to improve the online banking experience even further. To achieve constant progress, however, obstacles including usability problems, changing client expectations, and technological hiccups must be dealt with. Financial institutions may provide a better digital banking experience that satisfies the needs of contemporary clients and promotes long-term success in the cutthroat financial services market by implementing best practices and using technology advancements.

REFERENCES:

[1] C. I. Mbama *et al.*, "Digital banking, customer experience and bank financial performance: UK customers' perceptions," *Int. J. Bank Mark.*, 2018, doi: 10.1108/IJBM-11-2016-0181.

[2] L. Alboul *et al.*, "Digital banking, customer experience and financial performance: UK bank managers' perceptions," *J. Res. Interact. Mark.*, 2018, doi: 10.1108/JRIM-01-2018-0026.

[3] A. Megargel, V. Shankararaman, T. P. C Fan, and T. Fan Ping-Ching, "SOA maturity influence on digital banking transformation," *J. Bank. Technol.*, 2018.

[4] M. Bhardwaj and R. Aggarwal, "An Empirical Study on Effect of Experience on Consumer Adoption Intention towards Electronic Banking," *Int. J. Emerg. Res. Manag. Technol.*, 2018, doi: 10.23956/ijermt.v6i9.83.

[5] A. Megargel and T. P. C. Fan, "Institutional Knowledge at Singapore Management University SOA maturity influence on digital banking transformation SOA maturity transformation," *IDRBT J. Bank. Technol.*, 2018.

[6] R. Nalini, G. Sashi Kala, S. Prakash, A. Varghese Joseph, and R. Alamelu, "Digital Payments-Embellishing Customer Experience," in *7th IEEE International Conference on Computation of Power, Energy, Information and Communication, ICCPEIC 2018*, 2018. doi: 10.1109/ICCPEIC.2018.8525226.

[7] D. Additional *et al.*, "Distressed Asset Transfer Handbook: General Guidelines for the Purchase and Sale of Distressed Assets in the Financial Sector," *Financ. Stab. Board*, 2018.

[8] L. Lynch *et al.*, "The Marlboro Man As A 20th-Century David - A Philosophical Inquiry Into The Aristotelian Aesthetic Of Advertising," *J. Prod. Innov. Manag.*, 2018.

[9] R. Palomo Zurdo, Y. Fernandez Torres, and M. Gutierrez Fernandez, "Cooperative banking and digital transformation: towards a new relationship model with members and clients," *REVESCO-REVISTA Estud. Coop.*, 2018.

[10] Anonymous, "Payments Trends to Watch in 2019," *Am. Bankers Assoc. ABA Bank. J.*, 2018.

CHAPTER 11

INVESTIGATION ON THE CONCEPT OF CYBERSECURITY IN DIGITAL BANKING

Shefalika Narain, Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- shefalika.narain@atlasuniversity.edu.in

ABSTRACT:

The examination of cybersecurity in digital banking explores the essential tactics and procedures needed to safeguard financial organizations from ever-more-advanced cyberattacks. The increasing prevalence of digital banking systems has made it more important than ever to protect sensitive financial data and ensure transaction integrity. This research looks at intrusion detection systems, multi-factor authentication, and encryption as important components of cybersecurity in the context of digital banking. It looks at the several kinds of cyberthreats that are common in the sector, including malware, phishing, and insider threats, as well as the legal frameworks that control cybersecurity procedures. The study emphasizes the value of incident response plans, preventative measures, and cutting-edge technology like blockchain and artificial intelligence in boosting security. The research intends to provide insights into how financial institutions may successfully traverse the changing cybersecurity environment and secure the safety of their digital assets and client information by examining existing practices and upcoming developments.

KEYWORDS:

Compliance, Encryption, Incident Response, Multi-Factor Authentication, Phishing.

INTRODUCTION

The visual components and design of a digital banking platform that allows users to engage with the system are referred to as the user interface (UI). It consists of elements like menus, forms, buttons, icons, and general visual design. The creation of an interface that is aesthetically pleasing, practical, and simple to use is the main objective of UI design. Users may easily access and carry out a variety of banking tasks, including checking balances, moving money, paying bills, and obtaining account information when user interface design is done well. User Experience (UX) refers to the whole user experience that a user experiences from the moment they first enter a digital banking platform until they finish activities. To produce a smooth and fulfilling platform interaction, UX design places a strong emphasis on understanding user demands, habits, and preferences [1], [2]. It includes components including user flow, accessibility, usability, and the design's emotional effect. A well-designed user experience (UX) guarantees that users will find the platform easy to use, efficient, and fun, which will increase user happiness and engagement.

One of the core tenets of UI and UX design that has a big influence on user experience is intuitive navigation. It speaks to how simple it is for customers to locate and use the features or information they want on a digital banking platform. Because intuitive navigation offers a logical and unambiguous framework for users to follow, it reduces cognitive strain and frustration. An intuitive layout is necessary for navigation that is straightforward and consistent [3], [4]. Content and services should be arranged in a manner that is consistent with users' expectations and mental models. Users may become more comfortable and confident while navigating the site thanks to consistency in the layout, language, and design aspects. For example, usability may be improved by putting frequently used features, such as account

balances and transaction histories, in places that are simple to find. For efficient navigation, a hierarchical structure that is well-organized is essential. Digital banking systems have to use a logical structure that combines information and services that are connected. While auxiliary activities, like settings and assistance, should be accessible but less noticeable, primary operations, such as account management and transfers, should be presented. Users can more easily explore a platform and comprehend the relationships between various pieces when it is designed hierarchically.

