SOFTWARE SYSTEMS AND CONTEMPORARY APPLICATIONS

Dr. G. Shanmugarathinam
Dr. Zafar Ali Khan N

BOOKS ARCADE

Software Systems and Contemporary Applications

Software Systems and Contemporary Applications

Dr. G. Shanmugarathinam

Dr. Zafar Ali Khan N

BOOKS ARCADE
KRISHNA NAGAR, DELHI

Software Systems and Contemporary Applications

Dr. G. Shanmugarathinam
Dr. Zafar Ali Khan N

This book contains information obtained from highly regarded resources. Copyright for individual articles remains with the authors as indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

BOOKS ARCADE
Regd. Office:
F-10/24, East Krishna Nagar, Near Vijay Chowk, Delhi-110051
Ph. No: +91-11-79669196, +91-9899073222
E-mail: info@booksarcade.co.in, booksarcade.pub@gmail.com
Website: www.booksarcade.co.in

Year of Publication 2023

International Standard Book Number-13: 978-81-19199-15-0

CONTENTS

CHAPTER-1

INTERNET OF TRANSPORTATION SYSTEMS

Dr. G. Shanmugarathinam
Professor & HOD, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: shanmugarathinam@presidencyuniversity.in

A rise in the use of AVs has recently occurred and businesses are paying close attention to AVs. While the potential benefits of AVs for the transportation industry are quite promising, security and privacy issues pose additional difficulties that need to be resolved. The sensors are sensitive to malicious manipulation; for instance, IMUs are exposed to sound waves, and GPS receptors are prone to signal spoofing. Vehicles should validate sensor signals before acting on them [1]. Like any cyber-physical system, attacks against the Internet of Transportation Systems are frequent. Data is gathered in timely manner from systems like driverless cars in the future and autonomous vehicles now. Energy saving is necessary for electric transportation systems. Attacks on energy executives might result in accidents, fatalities, and abandonment on lonely roads as a result of attempts to weaken the security of such systems [2]–[4].

A test is being conducted to use the stream examination/learning techniques for transportation information while information science/ML approaches are being used to study the information of AVs. The Internet of Transportation Systems will also heavily depend on Data Science/AI/ML (Machine Learning) techniques for a variety of applications, including best headings, autonomous driving, and other uses.

The Adversary will become adept at using the AI models we use and will try to undermine our models [5]. The security of the population must be maintained despite the Internet of Transportation Systems' massive amounts of data collection. We anticipate that a significant portion of information exchange and analysis will be carried out via cloud-based services integrated with the Internet of Transportation System. In order to promote Intelligent Internet of Transportation Systems, this study looks at how Artificial Intelligence, Security, and the Cloud can work together. We start by looking at how network safety is coordinated. Then, we look at how a secure cloud may be utilized to finish data analysis for the transportation systems. We discuss information transportation system security and protection [6]. We discuss the integration of many components, such as cloud security and artificial intelligence, to create intelligent and trustworthy transportation systems.

System Analysis & Feasibility

The data that will be sent to the driverless car has been stored using IOT. However, there are certain issues with this system's security during data transmission.

<u>Advantages:</u>

- More Security
- Accurate data transfer
- Less cyber attacks

<u>Disadvantages:</u>

- Less security
- Improper data transfer
- More cyber-attacks System

To solve the issues currently present, we are adopting Cyber Security (CS) based data transmission to Autonomous vehicle in this system. Here, a cloud acts as a middleman to transmit sender files to an autonomous car. For further security, we use the CS-based Advanced Encryption Standard algorithm, which is employed to convert the sent data into cypher text. The private key that the sender generates for the specific AV may be used to decode the encrypted text [7]. In Figure 1 shows the cloud based model in which represent the link between the users and cloud account.

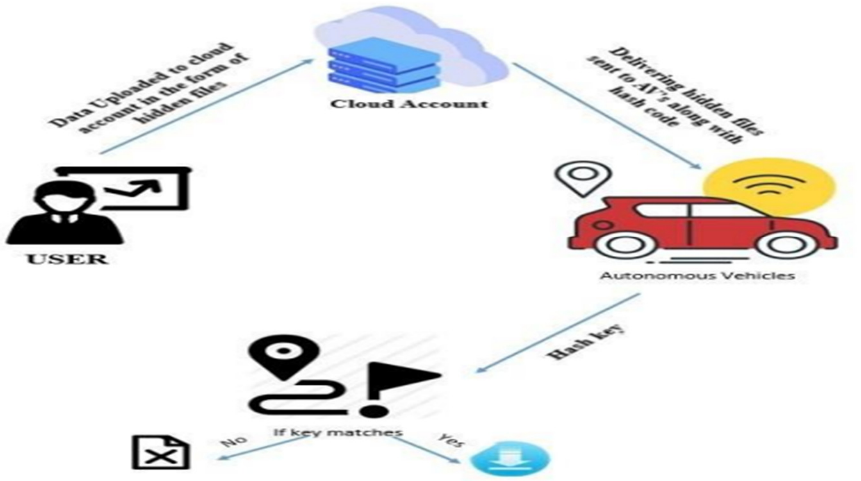
Data Uploaded to cloud account in the form of hidden files
Cloud Account
Delivering hidden files sent to AV's along with hash code
USER
Autonomous Vehicles
Hash key
If key matches
No
Yes

Figure 1: Showing the Cloud Based Model.

Bibliography

[1] P. Olsen and M. Borit, "The components of a food traceability system," *Trends in Food Science and Technology*. 2018. doi: 10.1016/j.tifs.2018.05.004.

[2] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K. Y. Lam, and L. H. Koh, "Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey," *IEEE Internet of Things Journal*. 2021. doi: 10.1109/JIOT.2020.3028368.

[3] M. Jin, Q. Zhang, H. Wang, and Y. Yuan, "Research on intelligent transportation system based on internet of things," *Int. J. Heavy Veh. Syst.*, 2020, doi: 10.1504/IJHVS.2020.108737.

[4] C. Liu and L. Ke, "Cloud assisted Internet of things intelligent transportation system and

the traffic control system in the smart city," *J. Control Decis.*, 2022, doi: 10.1080/23307706.2021.2024460.

[5] N. H. Kamarulzaman, N. A. Muhamad, and N. Mohd Nawi, "An investigation of adoption intention of halal traceability system among food SMEs," *J. Islam. Mark.*, 2022, doi: 10.1108/JIMA-11-2020-0349.

[6] I. Masudin, A. Ramadhani, D. P. Restuputri, and I. Amallynda, "The Effect of Traceability System and Managerial Initiative on Indonesian Food Cold Chain Performance: A Covid-19 Pandemic Perspective," *Glob. J. Flex. Syst. Manag.*, 2021, doi: 10.1007/s40171-021-00281-x.

[7] A. Corallo, M. E. Latino, M. Menegoli, and F. Striani, "What factors impact on technological traceability systems diffusion in the agrifood industry? An Italian survey," *J. Rural Stud.*, 2020, doi: 10.1016/j.jrurstud.2020.02.006.

CHAPTER-2

CLASSIFICATION OF SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC) MODEL

Dr. C. Kalaiarasan
Associate Dean, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: kalaiarasan@presidencyuniversity.in

Waterfall model as our software development cycle because of its step by step procedure while implementing and also shown in Figure 1.

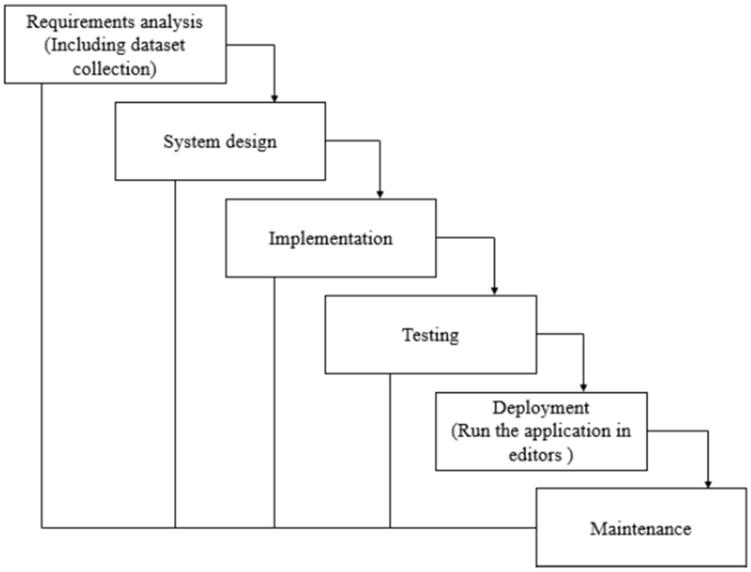
Requirements analysis (Including dataset collection)
System design
Implementation
Testing
Deployment (Run the application in editors)
Maintenance

Figure 1: Illustrated that the Waterfall Model [1]**.**

Requirement Gathering and Analysis: all potential needs of the system to be developed square measure captured during this part and documented in an exceedingly demand specification document.

System Style: the need specifications from 1st part square measure studied during this part and therefore the system style is ready. This technique style helps in specifying hardware and system needs and helps in shaping the system design.

Implementation: with inputs from the system style, the system is 1st developed in little programs known as units, that square measure integrated within the next part. Every unit is developed and tested for its practicality that is observed as Unit Testing.

Integration and Testing: All the units developed within the implementation part square measure integrated into a system when testing of every unit. Post integration the whole system is tested for any faults and failures.

Deployment of System: Once the purposeful and non-functional testing is done; the merchandise is deployed within the client setting or discharged into the market.

Maintenance: There square measure some problems that return up within the consumer setting. To fix those problems, patches square measure discharged. Also, to reinforce the merchandise some higher versions are released. Maintenance is done to deliver these changes in the customer environment [2].

It is examined in this section, after which a business proposal is presented together with a very generic project plan and some cost estimates. The practicability research of the intended system must be conducted throughout the system analysis process. This may be done to ensure that the company isn't burdened by the intended system. Understanding the most crucial requirements for the system is crucial for the practicability analysis [3].

Three key considerations involved in the feasibility analysis are:

- Economic Feasibility
- Technical Feasibility
- Social Feasibility

Economic Viability:

The goal of this analysis was to forecast the financial impact that the framework would have on the association. It is unclear how much more the organization will add to the framework's creative effort. The applications should be appropriate. As a result, the developed framework was also rather sensible, which was made possible by the fact that the vast majority of technological advances were freely available. Simply the modified items should be purchased.

Technical Viability:

This research is conducted to evaluate the framework's particular requirements, or the specialized plausibility. Any new framework shouldn't rely heavily on readily available specialist resources. High demand will result for the available specialist assets as a result. This will lead to the customer receiving several requests. The generated framework should have a minimal precondition as only trivial or incorrect modifications are required to implement this framework [4].

Social feasibility:

The part of study is to really take a glance at the degree of acknowledgment of the framework by the shopper [5], [6]. This incorporates the foremost common approach of making ready the shopper to profitably utilize the framework. The shopper mustn't feel compromised by the framework, rather ought to acknowledge it as a requirement. The degree of acknowledgment by the purchasers solely depends upon the techniques that square measure utilized to show the shopper concerning the framework and to create him at home with it. His degree of certainty ought to be raised with the goal that he's to boot able to create some valuable analysis that is invited, as he's the last shopper of the framework.

Bibliography

[1] L. Sherrell, “Waterfall Model,” in *Encyclopedia of Sciences and Religions*, 2013. doi: 10.1007/978-1-4020-8265-8_200285.

[2] A. A. A. Adenowo and B. A. Adenowo, “Software Engineering Methodologies: A Review

of the Waterfall Model and Object-Oriented Approach," *Int. J. Sci. Eng. Res.*, 2013.

[3] S. A. Alsagaby and M. T. Alharbi, "Cancer in saudi arabia (CSA): Web-based application to study cancer data among saudis using waterfall model," *J. Multidiscip. Healthc.*, 2021, doi: 10.2147/JMDH.S326168.

[4] M. S. Gharajeh, "Waterative Model: An Integration of the Waterfall and Iterative Software Development Paradigms," *Database Syst. J.*, 2019.

[5] L. Ordinez, C. Buckle, S. A. Kaminker, D. Firmenich, D. Barry, and A. Aguirre, "Assessing cycling social feasibility in a medium-size Patagonian city," *Transp. Res. Part D Transp. Environ.*, 2021, doi: 10.1016/j.trd.2021.102720.