By enabling users to find certain information or functions quickly, search and filtering features improve navigation. With the ability to modify and categorize data depending on user choices, a strong search tool should provide precise and pertinent results based on user queries. Users should be able to filter account statements by date range or look up transaction data, for instance The digital banking platform will adjust to varied screen sizes and devices thanks to responsive design, which guarantees a consistent and user-friendly experience across a range of devices [5], [6]. Flexible layouts, scaled photos, and media queries are some of the techniques used by responsive design principles to make sure that the platform works well on PCs, tablets, and smartphones. For consumers who access their accounts from numerous devices, this versatility is essential. The user experience and consumers' opinions of the digital banking platform are greatly shaped by aesthetics. In addition to increasing user engagement, a visually appealing design upholds the platform's credibility and corporate identity.

Arranging design components in a visual hierarchy helps consumers focus on key information and is a good way to steer their attention. Effective use of size, color, contrast, and positioning allows designers to draw attention to important features and messages. To attract customers' attention and make them quickly accessible, conspicuous buttons for important activities, such as "Transfer Funds" or "Pay Bill," should stand out via size and color contrast. A unified and identifiable user experience depends on maintaining brand consistency. The brand's identity should be reflected in the digital banking platform via the constant usage of graphics, fonts, colors, and logos. By ensuring that consumers identify the platform with the institution's broader brand image, brand consistency contributes to the development of trust and familiarity. A clean and intuitive interface is a result of design simplicity and clarity [7], [8]. Users can explore and engage with the platform more easily when a minimalist approach is used since it minimizes visual clutter and concentrates on key components. Users can focus on their jobs and avoid needless distractions with the aid of a clear and simple design.

Inclusion and accessibility are important factors in UI and UX design. Digital banking systems must be made to work with a range of user abilities, such as those involving motor, visual, or hearing impairments. The platform is made accessible to all users with the help of features like keyboard navigation, screen reader compatibility, and high-contrast options. The UI and UX of digital banking systems may be refined and improved with the help of usability testing and user input. Real users are used in usability testing, which helps designers find possible problems and opportunities for improvement [9], [10]. User feedback offers insightful information about their preferences, experiences, and problems. You may utilize a variety of user testing techniques, including focus groups, A/B testing, and usability studies, to get input and assess the efficacy of design aspects. An A/B test examines several design changes to see which works better, while usability studies watch people as they use the platform. Focus groups provide qualitative information about the opinions and experiences of people.

In an iterative design approach, the design is continually improved and refined in response to user input and testing outcomes. Iterative approaches are best for addressing problems found, testing new features, and improving the user experience overall for designers. Consistent enhancements and modifications guarantee that the platform maintains its focus on the user

and adapts to changing requirements. Users' general level of happiness and engagement with the digital banking platform is influenced by the design's emotional effect. A satisfying emotional experience builds platform trust and a feeling of connection while also increasing user loyalty. The goal of positive emotional design is to provide people with a joyful and engaging experience. The positive emotional effect is facilitated by elements like interactive features, welcoming language, and captivating graphics. For instance, customers' emotional connection with the platform may be strengthened by sending them customized greetings and congratulations for achieving milestones like saving a certain amount of money.

DISCUSSION

Strategies like gamification and incentives may improve user motivation and engagement. The digital banking experience may be enhanced by adding gamified components like challenges, badges, and incentives. For example, banks may provide incentives for finishing courses on financial literacy or hitting savings targets. Developing openness and trust is crucial to making a strong emotional impression. The design needs to communicate security measures, privacy rules, and customer support alternatives straightforwardly and reliably. Users who engage with the platform with confidence benefit from transparent design approaches.

By creating a smooth and linked experience, integration with other services improves the user experience overall. To provide a full solution, digital banking systems must be integrated with a range of financial services, tools, and third-party apps. Integration with financial management tools gives consumers a comprehensive picture of their financial condition, including investing platforms and budgeting applications. Banks may provide services that let customers monitor their spending, connect other accounts, and create financial objectives. The value and utility of the platform are increased by this integration. Financial transactions are streamlined by integration with payment and transfer services, such as bill payment systems and peer-to-peer payment platforms. It should be unnecessary for users to move between several applications or services to make payments and transfers inside the digital banking platform.

By making help easily accessible, customer support capabilities integrated into the digital banking platform improve the user experience. Users can easily get assistance and fix problems thanks to features like live chat, in-app messaging, and help centers. New trends and developments in technology will influence the direction of UI and UX design in digital banking. For banks and other financial institutions to continue offering their customers great experiences, they will need to keep up with these advances. The use of machine learning and artificial intelligence By allowing customized and predictive interactions, artificial intelligence (AI) and machine learning (ML) are revolutionizing user interface and user experience (UI) design. While ML algorithms may give customized suggestions and insights based on user behavior and preferences, AI-driven chatbots and virtual assistants can provide real-time help and assistance.

Voice user interfaces, or VUIs, are becoming more and more popular as a practical hands-free way to communicate with digital financial systems. Through speech interactions, customers may access account information, do banking operations, and obtain support thanks to voice commands and voice recognition technologies. With their immersive and interactive qualities, augmented reality (AR) and virtual reality (VR) have the potential to completely transform digital banking experiences. While virtual reality (VR) may build virtual banking settings for better user engagement, augmented reality (AR) can give visual overlays of financial data and account details.

As more and more banking services are provided online in the digital era, cybersecurity has emerged as a top priority for financial organizations. The way financial transactions are carried

out has been completely transformed by the incorporation of cutting-edge technology into digital banking, which provides previously unheard-of ease and efficiency. But this change has also made banks and their clients more vulnerable to a wide range of cyberattacks, which calls for strong security protocols to safeguard private data and preserve confidence. In digital banking, cybersecurity refers to a wide variety of procedures, tools, and approaches that are used to protect financial systems against fraud, theft, unauthorized access, and other hostile activity.

The dynamic and complex nature of cyber threats, including ransomware, phishing, malware, denial-of-service (DoS) assaults, and advanced persistent threats (APTs), has prompted the growth of cybersecurity in digital banking. Phishing attacks are still a common concern since they include tricking people into disclosing personal information by impersonating trustworthy organizations.

These assaults utilize social engineering strategies to trick people into divulging private information, including login passwords or bank account information. Malware, such as trojans, spyware, and viruses, also compromises data integrity by entering systems and posing serious hazards. Attacks utilizing ransomware, in which the perpetrator encrypts data and demands payment to unlock it, are becoming more commonplace. They cause significant disruptions to systems and result in large financial losses. Attacks known as denial-of-service (DoS) attempt to overload systems with excessive traffic to prevent services from operating and interfere with user access. Advanced persistent threats are persistent, highly focused attacks on systems that are often used for espionage or data exfiltration.

Financial institutions use a variety of security frameworks and best practices to strengthen their defenses in the face of these always-changing threats. Notable frameworks include the International Organization for Standardization (ISO) 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. An organized method for recognizing, safeguarding against, detecting, reacting to, and recovering from cyber events is offered by the NIST Cybersecurity Framework. Banks may create thorough security policies, carry out risk analyses, put in place the necessary controls, and regularly analyze and enhance their security posture by adhering to this framework. To help banks properly manage and safeguard sensitive data, ISO 27001 provides principles for creating, implementing, maintaining, and continuously improving information security management systems (ISMS).

Risk management, which includes the detection, evaluation, and mitigation of possible risks and vulnerabilities, is an essential part of cybersecurity in digital banking. Banking systems' security posture is assessed using risk assessment techniques including threat modeling, penetration testing, and vulnerability scanning. Vulnerability scans pinpoint vulnerabilities that an attacker potentially exploits, while penetration testing replicates actual assaults to evaluate how well security measures work. Threat modeling includes identifying risks, addressing them, and creating methods to counter possible attack vectors. Risk management strategies, such as risk acceptance, risk sharing, risk avoidance, and risk reduction, assist banks in allocating resources efficiently and prioritizing security measures.

Technological solutions, which cover different areas of data protection, threat detection, access control, and incident response, are essential to improving cybersecurity in digital banking. A key piece of technology that guarantees data integrity and secrecy while it's in transit is encryption. Sensitive data is shielded from unwanted access via encryption, which uses cryptographic techniques to transform data into an unreadable format. The protocols Secure Socket Layer (SSL) and Transport Layer Security (TLS) are often used in online interactions

to protect user data submitted to banking servers. In the case of a data breach, encrypted stored data including client information and transaction records offers an extra degree of security.

Another important technology that improves access security is multi-factor authentication (MFA), which requires users to give numerous forms of verification before they can access their accounts. Multi-factor authentication (MFA) often combines three factors: the user's knowledge (like a password), their possession (like a mobile device), and their identity (like biometric information).

Biometric authentication, such as fingerprint or face recognition, SMS or email verification codes, and one-time passwords (OTPs) are examples of common multi-factor authentication techniques. The possibility of unwanted access and account breach is greatly decreased with MFA.

To identify any threats and prevent unauthorized access, network traffic must be monitored and controlled by firewalls and intrusion detection systems (IDS). In their role as barriers between internal networks and outside sources, firewalls filter traffic according to pre-established rules and prevent harmful or questionable activities. To detect and notify users of possible security issues, such as unauthorized access attempts or unusual patterns suggestive of a cyberattack, intrusion detection systems (IDS) examine network traffic and system activity. Systems for managing security information and events (SIEMs) provide centralized cybersecurity event monitoring, analysis, and response capabilities. To detect and react to any threats instantly, SIEM systems collect and correlate data from several sources, including network logs, security devices, and apps. With SIEM systems, banks may take a proactive approach to threat management by using them to identify abnormalities, produce warnings, and perform forensic investigations.