[6] T. Akamatsu, T. Nagae, M. Osawa, K. Satsukawa, T. Sakai, and D. Mizutani, "Model-based analysis on social acceptability and feasibility of a focused protection strategy against the COVID-19 pandemic," *Sci. Rep.*, 2021, doi: 10.1038/s41598-021-81630-9.

CHAPTER-3

CLASSIFICATION OF FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENT

Dr. G. Shanmugarathinam
Professor & HOD, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: shanmugarathinam@presidencyuniversity.in

Functional and non-functional requirements are a cycle that makes it possible to monitor the development of a framework or programming activity. Desires are often divided into two categories: functional and nonfunctional circumstances. Functional prerequisites these are the fundamental requirements that the system must meet in order to fulfil the needs of the highest user, and they should be forced to be included in the system as a condition of the contract. These units specified or stated the kind of input to provide the system, the action carried out, and also the anticipated outcome. They differ from purely non-functional demands in that they are largely user-expressed desires that can be seen immediately within the finished product [1].

Examples of helpful requirements:

1. Every time a user enters into the system, they must authenticate themselves;
2. System shutdown in the event of a cyber-attack,
3. Every time a person registers for any code package for the first time, a verification email is sent to them.

Non-functional requirements

These are essentially the quality requirements that the framework must meet in order to comply with the undertaking contract. Each venture has a different level of demand or execution of these components [2]–[5]. They are also known as non behaviours requirements [6]. They mostly address issues like:

1. Portability
2. Security
3. Maintainability
4. Reliability
5. Scalability
6. Performance
7. Reusability
8. Flexibility

Examples of non-functional requirements:

1. Emails should be sent with a latency of no greater than 12 hours from such an activity [7].

2. The processing of each request should be done within 10 seconds.
3. The site should load in 3 seconds whenever of simultaneous users are > 10000

Requirement of Software and Hardware

Software Specifications:

Operating System	-	Windows 10 Python 3.9+
Server-side Script	-	PyCharm
IDE Libraries Used	-	Pandas, IO, OS, Random, Flask.

Hardware Specification:

Processor	i3/Intel Processor
RAM	8 GB (min)
Hard Disk	128 GB

Bibliography

[1] P. Becker, G. Tebes, D. Peppino, and L. Olsina, "Applying an Improving Strategy that embeds Functional and Non-Functional Requirements Concepts," *J. Comput. Sci. Technol.*, 2019, doi: 10.24215/16666038.19.e15.

[2] P. Shankar, B. Morkos, D. Yadav, and J. D. Summers, "Towards the formalization of non-functional requirements in conceptual design," *Res. Eng. Des.*, 2020, doi: 10.1007/s00163-020-00345-6.

[3] M. Binkhonain and L. Zhao, "A review of machine learning algorithms for identification and classification of non-functional requirements," *Expert Systems with Applications: X*. 2019. doi: 10.1016/j.eswax.2019.100001.

[4] D. Ameller *et al.*, "Dealing with Non-Functional Requirements in Model-Driven Development: A Survey," *IEEE Transactions on Software Engineering*. 2021. doi: 10.1109/TSE.2019.2904476.

[5] A. Jarzebowicz and P. Weichbroth, "A Qualitative Study on Non-Functional Requirements in Agile Software Development," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3064424.

[6] D. García-López, M. Segura-Morales, and E. Loza-Aguirre, "Improving the quality and quantity of functional and non-functional requirements obtained during requirements elicitation stage for the development of e-commerce mobile applications: An alternative reference process model," *IET Softw.*, 2020, doi: 10.1049/iet-sen.2018.5443.

[7] M. Younas, D. N. A. Jawawi, I. Ghani, and M. A. Shah, "Extraction of non-functional requirement using semantic similarity distance," *Neural Comput. Appl.*, 2020, doi: 10.1007/s00521-019-04226-5.

CHAPTER-4

UNIFIED MODELING LANGUAGE (UML)

Dr. Preethi
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: preethi@presidencyuniversity.in

Unified Modeling Language, or UML, is a standard, widely practical demonstrating language used in the area of item-focused computer programming. The standard was created by the Object Management Group and is attributed to them. The goal is for UML to become a standard language for creating models of item-centered computer programming. A Meta model and a documentation are two important components of UML's continuing structure. Later, a particular approach or process could also be added to, or connected to, UML [1]–[3]. The Unified Modeling Language is an everyday language for identifying, describing, building, and documenting programming framework quirks as well as those related to business displaying and other non-programming structures. The UML covers a variety of standard practices in design that have proven successful. in the exhibition of substantial and intricate structures. The process of developing objects-situated programmers and the process of improving products both rely heavily on the UML [4]. To convey the layout of programming projects, the UML mostly uses graphical documentations.

The Primary goals in the design of the UML are as follows:

- Why provide customers with a conversational, ready-to-use visual showing language so they may construct and exchange essential models.
- Add features of specialization and extendibility to the middle notions.
- Be independent of certain programming languages and development techniques.
- State a valid justification for understanding the broadcast language.
- Promote the market for OO equipment.
- Encourage other essential level advancement concepts including collaboration, frameworks, demonstrations, and components.
- Include established practices [5].

Use Case Diagram

- In the Unified Modeling Language (UML), a usage case outline is a kind of conduct chart that is defined by and created from a use-case analysis, as shown in Figure 1.
- It is motivated by the need to provide a graphical summary of the value provided by a framework with regard to entertainers, their goals (expressed as use cases), and any relationships between those use cases.

- The main goal of a usage case outline is to identify which performer's use of which framework capabilities. It is possible to depict the performers' jobs inside the framework [6].

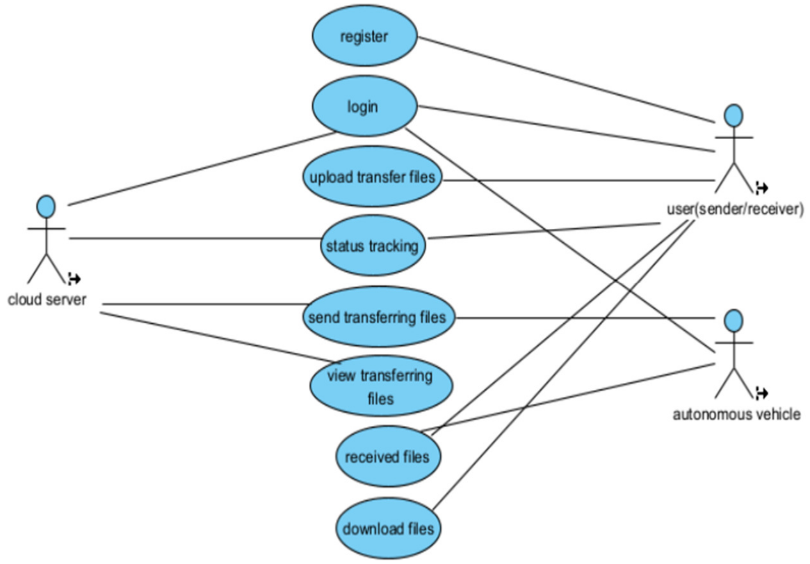

Figure 1: Display the Flow Diagram of Use case.

Class Diagram

A class chart in programming is a kind of static design graph that illustrates how a framework is built by displaying the classes that make up the framework, their traits, tasks or strategies, and links between the classes. Which class holds data makes sense shown in Figure 2 [7].

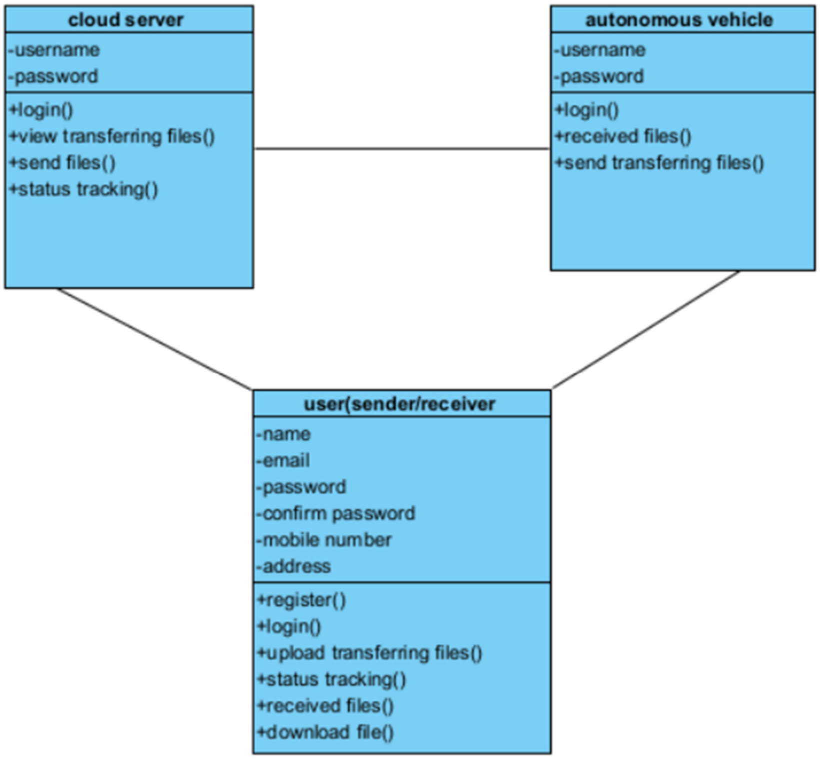

Figure 2: Showing the Block Diagram of Uses Classes.

Bibliography

[1] H. Fahmi, “Aplikasi Pembelajaran Unified Modeling Language Berbasis Computer Assisted Instruction,” *Query*, 2018.

[2] Haviluddin, “Memahami Penggunaan UML (Unified Modelling Language),” *Memahami Pengguna. UML (Unified Model. Lang.*, 2011.

[3] D. W. T. Putra and R. Andriani, “Unified Modelling Language (UML) dalam Perancangan Sistem Informasi Permohonan Pembayaran Restitusi SPPD,” *J. TeknoIf*, 2019, doi: 10.21063/jtif.2019.v7.1.32-39.

[4] S. Nasiri, Y. Rhazali, M. Lahmer, and A. Adadi, “From User Stories to UML Diagrams Driven by Ontological and Production Model,” *Int. J. Adv. Comput. Sci. Appl.*, 2021, doi: 10.14569/IJACSA.2021.0120637.

[5] O. Anas, T. Mariam, and L. Abdelouahid, “New method for summative evaluation of UML class diagrams based on graph similarities,” *Int. J. Electr. Comput. Eng.*, 2021, doi: 10.11591/ijece.v11i2.pp1578-1590.

[6] M. K. Hutauruk, “UML Diagram : Use Case Diagram,” *BINUS University*. 2019.

[7] R. Fauzan, D. Siahaan, S. Rochimah, and E. Triandini, “Automated Class Diagram Assessment using Semantic and Structural Similarities,” *Int. J. Intell. Eng. Syst.*, 2021, doi: 10.22266/ijies2021.0430.06.

CHAPTER-5

SEQUENCE DIAGRAM OF UNIFIED MODELING LANGUAGE

Dr. Nagaraj S R
Associate Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: - nagarajsr@presidencyuniversity.in

A grouping chart in the Unified Modeling Language (UML) depicts how cycles interact with one another and in what order [1]–[3]. It is constructed in the manner of the message sequence chart shown in Figure 1. Grouping charts are sometimes referred to as timing outlines, occasion graphs, and event scenarios [1].