Endpoint security solutions are aimed at protecting PCs, tablets, and smartphones from online dangers. Endpoint detection and response (EDR) systems, antivirus software, and anti-malware technologies are some of these solutions. Malicious programs are detected and eliminated by antivirus software, but anti-malware technologies provide extra defense against other kinds of threats. Advanced features for identifying, looking into, and addressing endpoint-based assaults are provided by EDR systems.

A crucial component of cybersecurity in digital banking is regulatory compliance, which makes sure that financial organizations follow certain norms and procedures. Respecting rules and guidelines helps safeguard client information, maintain confidence, and prevent negative legal and financial effects. The General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX), and the National Institute of Standards and Technology (NIST) recommendations are important laws and standards that are pertinent to digital banking. The General Data Protection Regulation (GDPR) lays down specifications for gathering, using, and keeping personal data. It also covers data security, consent, and breach reporting. While SOX establishes guidelines for financial reporting and internal controls, PCI DSS offers security standards for safeguarding credit card information and averting data breaches. NIST standards guide managing cybersecurity risks and safeguarding information systems.

Emerging trends and technology will affect cybersecurity in digital banking going forward, presenting both benefits and difficulties. Increasingly, cybersecurity is being improved via the use of artificial intelligence (AI) and machine learning (ML), which analyze vast amounts of data, see trends and spot abnormalities that might be signs of possible attacks. With the use of these technologies, banks may increase accuracy, automate danger detection, and more quickly address new risks. Blockchain technology, which is renowned for being decentralized and

unchangeable, offers safe and transparent transaction records, which might be used to improve cybersecurity. With implications for encryption techniques, quantum computing is a breakthrough in processing capacity. Banks are investigating quantum-resistant encryption techniques in anticipation of the effects of quantum computing on data security.

Regardless of whether users or devices are within or outside the network perimeter, zero trust architecture is an emerging cybersecurity concept that operates under the assumption that there is no trust by default. Strict access constraints, resource segregation, and ongoing user and device verification are all part of the zero trust concepts. To improve security and reduce the possibility of insider threats and illegal access, banks are using zero-trust strategies.

CONCLUSION

The examination of cybersecurity in online banking highlights the vital need for strong security protocols to shield financial institutions from constantly changing cyber threats. The security of sensitive data and transactions is becoming more and more difficult to ensure as digital banking grows. Encryption, multi-factor authentication, and extensive intrusion detection systems are essential cybersecurity techniques that are necessary to protect against threats including malware, phishing, and insider assaults. Ensuring that institutions satisfy basic criteria for securing client data and forming security procedures is largely dependent on regulatory compliance, which is fueled by frameworks like PCI-DSS and GDPR. To minimize harm and recover from security breaches, effective incident response planning and post-event analysis are essential. While emerging technologies like blockchain and artificial intelligence have the potential to improve cybersecurity, they also bring with them new difficulties. Financial institutions have to always update their security plans to counter new and emerging threats. Through the implementation of proactive security measures, adherence to regulatory standards, and use of cutting-edge technology, financial institutions may fortify their barriers and preserve client confidence in an ever-digitalizing society.

REFERENCES:

[1] K. S. Deeparani and B. Jeya Prabha, “Digital financial services: Role of cyber security for digital india,” *Int. J. Mech. Prod. Eng. Res. Dev.*, 2018.

[2] A. Pilishvili, “The Impact of a digital platform on the financial corporation in modern Russia,” *Espacios*, 2018.

[3] E. Pauwels and S. W. Denton, “Searching for Privacy in the Internet of Bodies.,” *Wilson Q.*, 2018.

[4] T. P. Novak, “Advocacy banking is at the heart of emerging tech: Incorporating emerging technology into the credit union space.,” *J. Digit. Bank.*, 2018.

[5] C. Biancotti and P. Ciocca, “Dry Rivers, Scary Strangers: Are Financial And Cyber Crises Alike?,” *Mil. Cyber Aff.*, 2018, doi: 10.5038/2378-0789.3.2.1061.

[6] N. Pokrovskaia, T. Khansuvarova, and R. Khansuvarov, “Network decentralized regulation with the fog-edge computing and blockchain for business development,” in *Proceedings of the 14th European Conference on Management, Leadership and Governance, ECMLG 2018*, 2018.

[7] A. K. Kibet, D. Gebresenbet Bayyou, R. Esquivel, D. G. Bayyou, and R. A. Esquivel, “Blockchain: It’S Structure, Principles, Applications and Foreseen Issues,” *J. Emerg. Technol. Innov. Res.*, 2019.

[8] C. A. T. Almeida and L. R. Herrera, "La ciberseguridad en el ecuador, una propuesta de organización," *Rev. Ciencias Segur. y Def.*, 2019.

[9] K. Digrazia, "Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach," *J. Bus. Technol. Law*, 2018.

[10] P. Singh and R. S. Rajput, "Cybersecurity Analysis in the context of Digital Wallets," *Int. J. Adv. Stud. Sci. Res.*, 2018.

CHAPTER 12

EXPLORATION OF THE ROLE OF DATA ANALYTICS IN DIGITAL BANKING

Suresh Kawitkar, Professor
ISME, ATLAS SkillTech University, Mumbai, India
Email id- suresh.kawitkar@atlasuniversity.edu.in

ABSTRACT:

The examination of data analytics' function in digital banking demonstrates how revolutionary it is for financial organizations. Data analytics makes use of both historical and current data to optimize operations, improve consumer experiences, and strengthen decision-making. This research looks at the several kinds of data analytics, including diagnostic, prescriptive, predictive, and descriptive analytics, and how they are used in banking. It emphasizes how effective risk management, individualized banking services, and fraud detection are all made possible by data analytics. The research also looks at data-gathering procedures, management strategies, and the incorporation of cutting-edge technology like machine learning and artificial intelligence. The goal of the research is to provide insights into how financial institutions may use data analytics to spur development and maintain a competitive advantage in the rapidly changing digital market by examining successful case studies and best practices.

KEYWORDS:

Analytics, Data Management, Fraud Detection, Personalization, Risk Management.

INTRODUCTION

The idea of cybersecurity in digital banking is crucial in today's financial environment because it emphasizes the vital necessity to safeguard private financial data and guarantee the security and integrity of online transactions. The emergence of digital banking has brought about a transformation in the financial sector by offering clients an unparalleled level of ease and availability. To protect their operations and client data, financial institutions now face a wide range of cybersecurity risks brought about by this digital transition. In digital banking, cybersecurity refers to a wide range of procedures, tools, and approaches used to ward against a constantly changing variety of online dangers [1], [2]. These dangers to digital banking systems include ransomware, phishing attempts, malware, advanced persistent threats (APTs), and denial-of-service (DoS) assaults.

Phishing attacks include the fraudulent solicitation of personal data, including financial information, usernames, and passwords, by disguising themselves as official correspondence from reliable sources. These assaults use social engineering strategies to trick people into disclosing personal information, which often results in account access being gained without authorization and monetary losses [3], [4]. As a result, digital banking companies put in place safeguards against phishing, such email filtering, user education, and sophisticated authentication methods. Another serious risk comes from malware, which compromises data integrity by invading systems and manifesting as viruses, trojans, and spyware. Numerous platforms, such as hacked software, rogue websites, and email attachments, may spread malware. Using intrusion detection systems to find and eliminate malware, installing antivirus software, and updating systems often are all examples of effective defenses.

Attacks using ransomware have become more well-known as a serious risk to online financial systems. Cybercriminals encrypt important data in these assaults and demand a ransom to unlock it, interrupting business operations and perhaps resulting in significant financial losses.

To counteract ransomware, financial institutions need to establish comprehensive backup and recovery plans, enforce stringent access restrictions, and educate staff members on safe computing procedures and ransomware threats. Attacks known as denial-of-service (DoS) attempt to overload systems with excessive traffic, which may interfere with the availability of services and affect users' ability to use digital banking platforms. Banks use traffic monitoring systems, firewalls, and load balancers all of which are capable of identifying and thwarting denial-of-service attacks to reduce this risk [5], [6]. APTs, or advanced persistent threats, are a more advanced and focused kind of cyberattack. APTs include persistent, covert attempts by attackers to get unauthorized access to systems, sometimes with the intention of espionage or data exfiltration. To identify and counter possible attacks before they have a substantial impact, combating sophisticated Persistent attacks (APTs) requires a mix of proactive threat information, ongoing monitoring, and sophisticated threat detection technology.

Putting strong security guidelines and best practices into place is a necessary part of a complete cybersecurity strategy for digital banking. A systematic method for handling cybersecurity threats is offered by the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which includes the steps of identifying, protecting, detecting, reacting, and recovering. Banks may create and enforce security policies, carry out risk analyses, put security controls in place, and constantly review and enhance their cybersecurity posture by using this framework. The International Organization for Standardization (ISO) 27001, which lays out specifications for creating, putting into practice, maintaining, and continuously enhancing information security management systems (ISMS), is another crucial framework. By putting in place the necessary security measures, banks may successfully handle and safeguard sensitive information when they comply with ISO 27001.

Risk management, which includes the detection, evaluation, and mitigation of possible risks and vulnerabilities, is a crucial part of cybersecurity in digital banking. Banks use techniques like threat modeling, penetration testing, and vulnerability scanning to do risk assessments. Whereas penetration testing mimics actual assaults to evaluate the efficacy of security precautions, vulnerability scans find holes in systems that attackers may exploit [7], [8]. Threat modeling includes identifying risks, addressing them, and creating methods to counter possible attack vectors. To efficiently allocate resources and prioritize security activities, banks also use risk management approaches including risk acceptance, risk sharing, risk avoidance, and risk reduction.

Improving cybersecurity in digital banking is mostly dependent on technological solutions. A key piece of technology that guarantees data integrity and secrecy while it's in transit is encryption. By converting data into an unintelligible format, encryption methods shield it from unwanted access. Online connections are often secured using the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols, and data that has been encrypted is protected in the case of a data breach. By forcing users to provide several forms of verification before gaining access to their accounts, multi-factor authentication, or MFA, improves access security. Multi-factor authentication (MFA) often combines three factors: the user's knowledge (like a password), their possession (like a mobile device), and their identity (like biometric information). Biometric authentication, such as fingerprint or face recognition, SMS or email verification codes, and one-time passwords (OTPs) are examples of common multi-factor authentication techniques. The possibility of unwanted access and account breach is greatly decreased with MFA.