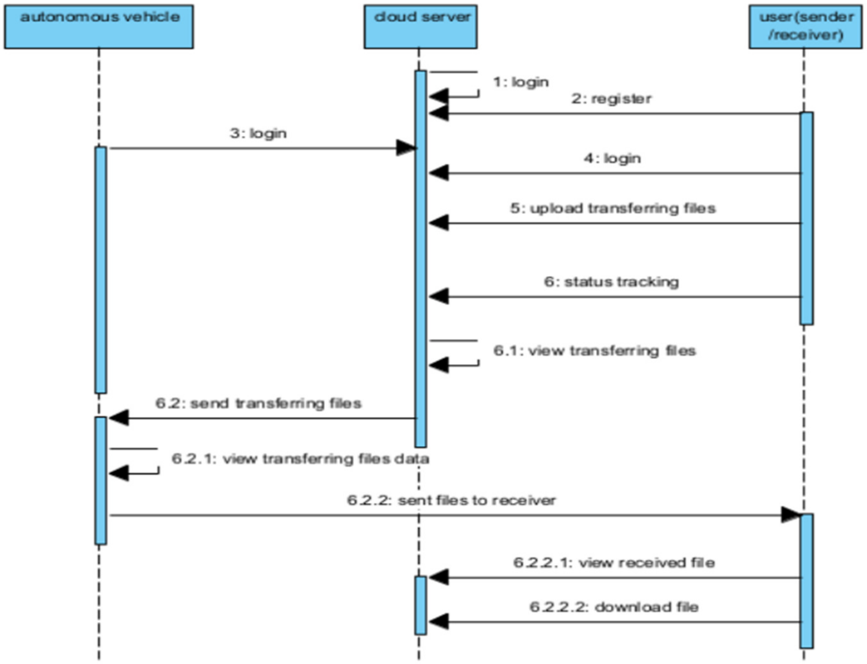
autonomous vehicle
cloud server
user(sender /receiver)
1: login
2: register
3: login
4: login
5: upload transferring files
6: status tracking
6.1: view transferring files
6.2: send transferring files
6.2.1: view transferring files data
6.2.2: sent files to receiver
6.2.2.1: view received file
6.2.2.2: download file

Figure 1: Illustrated that the Sequential Diagram [4].

Collaboration Diagram:

The strategy choice arrangement in the joint effort graph is unquestionable according to the enumeration methods shown below in Figure 2. The amount demonstrates how the procedures are used in a methodical manner. We used a board structure that is equivalent to the request to illustrate the definition of collaboration. The method calls are similar to those of a succession define. However, the crucial distinction is that the coordinated effort graph depicts the article relationship, but the succession definition does not associate [5]–[7].

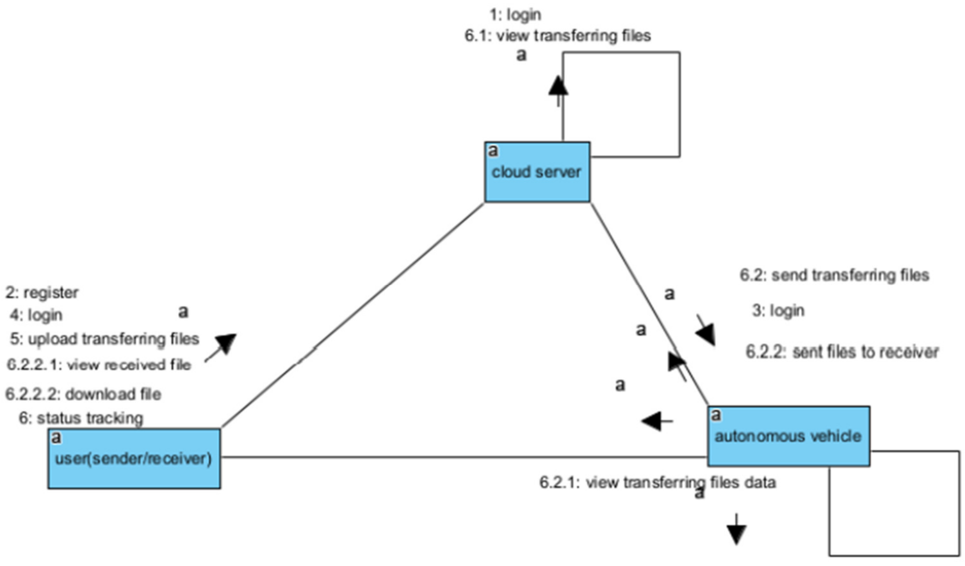
1: login
6.1: view transferring files
a
a
cloud server
2: register
4: login
5: upload transferring files
6.2.2.1: view received file
6.2.2.2: download file
6: status tracking
a
a
user(sender/receiver)
6.2: send transferring files
3: login
6.2.2: sent files to receiver
a
a
a
a
autonomous vehicle
6.2.1: view transferring files data
a

Figure 2: Illustrated that the Collaboration Diagram [8]**.**

Deployment Diagram

Sending an outline addresses a framework from the organization's point of view. It has a relationship to the portion outline because the sending charts are used to transmit the pieces. Hubs make up an outline for mailing. Hubs are the sole pieces of hardware used to deliver the application as mention in Figure 3.

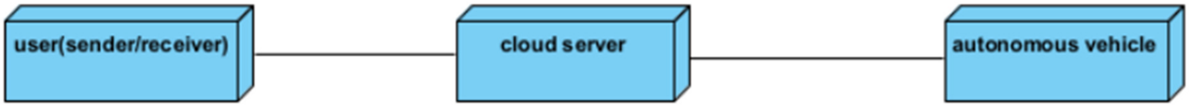

Figure 3: Display the Deployment Diagram.

Bibliography

[1] C. Alvin, B. Peterson, and S. Mukhopadhyay, “Static generation of UML sequence diagrams,” *Int. J. Softw. Tools Technol. Transf.*, 2021, doi: 10.1007/s10009-019-00545-z.

[2] M. Elsayed, N. Elkashef, and Y. F. Hassan, “Mapping UML sequence diagram into the web ontology language OWL,” *Int. J. Adv. Comput. Sci. Appl.*, 2020, doi: 10.14569/IJACSA.2020.0110542.

[3] B. Wei, H. S. Delugach, and Y. Wang, “From state diagrams to sequence diagrams: a requirements acquisition approach,” *Int. J. Comput. Appl.*, 2019, doi: 10.1080/1206212X.2017.1408982.

[4] S. Al-Fedaghi, “UML Sequence Diagram: An Alternative Model,” *Int. J. Adv. Comput. Sci. Appl.*, 2021, doi: 10.14569/IJACSA.2021.0120576.

[5] A. Kaur and V. Vig, “Automatic test case generation through collaboration diagram: a case study,” *Int. J. Syst. Assur. Eng. Manag.*, 2018, doi: 10.1007/s13198-017-0675-8.

[6] T. M. Maarouk, M. El Habib Souidi, and N. Hoggas, “formalization and model checking of

bpmn collaboration diagrams with dd-lotos," *Comput. Informatics*, 2021, doi: 10.31577/CAI_2021_5_1080.

[7] F. Dai, Q. Mo, T. Li, Z. Xie, and J. Qin, "Hybrid approach to define process choreographies," *Jisuanji Jicheng Zhizao Xitong/Computer Integr. Manuf. Syst. CIMS*, 2016, doi: 10.13196/j.cims.2016.02.009.

[8] T. Bultan and X. Fu, "Specification of realizable service conversations using collaboration diagrams," *Serv. Oriented Comput. Appl.*, 2008, doi: 10.1007/s11761-008-0022-7.

CHAPTER-6

INTRODUCTION TO USE OF SCRIPTING LANGUAGE

Dr. S.P. Anandaraj
Professor & HOD, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: - anandaraj@presidencyuniversity.in

Python's capacity for intuitive programming. This capability allows you to develop programmes and have them run fast and easily, and it is quite helpful. A content is a text file that contains the reasons for a Python programme. Scripts are, at their core, reusable. You can reuse stuff you've already generated without having to enter it again. Scripts might be modified Perhaps more crucially, you could use a word processor to alter the claims and produce many iterations of the data, starting with one document and going on to the next. You may then immediately execute each distinct version [1]–[4]. It is simple to create several projects with just a basic degree of typing. You will require a content management system in order to produce Python script documents. Any content management should work in this case. You may use pretty much any word processor, including Microsoft Word, Microsoft WordPad, Microsoft Notepad, and others, if required.

Difference between a script and a program Script:

If nothing else changes, scripts are often developed for the end user and may be separated from the application's main code, which is normally written in a different language. Scripts are often encrypted from source code or bytes, even though the programmers they supervise are frequently compiled to local machine code. Program: The executable instructions in the programme may be utilized directly by the computer. The same programme in human-readable source code from which executable programs are derived.

Python

Explain Python. Most likely, you ask yourself this. This book may have caught your attention if you need to develop applications but are not acquainted with the different programming languages. Alternatively, you could already be acquainted with programming languages like C, C++, C#, or Java and need to understand how Python differs from these "enormous name" dialects. I'll make an effort to make sense of it for you [5], [6]. Python-based ideas Feel free to go on to the next section if you don't care out about how’s and whys of Python. I'll attempt to explain to the reader why Python is, in my view, probably the finest programming language anybody could ever hope to find and why it's a wonderful one to start with in this part.

- An open-source language with broad applicability.
- Object-oriented, procedural, and functional
- Simple C, Obj C, Java, and Fortran interaction

- Getting connected to C++ is easy (by means of SWIG)
- Exceptionally intuitive setting

Python is a high-level, decoded, intelligent, and object-oriented language. Python is designed to be very transparent. It has less linguistic development than other dialects and often employs English terminology without emphasizing them.

1. Python is interpreted, therefore it is used at runtime by the translator. You don't need to set up your programme before using it. This, much like PERL and PHP.
2. Python is interactive; to build your projects, you can actually sit down at a Python prompt and have direct interactions with the translator.
3. Python is an object-oriented programming language, which means it wraps code inside of objects.
4. Python is a Great Language for Rookie Software Engineers - Python is a great language for novice software engineers and makes it easy to create a variety of applications, from basic text processing to games to WWW apps.

Among Python's attributes are:

1. Python is simple to learn because it has a clear language structure, few watchwords, and a straightforward design. The apprentice may rapidly take up the language because of this.
2. Python code is simple to comprehend since it is so well stated and readable.
3. Simple to maintain very simple to maintain Python's source code.
4. A large standard library bulk of the Python library runs on UNIX, Windows, and Macintosh platforms and is fully functional.
5. Intelligent Mode Python features a user-friendly mode that makes it simple to test and debug code.
6. Python is small because it can function on a number of equipment stages and has a constant connection point on each stage.
7. Extendable - Low-level modules may be accepted by the Python translator. Developers may expand or improve their tools using these modules.

Bibliography

[1] P. Biggar, E. De Vries, and D. Gregg, “A practical solution for achieving language compatibility in scripting language compilers,” *Sci. Comput. Program.*, 2012, doi: 10.1016/j.scico.2011.01.004.

[2] T. Sandeep, G. Dhana Laxmi, and K. Durga, “Scripting Languages for Research in Data Mining,” *Int. J. Eng. Comput. Sci.*, 2017.

[3] R. R. Codilan, “Waray Scripting Language (WSL): A mother tongue-based scripting language,” *Indian J. Comput. Sci. Eng.*, 2019, doi: 10.21817/indjcse/2019/v10i3/191003009.

[4] T. Bulatewicz, A. Allen, J. M. Peterson, S. Staggenborg, S. M. Welch, and D. R. Steward, “The Simple Script Wrapper for OpenMI: Enabling interdisciplinary modeling studies,”

Environ. Model. Softw., 2013, doi: 10.1016/j.envsoft.2012.07.006.

[5] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and É. Duchesnay, “Scikit-learn: Machine learning in Python,” *J. Mach. Learn. Res.*, 2011.

[6] P. Virtanen *et al.*, “SciPy 1.0: fundamental algorithms for scientific computing in Python,” *Nat. Methods*, 2020, doi: 10.1038/s41592-019-0686-2.

CHAPTER-7

STORING PUBLIC TRANSACTIONAL RECORDS USING BLOCKCHAIN TECHNOLOGY

Ms. Sandhya L
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: - sandhya.l@presidencyuniversity.in

Crowd funding has revolutionized the financing process and made it possible for start-ups and those in need to raise money without a lot of hassle or red tape. In the current model, a group of people aggregate their little cash contributions to a project or cause in hopes of receiving financial or non-financial rewards [1]–[3]. The needs and expectations of funders and fundraisers are matched by a crowd financing platform, which charges a commission [4].

A decentralized ledger created using blockchain technology is more effective, secure, and impervious to manipulation. Crowd funding will become more dependable, transparent, trustworthy, decentralized, affordable, and practical with the adoption of blockchain technology (Figure 1). The technology that will serve as a medium of exchange and transaction is provided by a crowd financing platform that served as an intermediary in the past [5].

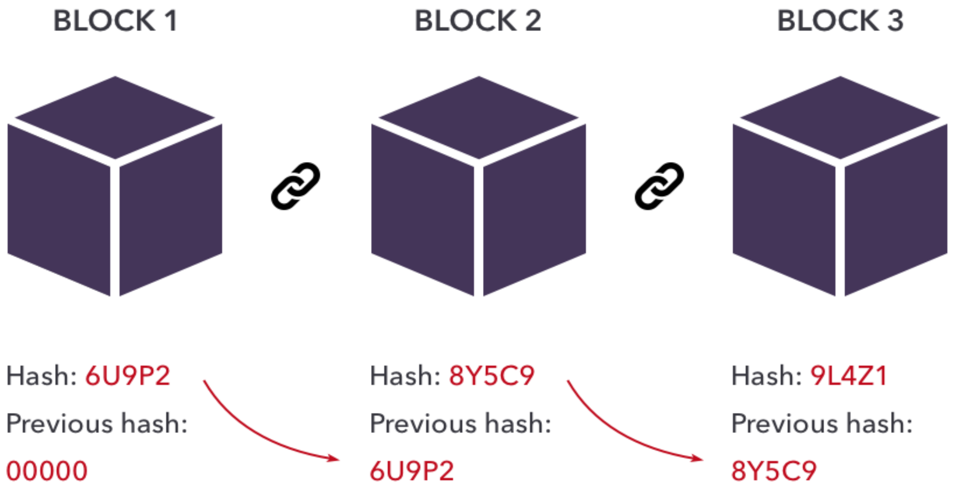

Figure 1: Display the Typical Blockchain [6]**.**

Blockchain

Blockchain technology is a framework for storing public transactional records sometimes referred to as "blocks" across multiple databases in a network connected by peer-to-peer nodes. This type of storage is frequently referred to as a "digital ledger." Every transaction in this ledger is validated and protected against fraud by the owner's digital signature, which also serves to authenticate the transaction. As a result, the data in the digital ledger is quite safe. The digital ledger can be described as a network of computers sharing a Google spreadsheet where transactional data are kept according to actual purchases. The intriguing aspect is that while everyone may view the data, it cannot be altered [7].

Drawbacks of Exiting Methods

There are issues with centralization and control coming from a single entity in the present techniques. If a platform's developer so chooses, users may not raise further funds, especially if doing so will negatively impact the platform. Even governments have the power to halt certain projects if they don't believe they are credible. The existing crowd funding system has a single point of failure, meaning that if it fails, the entire system will cease to function. Any system that aims for high availability or dependability, whether it be a business procedure, software program, or other industrial systems, should avoid single points of failure.

Architecture Design

The following architecture diagram is showing the basic working of the web application frontend and backend (Figure 2).

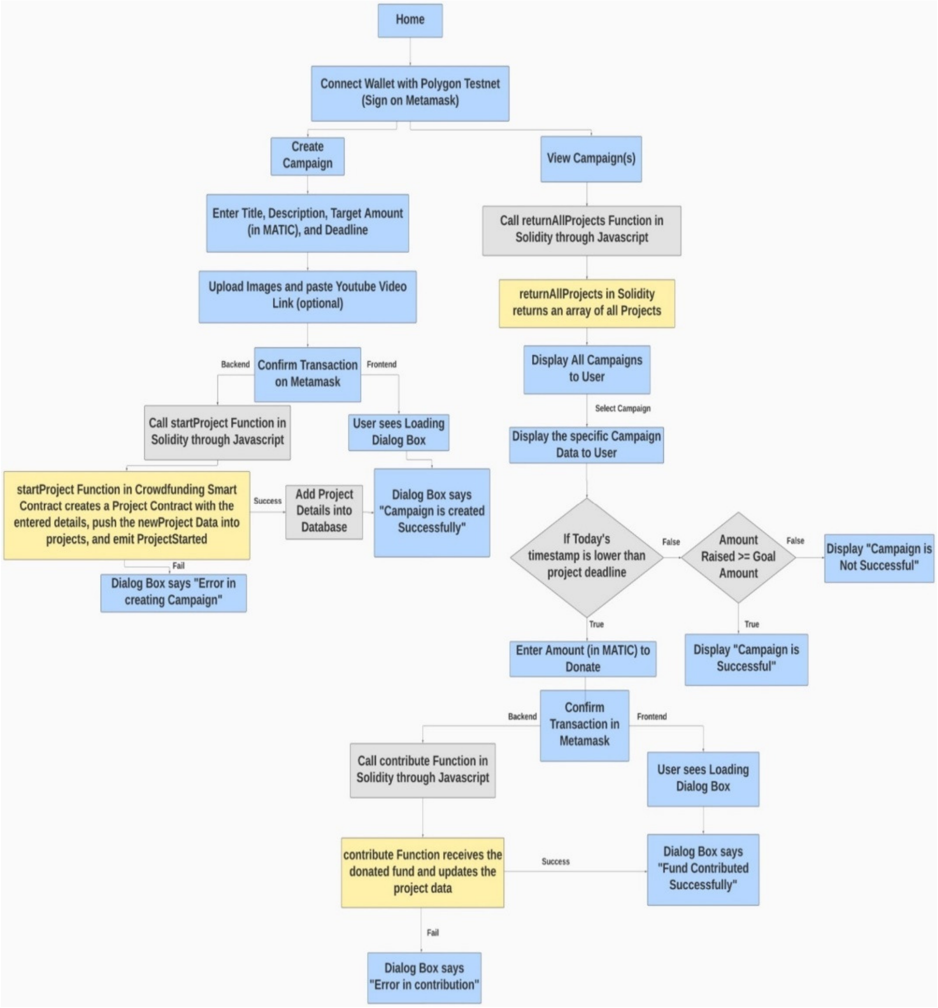
Home
Connect Wallet with Polygon Testnet (Sign on Metamask)
Create Campaign
View Campaign(s)
Enter Title, Description, Target Amount (in MATIC), and Deadline
Call returnAllProjects Function in Solidity through Javascript
Upload Images and paste Youtube Video Link (optional)
returnAllProjects in Solidity returns an array of all Projects
Backend
Confirm Transaction on Metamask
Frontend
Display All Campaigns to User
Select Campaign
Call startProject Function in Solidity through Javascript
User sees Loading Dialog Box
Display the specific Campaign Data to User
startProject Function in Crowdfunding Smart Contract creates a Project Contract with the entered details, push the newProject Data into projects, and emit ProjectStarted
Success
Add Project Details into Database
Dialog Box says "Campaign is created Successfully"
Fail
Dialog Box says "Error in creating Campaign"
If Today's timestamp is lower than project deadline
False
Amount Raised >= Goal Amount
False
Display "Campaign is Not Successful"
True
True
Enter Amount (in MATIC) to Donate
Display "Campaign is Successful"
Backend
Confirm Transaction in Metamask
Frontend
Call contribute Function in Solidity through Javascript
User sees Loading Dialog Box
contribute Function receives the donated fund and updates the project data
Success
Dialog Box says "Fund Contributed Successfully"
Fail
Dialog Box says "Error in contribution"

Figure 2: Display the Web and Front-End Working Diagram.

Bibliography

[1] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, “Blockchain technology and its relationships to sustainable supply chain management,” *Int. J. Prod. Res.*, 2019, doi: 10.1080/00207543.2018.1533261.

[2] A. Batwa and A. Norrman, “Blockchain technology and trust in supply chain management: A literature review and research agenda,” *Operations and Supply Chain Management*. 2021. doi: 10.31387/oscm0450297.

[3] Q. Wang, R. Li, and L. Zhan, “Blockchain technology in the energy sector: From basic research to real world applications,” *Computer Science Review*. 2021. doi: 10.1016/j.cosrev.2021.100362.

[4] O. Pal, B. Alam, V. Thakur, and S. Singh, “Key management for blockchain technology,” *ICT Express*, vol. 7, no. 1, pp. 76–80, Mar. 2021, doi: 10.1016/j.icte.2019.08.002.

[5] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Futur. Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.

[6] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *Int. J. Web Grid Serv.*, 2018, doi: 10.1504/IJWGS.2018.095647.

[7] C. Walsh, P. O’Reilly, R. Gleasure, J. McAvoy, and K. O’Leary, “Understanding manager resistance to blockchain systems,” *Eur. Manag. J.*, 2021, doi: 10.1016/j.emj.2020.10.001.

CHAPTER-8

VARIOUS MODULES AND THEIR INTEGRATION

Dr. Manjula H.M
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: -manjulahm@presidencyuniversity.in

Navbar

This is the most important section of the website, and the link to go to another page is right here. Links, a Button in the upper right to subscribe to a Blockchain network, and a wrapper to display whether the linked network is correct or not are child features of the Navbar. Every page of the website will always open with this module visible at the top [1].

Campaign List

The module, as its name implies, is in charge of displaying campaigns on the main and profile sections. Each list of campaigns includes several elements, such as the cover photo, title, description, stage of the campaign, and the amount of money raised. The user will be directed to the relevant campaign website by clicking on this module, where they may view the details, contribute to the cause, and request a refund [2].

Raise Funds (Form Component)

The campaign is created with this module using a three-step form method. There are only a few input fields for the title, description, date, and amount. The module provides a drag-and-drop image component in the second phase [3]–[5]. The user should be allowed to launch a new campaign after confirming.

Tab Module

The module is used in the profile section, where it displays all of the current users' funded campaigns and all donations based on a user's selection [6].

Carousel Module

It is used to display all of the pictures and videos that the user has uploaded for a certain campaign.

Main Donation Module

Users may easily give or get a refund because it is always shown next to the carousel module. From the application, users may launch and fund campaigns tailored to their requirements. On the first page, they will need to fill in the Title, Description, Target Amount in-network default token, and Deadline for their requirements. Then, they must supply a minimum of 1 and a maximum of 5 photographs for the project. Additionally, users can attach a YouTube link, which is encouraged for the project's validity but not needed.

The Target Amount, Deadline, unique ID, and user's current blockchain address will then be saved on the smart contract on the following page after the transaction has been validated. After that, the Cloudinary API for pictures will be utilized to store all of this data, including the photos, titles, descriptions, and YouTube links, on a server. The user can view their raised campaign on the Campaigns page if all goes as planned [7].

A separate user with a different address can donate to the campaign by simply choosing it and entering the desired amount. The user must then confirm the transaction on Metalmark after clicking the contribute button. In the end, money will be given to the smart contract from the donor's wallet. The money will be transferred to the campaign raiser's wallet after the campaign hits its goal. Whether or not the project is successful, the smart contract will reject any tokens sent to it. Either successful, running, or failed will be displayed on the front end. Users who gave will be able to request their refunds straight from the website for projects that were unsuccessful and unable to raise the desired amount within the allotted time frame. The blockchain will reverse or cancel any refund claim when the user hasn't given it. The person who created the project should be able to view all of their campaigns, along with all of the projects they have donated to thus far, in the profile section.

Bibliography

[1] J. Lu, G. Xu, S. Zhang, and B. Lu, “An effective sequence-alignment-free superpositioning of pairwise or multiple structures with missing data,” *Algorithms Mol. Biol.*, 2016, doi: 10.1186/s13015-016-0079-3.

[2] T. Keatinge, F. Keen, and K. Izenman, “Fundraising for right-wing extremist movements: How they raise funds and how to counter it,” *RUSI J.*, 2019, doi: 10.1080/03071847.2019.1621479.

[3] Q. Cheng and F. Junwen, “Logistic regression model analysis of institutional environment, corporate governance and IPO change to raise funds: A big data perspective,” *RISTI - Rev. Iber. Sist. e Tecnol. Inf.*, 2016.

[4] S. Pyo, H. R. Ma, S. Na, and D. H. Oh, “The crowdfunding model, collective intelligence, and open innovation,” *J. Open Innov. Technol. Mark. Complex.*, 2021, doi: 10.3390/joitmc7030196.

[5] M. P. Rahman, M. A. Mohd Thas Thaker, and J. Duasa, “Developing a Sharīʿah-compliant equity-based crowdfunding framework for entrepreneurship development in Malaysia,” *ISRA Int. J. Islam. Financ.*, 2020, doi: 10.1108/IJIF-07-2018-0085.