To identify possible threats and prevent unauthorized access to networks, firewalls and intrusion detection systems (IDS) are essential tools for monitoring and managing network traffic. As barriers between internal networks and outside sources, firewalls filter traffic

according to preset rules and stop harmful activities. To detect and notify users of possible security issues, such as unauthorized access attempts or unusual patterns suggestive of a cyberattack, intrusion detection systems (IDS) examine network traffic and system activity [9], [10]. Systems for managing security information and events (SIEMs) provide centralized cybersecurity event monitoring, analysis, and response capabilities. To detect and react to any threats instantly, SIEM systems collect and correlate data from several sources, including network logs, security devices, and apps. With SIEM systems, banks may take a proactive approach to threat management by using them to identify abnormalities, produce warnings, and perform forensic investigations.

DISCUSSION

Solutions for endpoint security concentrate on shielding specific machines from online dangers. Endpoint detection and response (EDR) systems, antivirus software, and anti-malware technologies are some of these solutions. Malicious programs are detected and eliminated by antivirus software, but anti-malware technologies provide extra defense against other kinds of threats. Advanced features for identifying, looking into, and addressing endpoint-based assaults are provided by EDR systems. A crucial component of cybersecurity in digital banking is regulatory compliance, which makes sure that financial organizations follow certain norms and procedures. Respecting laws like the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), and the General Data Protection Regulation (GDPR) helps safeguard consumer data, maintain confidence, and prevent negative legal and financial effects. The General Data Protection Regulation (GDPR) lays down specifications for gathering, using, and keeping personal data. It also includes clauses on data security and breach reporting. While SOX establishes guidelines for internal controls and financial reporting, PCI DSS offers security standards for safeguarding credit card information. Adherence to these requirements guarantees banks maintain strong security protocols and protect confidential data.

Emerging trends and technology are shaping the future of cybersecurity in digital banking, presenting both possibilities and difficulties. Increasingly, cybersecurity is being improved via the use of artificial intelligence (AI) and machine learning (ML), which analyze vast amounts of data, see trends and spot abnormalities that might be signs of possible attacks. With the use of these technologies, banks may increase accuracy, automate danger detection, and more quickly address new risks. Blockchain technology, which is renowned for being decentralized and unchangeable, offers safe and transparent transaction records, which might be used to improve cybersecurity. With implications for encryption techniques, quantum computing is a breakthrough in processing capacity. Banks are investigating quantum-resistant encryption techniques in anticipation of the effects of quantum computing on data security. A new cybersecurity paradigm called "zero trust architecture" segmented resources, tightly controlled access, and ongoing user and device verification. It assumes no trust by default. To improve security and reduce the possibility of insider threats and illegal access, banks are using zero-trust strategies.

Analytics has become a disruptive force in the banking industry, radically changing the way financial institutions function and engage with their clientele. Advanced analytics has transformed decision-making procedures, increased operational effectiveness, and greatly enhanced client experiences in banking operations. This shift is fueled by analytics' capacity to extract useful information from massive data sets, allowing banks to make more deliberate and well-informed choices. Data analytics, which is the methodical analysis of data sets to find patterns, correlations, and trends that guide decision-making, is at the center of this revolution. The amount, diversity, and velocity of data that banks have access to has greatly increased with the introduction of big data. Real-time access to transactional data, client interactions, social

media activity, and market trends gives banks a plethora of information they can use to their advantage. Banks are now better equipped to examine and understand this data thanks to advanced analytics methods like AI, machine learning, and predictive analytics.

One of the main instruments influencing the change in banking procedures is predictive analytics. Forecasting future trends and behaviors based on past data is made possible for banks by predictive analytics, which uses statistical algorithms and machine learning methods. For instance, by examining past borrowing trends, repayment patterns, and other financial data, banks might utilize predictive models to spot possible credit problems. As a result, there is a decreased chance of default and an improvement in the performance of the credit portfolio as a whole. This also enables more precise risk assessment and educated lending choices.

Predictive analytics is also essential for personalizing and segmenting customers. Banks may divide their clientele into several categories according to demographics, past transactions, and behavior by analyzing consumer data. Banks may customize their services and communications to each client segment's unique requirements and preferences thanks to this segmentation. To increase engagement and conversion rates, for example, tailored marketing campaigns may be created to target consumers with relevant goods and services. Predictive analytics may also assist banks in anticipating client requirements and offering proactive solutions, such tailored financial guidance or suggested products.

AI and machine learning are also crucial in changing banking procedures. Compared to previous approaches, these technologies allow banks to handle and analyze massive amounts of data more accurately and efficiently. By seeing intricate patterns and connections in data that aren't always obvious, machine learning algorithms may provide us with a better understanding of consumer behavior, industry trends, and operational efficiency. Artificial intelligence (AI)-enabled chatbots and virtual assistants, for instance, may manage consumer transactions and questions, offering real-time help and improving the entire customer experience. Additionally, these technologies allow banks to automate repetitive processes like fraud detection and transaction processing, freeing up resources for more strategic endeavors.