[6] V. Hartarska and D. Nadolnyak, “Does rating help microfinance institutions raise funds? Cross-country evidence,” *Int. Rev. Econ. Financ.*, 2008, doi: 10.1016/j.iref.2007.05.008.

[7] S. Riyanti, M. Hatta, S. Norhafizah, M. N. Balkish, Z. M. Siti, A. H. Hamizatul Akmal, and A. Normawati, “Organ donation by sociodemographic characteristics in Malaysia,” *Asian Soc. Sci.*, 2014, doi: 10.5539/ass.v10n4p264.

CHAPTER-9

BLOCKCHAIN TECHNOLOGY USED FOR MANAGE THE TRANSACTION RECORD

Dr. Harish Kumar K.S.
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: -harishkumar@presidencyuniversity.in

Blockchain technology is a decentralized ledger that records every transaction that takes place on it and is more effective, secure, and impervious to manipulation. It is made up of a network where each node has an equal amount of authority and power. Crowdfunding is a method of jointly raising money for a cause or commercial endeavour to get monetary assistance at an early stage. Crowdfunding has changed the way that money is raised and made it possible for start-ups and those in need to raise money without a lot of hassle or red tape. In the current model, a group of people aggregate their little money available to a project or cause in hopes of receiving financial or non-financial rewards. The needs and expectations of funders and petitioners are matched by a crowdfunding platform, which also charges a fee. With the use of blockchain, crowdfunding will become more dependable, transparent, trustworthy, decentralized, affordable, and practical [1]–[3].

The technology that will serve as a medium of trade and transaction is provided by a crowdfunding site and has served as an intermediary in the past. Additionally, there are issues with administration and control from a single company in the established crowdfunding platforms. If a platform's developer so chooses, users might not always raise further funds, especially if doing so will negatively impact the platform. Even governments have the power to halt certain programs if they don't believe they are credible. The existing crowdfunding system has a single point of failure, meaning that if it fails, the existing network will cease to function. Any system which it aims for high availability or consistency, whether it be a business procedure, software program, or perhaps other industrial systems, should avoid single points of failure. Building a decentralized fundraising web application is the main objective of the effort to improve upon the flaws of the existing solutions [4].

Used Technologies

- **JavaScript**

A text-based programming language called JavaScript is used to develop dynamic and interactive online apps and browsers [5].

- **Cascading Style Sheet**

To design and layout web pages, CSS (Cascading Style Sheets) is employed. For instance, CSS can be used to change the font, color, size, and spacing of the content, divide it into numerous columns or add animations and other ornamental elements [6].

- **Solidity**

The Ethereum Network team specifically developed Solidity, an object-oriented programming language, for building and developing smart contracts on Blockchain systems. In the blockchain system, it is used to establish smart contracts that carry out business logic and produce a string of transaction records.

Libraries and Frameworks Used

1. **Next JS**: React. js-based JavaScript framework with direct API development capability. Additionally, server-side rendering is supported, which is crucial for SEO. Next utilises file-based routing, which is beneficial for developers.
2. **Ethers JS (web3)**: Tools and full implementation of an Ethereum wallet in JavaScript and Typescript.
3. **NodeJS:** On Chrome's V8 engine, NodeJS is a JavaScript runtime environment. It effectively runs JavaScript code outside of the browser. It is primarily utilised for creating backend APIs.
4. **MongoDB:** Database that is not relational. It employs documents that resemble JSON and optional schemas.
5. **Browser Image compressor**: To conserve bandwidth, this module is used to reduce the resolution or storage size of JPEG and PNG images before uploading them to the application server.
6. **React Bootstrap**: Designing and interface
7. **Ganache**: It is employed to set up a private Ethereum Blockchain for testing Solidity contracts.
8. **Git:** Git is a distributed version control system that is free and open source and is made to efficiently and quickly handle projects of all sizes.
9. **Heroku***:* Used for cloud deployment of web applications. For the NodeJS runtime, it is a simple, one-tap deployment solution.
10. **Truffle**: Blockchain asset pipeline, development environment, and testing framework using the Ethereum Virtual Machine (EVM) [7].

Uses of Packages

1. "axios": "^0.26.1",
2. "bootstrap": "^5.1.3",
3. "bootstrap-icons": "^1.8.1",
4. "browser-image-compression": "^1.0.17",
5. "ethers": "^5.5.4",

6. "fast-sort": "^3.1.3",
7. formidable": "^2.0.1",
8. "formik": "^2.2.9",
9. "moment": "^2.29.1",
10. "mongoose": "^6.2.9",
11. "next": "12.1.0",
12. "nprogress": "^0.2.0",
13. "react": "17.0.2",
14. "react-bootstrap": "^2.1.2",
15. "react-circular-progressbar": "^2.0.4",
16. "react-dom": "17.0.2",
17. "react-responsive-carousel": "^3.2.23",
18. "uuid": "^8.3.2"
19. "yup": "^0.32.11"

Bibliography

[1] P. Meier, J. H. Beinke, C. Fitte, J. Schulte to Brinke, and F. Teuteberg, “Generating design knowledge for blockchain-based access control to personal health records,” *Inf. Syst. E-bus. Manag.*, 2021, doi: 10.1007/s10257-020-00476-2.

[2] S. Huang, G. Wang, Y. Yan, and X. Fang, “Blockchain-based data management for digital twin of product,” *J. Manuf. Syst.*, 2020, doi: 10.1016/j.jmsy.2020.01.009.

[3] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu, and F. Wang, “ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care,” *J. Med. Internet Res.*, 2020, doi: 10.2196/13598.

[4] C. Walsh, P. O’Reilly, R. Gleasure, J. McAvoy, and K. O’Leary, “Understanding manager resistance to blockchain systems,” *Eur. Manag. J.*, 2021, doi: 10.1016/j.emj.2020.10.001.

[5] M. Doernhoefer, “JavaScript,” *ACM SIGSOFT Softw. Eng. Notes*, 2006, doi: 10.1145/1142958.1142972.

[6] B. D. Blansit, “An introduction to Cascading Style Sheets (CSS),” *J. Electron. Resour. Med. Libr.*, 2008, doi: 10.1080/15424060802453811.

[7] J. Li, M. Lu, G. Dou, and S. Wang, “Big data application framework and its feasibility analysis in library,” *Inf. Discov. Deliv.*, 2017, doi: 10.1108/IDD-03-2017-0024.

CHAPTER-10

TRADITIONAL FUNDRAISING PROBLEM AND SOLUTION

Mr. Manjunath K.V.
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: -manjunathkv@presidencyuniversity.in

The major methods for bridging the finance chain gap have historically been banks as well as venture capital funds. If a bank or investment capitalist is interested in the project, they will fund it in exchange for something, such as equity in the case of fund managers or loan interest in the case of banks, depending according to how the startup founder pitches his undertaking to them. However, there are negatives to this method of cash raising [1]–[4]. The project developers from impoverished nations or remote locations do not have a connection to the enormous amounts of time, money, and important resources required for this fundraiser procedure. If a bank loan is a preferred method for financing a project, the bank may create a blockage since it wants the founder to put up security for the loan amount and expects clear evidence of how the research study generates money.

The problems with the conventional technique of fundraising can be solved through crowdfunding. Through crowdfunding, an individual or an organization with a problem-solving concept can raise money from a large number of people who wish to support the enterprise. Anyone with an idea can use crowdfunding to showcase it to potential investors who are willing to invest. The principal advantages of crowdfunding are:

- Access to a sizable pool of registered investors who can view the campaign and participate in it.
- Gain a high-level comprehension of the idea's traction, addressable market, and value offer.
- Having the concept presented to different investors enables the startup founder to validate and improve his products.
- The finest thing about online crowdfunding is its propensity to streamline and streamline the campaign creator's fundraising efforts by creating single, interests and abilities that target all potential investors, obviating the need to approach every single one of them separately.

The main problems with these well-known p2p lending platforms are that they are concentrated institutions under the direction of a business that levies hefty fees and regulates campaigns. This process can be aided by blockchain-based crowdfunding platforms by decentralizing the fundraising paradigm used by enterprises like Kickstarter and others. Due to their high maintenance fees, centralized middlemen like Kickstarter and Indiegogo can be replaced because of the distributed ledger of the blockchain. Blockchain crowdfunding is a more pure form of practice because it does not use any middlemen to connect backers and enterprises. A crowdfunding software enables producers to promote their campaigns and then ask an audience of wealthy investors for money. If the funding is successful, it will reward the sponsors with tokens relevant to the campaign; alternatively, it will return the backer's investment. Blockchain, an immutable distributed ledger, tracks and accounts for each of these numerous transactions, making it difficult to manipulate. Additionally, blockchain eliminates the manipulation and manipulation used by corporate crowdfunding sites that have more access to the same campaigns that are running on their platform than is necessary.

Bit coin and the Blockchain

In recent years, bitcoin gained a lot of popularity and established itself as a household word. However, the overwhelming majority of people are unaware of the blockchain technology that underpins bitcoin. Bitcoin is an application of blockchain that is not controlled by a central bank or a single administration; instead, it can be directly supplied between users on the peer-to-peer bitcoin network. Bitcoin transactions that move from one account to another are tracked in a transparent distributed ledger known as the blockchain and are cryptographically validated by nodes connected to the network. When network nodes engage in a process known as mining, they are rewarded with bitcoins. Several locations officially accept bitcoins as payment for local money, goods, or services [5]–[8]. The foundation of this project is a blockchain called Ethereum, which is a precursor to Bitcoin and has the additional capability. Blockchain technology powers all cryptocurrencies, not only Bitcoin and Ethereum, hence it is crucial that we thoroughly examine this technology. Let's first gain an overview of the Bitcoin transaction system, which lays the groundwork for comprehending the Ethereum transaction system. Next, a presentation of the blockchain, which is the backbone of both Bitcoin and Ethereum, will be given.

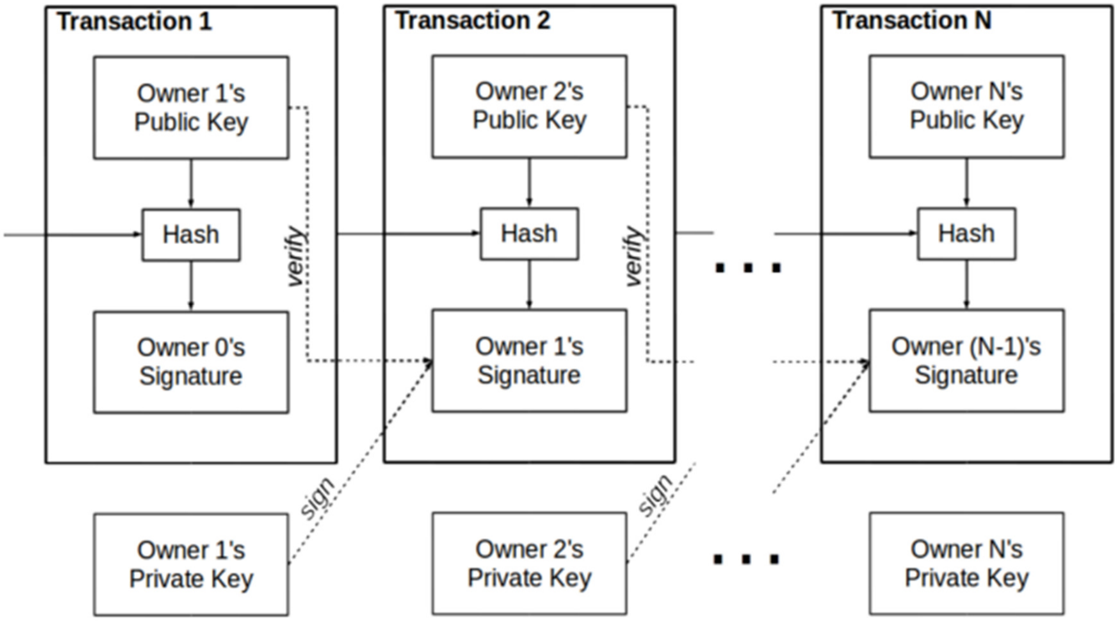

Figure 1: Displaying the Bitcoin Transaction Chain of Ownership.