Analytics has also had a big influence on the identification and prevention of fraud. Sophisticated fraudsters might readily circumvent the manual procedures and static rules that were often the foundation of traditional fraud detection techniques. On the other hand, analytics offers a more flexible and dynamic method of fraud detection. Through the examination of transaction patterns, behavioral abnormalities, and past fraud data, financial institutions may promptly detect questionable activity and take more efficient action. With the capacity to continually learn from fresh data, machine learning algorithms can identify new fraud schemes with greater accuracy and fewer false positives.

Applying analytics significantly improves operational efficiency. Data-driven insights may help banks increase overall performance, enhance resource allocation, and reduce procedures. Analytics, for example, may assist banks in identifying operational bottlenecks, such as slow loan processing times or ineffective customer care. Banks can save expenses, increase customer happiness, and improve operational efficiency by solving these problems. Analytics may also help with strategic decision-making by offering perceptions of competition positioning, market trends, and expansion prospects. This enables banks to decide on product development, market growth, and investment plans with more knowledge. The usage of analytics has greatly enhanced the customer experience. Banks may use data to better understand the interests, habits, and problems of their customers. They can provide more relevant and customized consumer experiences as a result. For instance, analytics may assist banks in identifying typical client complaints and streamlining their operations to more successfully resolve these

problems. To ensure that digital banking platforms such as mobile applications and online banking interfaces meet client expectations and provide a flawless user experience, data-driven insights may also be utilized to improve them.

Better risk management is also made possible by the use of analytics in banking procedures. Banks can detect possible risks and weaknesses, such shifts in consumer behavior or changes in economic circumstances, by examining historical data and market patterns. This enables banks to create more effective risk management plans and make well-informed choices on risk reduction. Analytics may also help with regulatory compliance by offering insights into things like know-your-customer (KYC) and anti-money laundering (AML) regulations. Data may be used by banks to track and examine transactions, spot questionable activity, and make sure rules are being followed.

The creation of cutting-edge financial services and solutions is another indication of how analytics is revolutionizing banking operations. Banks may create innovative and customized financial products by using data-driven insights to detect emerging trends and consumer demands. Based on consumer information and preferences, banks may, for instance, create unique loan products, individualized investment portfolios, and creative payment methods. This gives banks a competitive advantage in the market and improves the value offered to clients. Notwithstanding the many advantages of analytics in banking, banks nevertheless need to take certain issues and concerns into account. Since the collecting and processing of sensitive consumer data necessitates strict safeguards against unauthorized access and breaches, data privacy and security are critical considerations. To secure consumer data, banks must employ strong security measures and make sure that data protection laws are followed. In addition, the business must acquire the necessary skills and competencies and foster a culture of data-driven decision-making to successfully integrate analytics into banking procedures.

By giving banks the instruments and insights they need to better decision-making, operational efficiency, and customer experience, analytics has completely changed the way banks do business. Banks can improve procedures, reduce risks, and get a deeper understanding of client behavior by using AI, machine learning, and predictive analytics. While there are issues with data security and privacy that need to be resolved, analytics has several advantages in banking that spur innovation and provide businesses with a competitive edge in the always-changing financial sector. The use of analytics in banking is anticipated to rise as technology develops, presenting new chances for development and change.

Customer insights and personalization are now essential for creating a competitive advantage and improving the customer experience in the world of digital banking. The capacity to customize services and interactions to meet the unique demands of each consumer is changing the way banks deal with their customers. The increasing availability of data and sophisticated analytics tools, which allow banks to glean valuable insights from consumer interactions and behavior, are the driving forces behind this shift. The profound comprehension of a client's preferences, actions, and requirements that comes from examining data gathered from several touchpoints is referred to as customer insights. Digital banking systems provide a multitude of data that may be used to create a detailed profile of each client, including browsing habits, transaction histories, and interaction patterns. Banks may learn a great deal about the unique spending patterns, financial objectives, and preferences of their customers by using this data. A significant benefit of using client data in digital banking is the capacity to provide incredibly customized experiences. Customizing goods, services, and communications to each unique customer's requirements and preferences is known as personalization. Banks, for instance, may provide targeted marketing efforts, tailored product suggestions, and individualized financial advice by using data-driven insights. Banks can increase client pleasure, foster loyalty, and

promote engagement by tailoring their services to their preferences. By predicting future requirements and behaviors based on previous data, predictive analytics is essential to consumer customization. Predictive algorithms, for example, may determine which consumers, based on their transaction history and financial trends, are most likely to need a mortgage or personal loan. This enables banks to provide relevant goods and services to clients before they ever communicate their demands. Additionally, predictive analytics may be used to foresee possible problems. For example, it can be used to identify clients who could be in danger of loan default and provide them with specialized assistance or intervention.