When the owner of a coin initiates a brand-new transaction and digitally signs a hash of the previous transaction and the owner's public key that is appended to the coin, the sovereignty of the currency is transferred. As can be seen in Figure 1: Bitcoin transaction chain of ownership, a smart contract is added to the chain after being signed. Many inputs, each of which must be signed separately, as well as numerous different outputs, may be included in a transaction. This design was chosen mostly because coins can be mixed and split during operations rather than having to be handled sequentially, as would be the case when utilising the lowest unit of currency, such as pennies. The recipient of the coinage can verify the ownership chain thanks to this transactional chain technology. The recipient cannot establish that the coin has already been spent, which creates a new issue known as the double spending problem. Similar to bitcoin, earlier types of money experienced issues with double-spending. The main achievement of bitcoin was the creation of a novel mechanism that allows it to function without depending on a reliable third party to perform transactions, unlike the majority of the cryptocurrency exchanges that came before it. Blockchain, a fragmented digital public ledger run by a peer-to-peer network to preserve unanimity on the system's current state, was the new mechanism created by bitcoin. Since everyone on the networks will agree on the same collection of transactions that indicate the current status of the coin ownership thanks to the consensus mechanism built into the system, it is virtually impossible to spend the same coin more than once.

Bibliography:

[1] V. C. Ziotti and A. B. Leoneti, “A decision-making method for consensus building applied to increase the chance of decision implementation in NPOs: The case of fundraising problem,” *Brazilian J. Oper. Prod. Manag.*, 2022, doi: 10.14488/BJOPM.2021.044.

[2] R. Bennett and R. Vijaygopal, “What if the company’s ‘charity of the year’ is an organisation that deals with severe to moderate mental disability?: A case study of fundraising problems and possibilities,” *J. Soc. Mark.*, 2019, doi: 10.1108/JSOCM-01-2019-0004.

[3] M. Soleh, “Zakat Fundraising Strategy: Opportunities and Challenges in Digital Era,” *J. Nahdlatul Ulama Stud.*, 2019, doi: 10.35672/jnus.v1i1.1-16.

[4] O. Ignatjeva and A. Pletnev, “Social entrepreneurship in Saint-Petersburg as green economy aspect,” 2021. doi: 10.1051/e3sconf/202124410041.

[5] R. Recabarren and B. Carbunar, “Tithonus: A Bitcoin Based Censorship Resilient System,” *Proc. Priv. Enhancing Technol.*, 2019, doi: 10.2478/popets-2019-0005.

[6] S. T. Yalla and P. Nikhilendra, “An overview on Schlieren optics and its applications Studies on mechatronics,” *Lect. Notes Electr. Eng.*, 2020.

[7] C. Elisabetta, Z. Baltico, D. Catalano, D. Fiore, and R. Gay, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*. 2017.

[8] D. Noble and K. Patil, “Blockchain in Stock Market Transformation: A Systematic Literature Review,” *Rev. Gestão Inovação e Tecnol.*, 2021, doi: 10.47059/revistageintec.v11i4.2551.

CHAPTER-11

CROWD FUNDING APPLICATION

Dr. A. Jayachandaran
Professor & HOD, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: - ajayachandran@presidencyuniversity.in

The goal of the crowdfunding app is to establish an environment where anyone can easily launch or support a campaign intended to develop new goods or services. By offering a long-term incentive communication platform on the internet of value, crowdfunding dapp offers a platform for crowdsourcing funds [1]–[3].

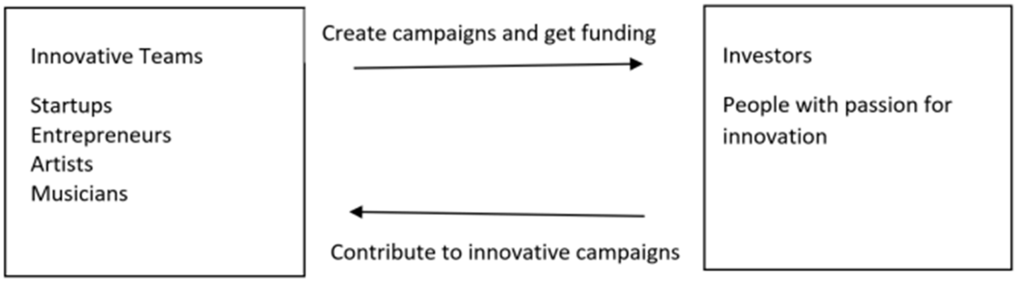
Innovative Teams
Startups
Entrepreneurs
Artists
Musicians
Create campaigns and get funding
Investors
People with passion for innovation
Contribute to innovative campaigns

Figure 1: Illustrated the Crowdfunding app Platform Ideology.

As depicted in Figure 1, the ideology behind the fundraising campaign dapp platform states that teams or individuals, including startup founders, business site supervisors, musicians, filmmakers, etc., will be able to obtain funding by issuing ERC20-type tokens on the blockchain in a particularly straightforward manner. Ethereum-based smart contracts that have been installed control the administration's finances. The blockchain sometimes doesn't record a campaign's metadata, such as its campaign image, video, description, etc. In this study, we utilise the personalities "creator" and "investor," who use the platform for varying reasons. If we do not distinguish between the two roles, we refer to both characters as "users." The phrase "creator(s)" refers to someone or a group using the platform to develop a campaign and generate money, such as a startup team, a painter, a director, or an entrepreneur. The term "investor(s)" refers to a person who utilises the platform to look for appealing initiatives and makes contributions to those projects to earn project-specific tokens [4]–[7]. The language is mostly meant to simulate a professional use case in which an entrepreneur seeks to acquire capital for the establishment of his project or enterprise.

A creator must have a good understanding of what he wants to produce and how his offering or service will benefit the platform's stakeholders to establish a campaign. The creator cannot expect his campaign to be successful if he does not feel confident in his good or service. The potential of his campaign receiving funding will be high if he has completed his proposal, is confident about the deadlines for his deliverables, has the necessary resources that construct the product, and has completed some market research. Every campaign has a deadline for raising money, and the campaign administrator sets this deadline to offer them the first and most flexibility possible. A campaign needs to include a name, the name of the campaign author, a short description, a lengthy description, a banner image, and a campaign video. That the next step is for him to choose how many tokens to distribute as well as their value, names, and symbols. To receive the monies if his campaign is a winner, he must also reveal his Ethereum wallet address.

The campaign's success is not guaranteed; it fully rests somewhat on the creator's market research assessing how much demand there is for the product or service and now on his ability to gain investors' traction. An investor can browse across all the campaigns on the crowdsourced dapp platform, search for or sort the campaigns according to his preferences, and then deposit ether to help his preferred campaign. To invest and expect to be paid for the transaction (gas) to be mined, the investor needs to have enough money in his pocketbook. Depending on the criteria established by the inventor, he can claim the campaign-specific tokens if the project is successful. He may obtain a return of the ether he invested in that particular campaign if it is unsuccessful. The incentives for an entrepreneur to invest in a campaign that, in his estimation, might be successful and in which the token's value might rise in the future are the campaign-specific currencies.

The purpose of UI is to make using the platform and achieving success as easy as possible for the developer and investor. The following are the essential basic UI features that must be used to successfully use the platform:

1. Provide an online platform that lists all the campaigns.
2. Offer a platform for campaigning investment.
3. Offer a campaign development interface.
4. Offer a platform for listing all of the creator's activities so that investors can follow his efforts and claim monies if they are successful.
5. Offer a user interface that allows consumers to view a list of all the campaigns they previously invested in and, depending on the campaign's outcome, request a refunded investment or tokens particular to that campaign.

Campaign Creation and Management

Users need the ability to set up ads and keep track of the Ethereum capital invested in those campaigns. The user navigates to the "Register Campaign" page from the new website and enters all the required information including campaign name, promoter name, description, banner image, banner video and comprehensive ad information. He then comes to the token design screen, where he enters all the specifications for the campaign-specific token, including its name, symbolism, the cost in tokens per unit of contributed ether, and the quantity he chooses to distribute. . Campaigns are created on the Ethereum blockchain using the specified values after the contract creation is initiated. Campaigns are planned to end at a time specified by the creator in days. Only their campaigns are displayed on the campaign developers' page. Using the Campaign Creator Dashboard, he can get a list of all contributors for each campaign with their investment amount and time. If the campaign is successful, he can recover the money from the same dashboard.

Investing Ether into Campaigns

After entering a campaign description page, readers can learn about the campaign and provide ether to it. To confirm the sum they wish to invest and the specific account during which they wish to do it, they are going to undergo several reviews . After making all of their choices and investing successfully, an investor would monitor his investments on the investor details page. An investor can claim his campaign-specific tokens from the Investor centre console after a successful fundraising, and if the operation is a failure, he can reclaim the funds he deposited in it. Additionally, he can recover all of his many expenditures if he made them more than one time.

Bibliography

[1] A. Ordanini, L. Miceli, M. Pizzetti, and A. Parasuraman, “Crowd-funding: Transforming customers into investors through innovative service platforms,” *J. Serv. Manag.*, 2011, doi: 10.1108/09564231111155079.

[2] Y. Z. Li, T. L. He, Y. R. Song, Z. Yang, and R. T. Zhou, “Factors impacting donors’ intention to donate to charitable crowd-funding projects in China: a UTAUT-based model,” *Inf. Commun. Soc.*, 2018, doi: 10.1080/1369118X.2017.1282530.

[3] T. Huang and Y. Zhao, “Revolution of securities law in the Internet Age: A review on equity crowd-funding,” *Comput. Law Secur. Rev.*, 2017, doi: 10.1016/j.clsr.2017.05.016.

[4] B. Yasar, “The new investment landscape: Equity crowdfunding,” *Central Bank Review*. 2021. doi: 10.1016/j.cbrev.2021.01.001.

[5] E. Mollick, “The dynamics of crowdfunding: An exploratory study,” *J. Bus. Ventur.*, 2014, doi: 10.1016/j.jbusvent.2013.06.005.

[6] M. Farhoud, S. Shah, P. Stenholm, E. Kibler, M. Renko, and S. Terjesen, “Social enterprise crowdfunding in an acute crisis,” *J. Bus. Ventur. Insights*, 2021, doi: 10.1016/j.jbvi.2020.e00211.

[7] H. Horta, M. Meoli, and S. Vismara, “Crowdfunding in higher education: evidence from UK Universities,” *High. Educ.*, 2022, doi: 10.1007/s10734-021-00678-8.

CHAPTER-12

TECHNICAL BACKGROUND OF BLOCKCHAIN BASED FUNDRAISING PROTOCOL

Dr. Zafar Ali Khan N
Associate Professor & HOD, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: -zafaralikhan@presidencyuniversity.in

Distributed Ledgers

A distributed ledger is a database of assets that are administered by a wide network of users, each of whom has a version of the entire ledger. Traditional data management systems, on the other hand, are concentrated in a single server or company, thereby making them particularly susceptible to cyber-attacks. Nodes are participants in distributed systems that might be actual or virtual, such as businesses, computers, or people. The decentralized ledger's underlying algorithms are considered to as blockchain technology. The term "blockchain" accurately describes the logic behind the mechanism: fresh network operations are collected into blocks, which are then joined with earlier blocks to form a chain including cryptographic signatures. The blocs are linked to one another securely by these signatures. Changing an existing block in the chain would render all subsequent blocks invalid in the eyes of the rest of the network because the cryptographic signature is depending on the chain of all previous blocks [1]. This makes blockchain's ground-breaking financial crime system possible, as no participants would accept transactions starting from a changed version of this chain when a data record is presented.

Cryptography

Distributed ledgers use cryptographic hash algorithms to secure the information they process. The return of a cryptographic hash function is referred or cryptographic signature in this work. A cryptographic hash function preserves the integrity and secrecy of the initial value while one-way aerial imagery from its original size to a fixed size [2]–[4]. In plenty of other words, a hash function represents the function that enables this transformation, and a hash is just the result of a particular input. Mathematical calculations known as one-way functions cannot be computed backwards. Elliptic curves are an illustration of that kind of particular type of function. The proof-of-work computing problems and transactions described in this paper use the SHA-256 hash algorithm technique, which creates a 32-byte (256-bit) hash that is effectively a very significant number (circa 10168) [4]. An asymmetric cryptography methodology based on pairs of keys, the private key and the public key, is used to secure every operation on a blockchain platform. The plan operates as follows: The pair of keys are first generated via a key creation algorithm. Then, anyone who has the public key can encrypt a message, but only the owner of the appropriate credentials can decrypt that communication. A private key is a secret number that is obtained at random and is visible only to its user. It is long enough to defend against brute force attacks. While the public key acts as a user's virtual identity, the private key also can apply distinctive electronic documents to establish ownership of digital assets, agreements, or actions of a given private key owner. Multi-signature arrangements, for instance, are agreements that are secured by cryptography and are signed by multiple parties. The blockchain's users each have their own set of cryptographic keys that they may use to authorize their actions, send and receive private messages, and manage the privacy of their sensitive and intimate data, including their real-world identities. In fact, in conformity with the network's geographic dispersion, sensitive data is never kept on a central server and is always safeguarded by the associated private key, giving the user entire authority and privacy [5].

Consensus Mechanisms

The bitcoin transaction uses a consensus process in place of something like a third party to validate new blocks and appropriately chain them to other ledgers. By setting a threshold number of participants that must concur on the validity of new blocks before they can join the network, this consensus process assures objectivity of the channel for users and newcomers. Proof-of-work, proof-of-stake, and hybrid mining systems are all used by nodes known as miners to manage and vouch for transactions. The blockchain protocol for Bitcoin employs a proof-of-work methodology, which uses an energy-intensive cryptographic puzzle to probabilistically calculate each node's manpower and compensate the first node to solve it [3]. The likelihood of being the first to solve the mathematical challenge, mining a block, and receiving a reward is commensurate to the computer power required to do it. To ensure good behavior and activities of the miners and safeguard the system, incentives like block rewards or credit card fees, both of which are paid in the form of currency value, are used. Game theory predictions about miner behaviors and the suitability of their incentives underlying the security of the Bitcoin consensus mechanism. It is less lucrative to steal from the network than to be a registered miner due to high computation expenses and high mining rewards. However, it is popular for miners to band together into pools to split rewards and reduce the volatility of their earnings, which could obstruct this fundamental dynamic. By adjusting the complexity of the computation puzzle, the issue of rewards can be made depending both mining power and network requirements. A single miner or mining pool needs to control more processing power than the consensus threshold specified by the protocol for the system to become susceptible [6].

The inefficiency of getting multiple miners compete to mine blocks by participating in energy-intensive tasks, yet only the winner effectively mines a block and contributes to the network's decentralized network, continues to be a major downside of proof-of-work systems. To avoid energy-intensive operations or cut down on the time it takes to validate a transaction, alternative consensus mechanisms are being researched. The proof-of-stake system is just the most often used substitute for the proof-of-work approach. Instead than allocating extraction tasks based on the computational capabilities of the miner, this mining protocol does such. Because they are likely to lose the most from a decline in the value of the digital currencies as a result of fraud, the nodes owning the largest shares of the network have the most incentive to preserve its security and viability. When opposed to proof-of-work algorithms, proof-of-stake algorithms have the following advantages: less energy wasted, less chance of computation power takeover attacks, lower entrance barriers and consequent centralization through mining pools, and quicker block validations. However, proof-of-stake systems have several limitations linked to incentive compatibility and lack of objectivity. As a result, each mechanism has disadvantages and advantages of its own, and hybrid systems have been created to combine the best features of each. Delegated proof-of-stake is a different type of system. Although it uses delegate mining machines that are rewarded for desirable deeds and reprimanded for fraud, it is built on the proof-of-state process. The system addresses several issues with pure proof-of-stake algorithms by using things of interest to elect the delegates, such as damage deposit systems. To examine this field's accessibility and security, more studies are required [7].

Bibliography

[1] M. C. Ballandies, M. M. Dapp, and E. Pournaras, "Decrypting distributed ledger design—taxonomy, classification and blockchain community evaluation," *Cluster Comput.*, 2022, doi: 10.1007/s10586-021-03256-w.

[2] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *Int. J. Adv. Comput. Sci. Appl.*, 2018, doi: 10.14569/IJACSA.2018.090354.

[3] J. Wang, L. Liu, S. Lyu, Z. Wang, M. Zheng, F. Lin, Z. Chen, L. Yin, X. Wu, and C. Ling, "Quantum-safe cryptography: crossroads of coding theory and cryptography," *Science China Information Sciences*. 2022. doi: 10.1007/s11432-021-3354-7.

[4] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3052867.

[5] B. T. Hammad, A. M. Sagheer, I. T. Ahmed, and N. Jamil, "A comparative review on symmetric and asymmetric dna-based cryptography," *Bull. Electr. Eng. Informatics*, 2020, doi: 10.11591/eei.v9i6.2470.

[6] W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *J. Cyber Secur. Technol.*, 2017, doi: 10.1080/23742917.2017.1384917.

[7] V. Chamola, A. Jolfaei, V. Chanana, P. Parashari, and V. Hassija, "Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography," *Comput. Commun.*, 2021, doi: 10.1016/j.comcom.2021.05.019.

CHAPTER-13

INTRODUCTION TO TECHNICAL BACKGROUND FOR FUNDRAISING PROTOCOL

Dr. Swati Sharma
Associate Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: -swati.sharma@presidencyuniversity.in

Scalability

Scalability challenges, which are closely tied to security concerns, are critical for the success of distributed ledger solutions. Furthermore, scaling issues are present in many of the fundamental features of distributed ledgers, including the consensus process. The stability of miners' incentive schemes across changes in mining power, the number of participants, the quantity of concerning money, and its distribution throughout the network, for example, is a major worry for the consensus process in public blockchains. The storage capabilities of the participating nodes in the network provide another difficulty in scaling [1]–[4]. Theoretically, every node in a safe blockchain should have a complete copy of the ledger's history on its hard drive. In reality, according to the fundamental logic of blockchains, a consensus mechanism must perform verifications with transaction histories across many ledgers in the network and numerous storage sites are required for this to happen. When high storage capacities become an entrance barrier for miners, the network's consensus becomes centralized and controlled solely by high-capacity storage nodes, weakening the distributed security claims. These storage needs rise as the network grows, leading to elitist network dynamics. In 2009, the white paper for Bitcoin suggested the use of Merkle Trees, a multilevel hashing technique, to reduce the amount of disc space needed by blockchain networks. This storage structure is designed so that nodes may validate transactions without downloading the complete ledger by tying their timestamp to the block header hash28. Using root hashes that include all transactions ensures security. These transactions are organised as a multilevel tree hash, where hashes are connected by an upward propagation technique that may detect changes at any level below the top of the tree without downloading the whole history. As a result, lighter nodes that merely store block headers may coexist alongside complete nodes on the network. While only downloading a tiny portion of the blockchain, these smaller nodes may validate transactions without participating in the consensus mining process. The Merkle tree protocol and its protocol, Simplified Payment Verification (SPV), are essential for the scalability of blockchains.

Scalability issues are growing as a result of how quickly the transactions are being executed. Larger blocks, for instance, allow for quicker transaction processing. Larger blocks, however, need more computing power for the mining process, which once again tends to make the validation task more elitist. Mining is therefore restricted to high-CPU miners, which lessens the decentralisation of the whole process. This reasoning eventually leads to a trade-off between the network's scalability and security or between the danger of centralization and processing speed. The State Channels method of increasing the scalability potential of blockchains seems to promise in this respect. State Channels enable safe transactions to be carried out outside the blockchain by allowing one to block the state of a specific interaction. When necessary, the channel may be closed by returning to the blockchain the outcome of that conversation. A multi-signature agreement, which may be included in a blockchain network, locks the real state of the database, making it only unlockable with a legitimate signature from each party involved. Activities are executed and signed just like they would on the network between these two states, however, they are recorded on an off-chain channel rather than the blockchain. Each transaction is signed, therefore each new signatory from an actor will replace the current one. The pending multi-signature state may be released if the actors return to the last transaction they collaborated on and confirm it by registering it on the blockchain. Thus, just the most recent consensus state is recorded on the blockchain but limitless simultaneous state changes are achievable off-chain, significantly reducing the need for computing capability and disc space.

In a broader picture of a blockchain ecosystem, it is crucial to keep in mind that several blockchain networks with different protocols could be required to coexist in the same area to meet diverse objectives since scalability and security difficulties commonly involve compromises. Blockchains must be able to communicate with one another outside of the marketplaces for transacting althorns in such a setting. Blockchains must be able to move assets associated with their proof of possession30 to other blockchains for this to be practicable. Side chains are cryptographic protocols with this capability; they employ SPV proof as their foundational transferring method to ascertain the history or ownership of another cryptocurrency. By tying side chains' security procedures to linked ecosystems, the author further claims that perhaps the presence of side chains does have the potential to boost security and enhance scalability in comparison to isolated blockchains. The author takes into account several feasible approaches to scalability problems, extending from application-specific to generalized, as the approach discussed above.

Transactions

A crucial component of distributed ledger systems is interaction. It's crucial to bear in mind while examining the whole range of blockchain technologies that monetary implementations are not a requirement for blockchain and that interactions don't always include financial transactions. The word "transaction" may be looser in the context of blockchains than it is in other contexts. It refers to any function performed on the network and may thus take several different forms, such as messages, tokens, calls, or triggers. Any user who is linked to the network may start them and deliver them to another user. The core of the blockchain is unstructured before it is commercial or monetary, as the author of the introduction to blockchain technology states. However, a vital ingredient of many important contemporary blockchain technologies, the majority of which are present in the economic sector, is financial transactions. This is shown by the Bitcoin protocol, which based its understanding of the condition of the world only on transactions rather than concepts of amounts or accounts [5]–[8]. These crypto-economic transactions differ from conventional banking transactions in many ways, including the idea of payment finality. A payment becomes irreversible as soon as it is recorded in the database, and it clears practically immediately with almost no default risk. In comparison to conventional banking institutions, these dramatic improvements in transaction speed and unsustainability constitute large savings in financial intermediation and a gain in security. The transactions are carried out between two network nodes, which might stand in for users, smart contracts, or virtual agents. Each entity has a private key and a public key, which were both produced via cryptography. A hash of the shared secret key creates the public key. A transaction is essentially a change in the ownership of a coin or digital asset that is associated with a specific owner through his shared secret key. An owner forfeits the associated ownership rights if he forgets his private key. The transmitter must use his private key to add a digital signature to an item and connect it to the recipient's public key to start a transaction. If coins are exchanged, each coin serves as an input for the transaction and includes two pieces of data: a distinguishing reference and the owner's private key's cryptographic signature. The reference must be present in the network's greatest recent state and contain the same digital signature as its most recent owner for it to be legitimate. A chain of verified digital signatures detailing the coins or digital asset's ownership provenance would then be present.

Bibliography

[1] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, “Solutions to Scalability of Blockchain: a Survey,” *IEEE Access*, 2020, doi: 10.1109/aCCESS.2020.2967218.

[2] D. Khan, L. T. Jung, and M. A. Hashmani, “Systematic literature review of challenges in blockchain scalability,” *Applied Sciences (Switzerland)*. 2021. doi: 10.3390/app11209372.

[3] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, “Scalability Challenges in Healthcare Blockchain System-A Systematic Review,” *IEEE Access*. 2020. doi: 10.1109/ACCESS.2020.2969230.

[4] A. I. Sanka and R. C. C. Cheung, “A systematic review of blockchain scalability: Issues, solutions, analysis and future research,” *Journal of Network and Computer Applications*. 2021. doi: 10.1016/j.jnca.2021.103232.

[5] X. F. Liu, X. J. Jiang, S. H. Liu, and C. K. Tse, “Knowledge Discovery in Cryptocurrency Transactions: A Survey,” *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3062652.

[6] A. Jabbar and S. Dani, “Investigating the link between transaction and computational costs in a blockchain environment,” *Int. J. Prod. Res.*, 2020, doi: 10.1080/00207543.2020.1754487.

[7] D. Roeck, H. Sternberg, and E. Hofmann, “Distributed ledger technology in supply chains: a transaction cost perspective,” *Int. J. Prod. Res.*, 2020, doi: 10.1080/00207543.2019.1657247.

[8] G. Sladić, B. Milosavljević, S. Nikolić, D. Sladić, and A. Radulović, “A blockchain solution for securing real property transactions: A case study for serbia,” *ISPRS Int. J. Geo-Information*, 2021, doi: 10.3390/ijgi10010035.