Another crucial component of customization in digital banking is customer segmentation. Banks may develop tailored strategies for each set of clients by dividing them into various categories according to criteria like financial objectives, transaction behavior, and demographics. A bank may, for instance, divide up its clientele into categories like young professionals, seniors, and proprietors of small businesses. Following that, each section may get messages and product offers that are customized for their unique requirements and phases of life. By concentrating resources on the most promising client categories, this strategy not only increases the relevance of the bank's offers but also boosts the effectiveness of marketing initiatives.

Personalization is further enhanced by machine learning and artificial intelligence (AI), which allow banks to examine large, complicated data sets and spot trends that would not be visible with conventional approaches. Large volumes of data may be processed in real-time by AI algorithms, which can then provide insights to customize suggestions and client interactions. AI-driven chatbots, for instance, can evaluate consumer inquiries and provide tailored answers according to the user's preferences and past interactions. In a similar vein, transaction data analysis using AI may reveal spending patterns and provide tailored financial advice or warnings. Customer service is included in the customization that is included in digital banking. Real-time communication and assistance are possible via digital channels including internet platforms and mobile applications. Features like responsive chatbots, customized account management tools, and customized alerts may all be used to provide personalized customer assistance. Banks may improve the general customer experience and forge closer bonds with their customers by offering tailored assistance.

As digital banking becomes more personalized, data security and privacy become more important factors to take into account. Banks must make sure that the massive volumes of consumer data they gather and analyze are safe from intrusions and breaches. Encryption and multi-factor authentication are two strong security measures that must be used to protect client data and maintain confidence. To guarantee that client data is handled properly and openly, banks must also abide by data protection laws, such as the General Data Protection Regulation (GDPR). Personalization and consumer information provide several advantages in digital banking. Banks can improve customer happiness, engagement, and loyalty by using data to identify and address the unique requirements of each client. Banks may set themselves apart in a crowded market by providing consumers with memorable, relevant experiences via personalization. Financial institutions' performance will be largely determined by their capacity to use consumer information and provide tailored experiences as digital banking develops.

CONCLUSION

In digital banking, data analytics plays a critical role in transforming the way financial institutions function and engage with their clientele. Banks may provide more individualized and focused services by using data analytics to get deeper insights into the preferences, habits, and trends of their customers. Banks may increase operational efficiency, reduce risks, and

make better decisions by using descriptive, diagnostic, predictive, and prescriptive analytics. Specifically, prescriptive analytics offers practical suggestions for strategy optimization, while predictive analytics helps predict client demands and possible hazards. The amalgamation of cutting-edge technology like artificial intelligence and machine learning augments the potential of data analytics, hence permitting more precise fraud identification and improved consumer satisfaction. To properly use data analytics, however, several issues like data quality, privacy, and regulatory compliance need to be resolved. Robust data management procedures, well-defined goals, and constant trend adaption are necessary for the successful use of data analytics techniques. The financial services sector will need the strategic use of data analytics to drive innovation, enhance client happiness, and sustain a competitive edge as digital banking continues to develop.

REFERENCES:

[1] C. Lehrer, A. Wieneke, J. vom Brocke, R. Jung, and S. Seidel, "How Big Data Analytics Enables Service Innovation: Materiality, Affordance, and the Individualization of Service," *J. Manag. Inf. Syst.*, 2018, doi: 10.1080/07421222.2018.1451953.

[2] J. Marous, "Five Innovation Trends That Will Define Banking in 2019," *Financ. Brand Newsl.*, 2018.

[3] R. Balica, "Big data learning analytics and algorithmic decision-making in digital education governance," *Anal. Metaphys.*, 2018, doi: 10.22381/AM1720187.

[4] D. M. S. Dashrathrao, "Trends and Challenges of ICT in Indian Banking Sector," *Int. J. Trend Sci. Res. Dev.*, 2018, doi: 10.31142/ijtsrd18692.

[5] R. K. Behera, A. K. Sahoo, and C. Pradhan, "Big Data Analytics in Real Time - Technical Challenges and its Solutions," in *Proceedings - 2017 International Conference on Information Technology, ICIT 2017*, 2018. doi: 10.1109/ICIT.2017.39.

[6] M. Nawaz, L. Motiwalla, and A. V. Deokar, "Usage-Driven Personalized Mobile Banking Application," 2018. doi: 10.1145/3209626.3209736.

[7] R. Chellam, "Econ 4.0: How big is big data?," The Edge Malaysia.

[8] M. B. Fox, L. Glosten, and G. Rauterberg, *Palgrave Studies in Digital Business & Enabling Technologies*. 2018.

[9] E. Indriasari, F. L. Gaol, and T. Matsuo, "Digital Banking Transformation: Application of Artificial Intelligence and Big Data Analytics for Leveraging Customer Experience in the Indonesia Banking Sector," in *Proceedings - 2019 8th International Congress on Advanced Applied Informatics, IIAI-AAI 2019*, 2019. doi: 10.1109/IIAI-AAI.2019.00175.

[10] C. Giebe, L. Hammerström, and D. Zwerenz, "Big Data & Analytics as a sustainable Customer Loyalty Instrument in Banking and Finance," *Financ. Mark. Institutions Risks*, 2019, doi: 10.21272/fmir.3(4).74-88.2019.