CHAPTER-14

THRESHOLD MONITORING

Dr. Zafar Ali Khan N
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: zafaralikhan@presidencyuniversity.in

Threshold monitoring establishes appropriate behaviour thresholds and monitors whether they are reached. This might be as basic as a certain number of unsuccessful login attempts or as complicated as tracking the user's connection time and data download rates. Threshold monitoring defines what appropriate behaviour is. It might be difficult to define invasive behaviour just in terms of thresholds. Establishing appropriate threshold values or appropriate time intervals for checking such threshold values might be challenging. This may lead to a high percentage of false positives, when the system interprets regular use as a possible assault [1]–[4].

Resource Profiling

It creates a historical use profile and monitors resource utilisation throughout the whole system. Unusual readings may be a sign of ongoing criminal behaviour. Changes in system utilisation as a whole may be challenging to understand. A rise in utilisation can just be a sign of something good, like a faster process, as opposed to a security breach.

User/Group Work Profiling

The IDS keeps track of each user's and group's unique work profiles. These groups and users must adhere to these profiles. The user's predicted work profile is modified to reflect changes in his or her activity. Some systems make an effort to keep track of how long-term and short-term profiles interact. Long-term accounts provide a snapshot of usages over an extended period of time, although short-term profiles highlight recently changed work habits. However, a sporadic or fluctuating user base might be challenging to characterize. When profiles are defined too broadly, every activity may pass inspection, but when they are defined too tightly, user work may be hampered [5]–[8].

Executable Profiling

Executable profiling aims to quantify and keep track of how applications make use of system resources, with a focus on those where activity can always be linked back to a single originating user. For instance, it is often impossible to identify the exact user who launched a system service. By analyzing how system objects like files and printers are often used, not only by the customer but additionally by other system topics on the part of users, viruses, Trojan horses, parasites, and other software threats are handled. If malware get full access to user-executable software. The idea of least privilege does not apply to software, which is simply restricted to the rights required for effective operation. This system's open design enables viruses to subtly alter and infect completely unrelated system components. IDS is able to recognize activities that can point to an attack because to executable profiling. Once a possible threat is found, each IDS has its own means of informing the administrator, such as through network message or email.

Intrusion Detection and Prevention in CoAP Wireless Sensor Networks

This assignment assessed the effectiveness of anomaly-based intrusion detection in mitigating DoS attacks against this kind of communication environments in the framework of an IDS framework for something like the detecting and preventing of assaults within Internet-integrated CoAP networks. It is crucial to prevent as many intrusions as possible while simultaneously assuring a low rate of false negatives, even if this implies increasing false positives, in order to develop a Support seamless in Internet-integrated CoAP sensing applications. This must be taken into account when aiming for maximum accuracy. According to the findings, authors can also draw the conclusion that the multi-class problem methodology is appropriate if the security manager is willing to take part in and competent of identifying specific attacks, as findings demonstrate that a linear Kernel or even a polynomial Kernel should provide highest accuracy. On the other hand, the binary class method is effective in identifying the majority of anomalous (ERRONEOUS) behaviours. When a passive IDS found malicious behaviour, it would provide an alert or a log entry but would not undertake any further action. An active IDS, also known as an intrusion detection and prevention system (IDPS), would provide warnings and log entries in addition to having the option of being set up to perform certain actions, such as banning IP addresses or limiting access to certain resources.

In conclusion, they think that the results of their experimental assessment point to the viability of anomaly-based intrusion detection as a defence against external and Internet-based assaults that jeopardise the security and stability of devices in 6LoWPAN and CoAP communication networks. The recommended system may be modified to incorporate more algorithms such as K-NN, Neural Networks, including Random Forests, even though SVM was used as the sole classifier method. In order to further our understanding of this topic, we want to construct and assess various algorithms within the framework that has been proposed. By adopting machine learning models which are more demanding in terms of computing resources like latency, storage, and computation complexity, the inclusion of various methods will also enable the assessment of the proposed system's scalability. Additionally, and from a more pragmatic implementation perspective, the current way of determining the features is another aspect that we aim to target. The computational performance of this step may surely be improved by creating an application that computes attributes directly from the captured data. Future versions will handle more incursions, notably those that try to manipulate the CoAP protocol's use guidelines and semantics, whether they come from internal or external intruders.

Anomaly Detection using Fuzzy Q-learning Algorithm in Wireless Network

In comparison to the Fuzzy Logic Controller as well as the Q-learning algorithm alone, the invention of a classification algorithm algorithmic approach for online IDS identifies DDoS assaults with an accuracy of 85.88 percent. The complexity and dimensionality of the chosen feature sets must be decreased to achieve the desired condition. The simultaneous completion of discretization, extraction of features, and accuracy computation in this study saves time and enables the construction of a more complete detection. The greatest classification accuracy has been found when various parameters are applied to all parameters while utilizing fuzzy Q Learning to identify continuous attack features. A number of data sets, comprising NSL-KDD, CAIDA, and Mixture datasets are used to assess the proposed technique, proving the system's utility in a real-time intrusion detection setting. The proposed technique achieves a higher classification accuracy of 88.77 percentage and a lower minimal cost functional of 65.76 percent throughout the CAIDA dataset when compared to other current detection methods (such as fuzzy logic controllers and Q-learning utilised in wireless networks). Aside from processor speed, power consumption rate, overall response accuracy, other performance indicators like these would be needed to evaluate the IDS's performance due to the wide variety and magnitude of DDoS assaults. An essential area of research in the security industry is novel threat detection.

Bibliography

[1] P. Parthasaradhy and K. Manjunathachari, "Accident avoidance and prediction system using adaptive probabilistic threshold monitoring technique," *Microprocess. Microsyst.*, 2019, doi: 10.1016/j.micpro.2019.102869.

[2] S. wei XU, Y. WANG, S. wei WANG, and J. zheng LI, "Research and application of real-time monitoring and early warning thresholds for multi-temporal agricultural products information," *J. Integr. Agric.*, 2020, doi: 10.1016/S2095-3119(20)63368-8.

[3] M. T. Abraham, N. Satyam, M. A. Bulzinetti, B. Pradhan, B. T. Pham, and S. Segoni, "Using field-based monitoring to enhance the performance of rainfall thresholds for landslide warning," *Water (Switzerland)*, 2020, doi: 10.3390/w12123453.

[4] X. Wu, H. Wang, G. Jiang, P. Xie, and X. Li, "Monitoring wind turbine gearbox with echo state network modeling and dynamic threshold using SCADA vibration data," *Energies*, 2019, doi: 10.3390/en12060982.

[5] C. Yang, D. Chowdhury, Z. Zhang, W. K. Cheung, A. Lu, Z. Bian, and L. Zhang, "A review of computational tools for generating metagenome-assembled genomes from metagenomic sequencing data," *Computational and Structural Biotechnology Journal*. 2021. doi: 10.1016/j.csbj.2021.11.028.

[6] Z. Lu, Y. Hu, Y. Chen, and B. Zeng, "Personalized outfit recommendation with learnable anchors," 2021. doi: 10.1109/CVPR46437.2021.01253.

[7] Y. Y. Chen, A. J. Cheng, and W. H. Hsu, "Travel recommendation by mining people attributes and travel group types from community-contributed photos," *IEEE Trans. Multimed.*, 2013, doi: 10.1109/TMM.2013.2265077.

[8] B. Teater and M. Baldwin, "Exploring the learning experiences of students involved in community profiling projects," *Soc. Work Educ.*, 2009, doi: 10.1080/02615470802478220.

CHAPTER-15

WIRELESS ANOMALY DETECTION

Dr. Mahalakshmi
Assistant Professor, Department of Computer Science and Engineering,
Presidency University, Bengaluru, Karnataka, India.
Email Id: mahalakshmi@presidencyuniversity.in

A wireless sensor network (WSN) is a collection of widely dispersed autonomous sensors that work together to jointly monitor a variety of environmental and physical variables, including noise, pressure, mobility, and pollution. In numerous industrial and civic areas, such as industrial process, control and monitoring equipment health monitoring, environmental and habitat able to monitor, healthcare applications, remote monitoring, and traffic management, WSNs have so far been effectively used.

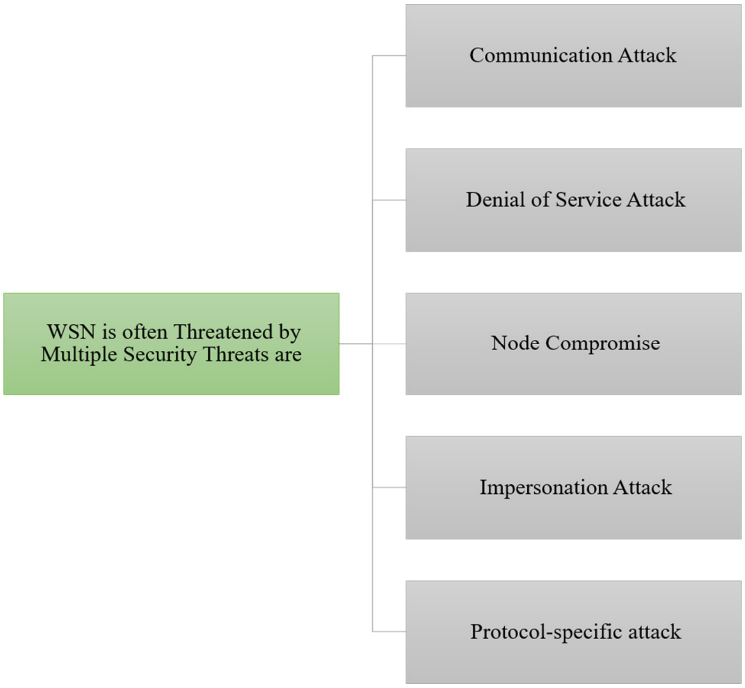

Figure 1: Illustrates the WSN is often Threatened by Multiple Security Threats.

There is minimal to no infrastructure in some kind of a typical WSN. Unstructured WSN deployment is defined as one that is carried out in an ad hoc way. Contrarily, a structured network is one that has been implemented in a pre-planned way. To improve the overall performance of the system, each sensor node has the possibility of being built up with a number of network services, such as localization, coverage, synchronization, data compression and consolidation, and security [1]–[3]. The conventional five-layer communication protocol stack, consisting of the physical layer, layer of data links network layer, transmission control protocol, and application layer, is used by sensor nodes to interact with one another. Due to the inherent characteristics of WSN, a sensor node's access to resources like energy, memory, processing power, bandwidth, and communications is severely constrained. As a result, both internal and external security risks might affect WSN. Additionally, as the network is often built close to the event's medical standpoint, physical access is permitted for sensor nodes. However, due to cost constraints, tamper-resistance is not provided. What's worse, since public communication channels are employed, any internal and external equipment may record the information flow. As a result, a WSN is frequently endangered by a variety of security concerns, which may be divided into the following categories in Figure 1.

A Wireless Sensor Network (WSN) is a collection of autonomous nodes that are connected together by a wireless channel and placed in dangerous or unmonitored environments, such as deep forests, the desert, the ocean, or volcanoes. WSN makes use of a significant number of sensor nodes to gather information on temperature, sound, altitude, humidity, and light in various surroundings. WSN may be used for a variety of things, such as detecting forest fires, monitoring the environment, identifying mechanical stress after an earthquake, mapping biodiversity to observe animals, and keeping an eye on patients in critical care units. Monitoring every sensor node is impossible since they are generally placed in unsupervised places. Therefore, these sensors may malfunction at any moment or a node may be attacked by an attacker, degrading the network and making it difficult to get data from the sensors. We have limitations due to finite resources in terms of energy, memory, bandwidth, and communication, in addition to the failures of these sensors. WSN is often open to several types of assaults. Due to considerations like wireless medium, short transmission range, Ad hoc deployment, toxic atmosphere, and limited energy, security is the main problem in WSN. They have two alternative strategies for securing these sensors in WSN, prevention-based and detection-based [4]–[6].

The prevention-based tactics in WSN serve as the first line of protection against security assaults. The key component of the prevention-based approach is cryptography, which demands greater processing time and resources. As a result, this is not the ideal method for WSN. The detection-based approaches, on the other hand, would be more appropriate since they employ misuse/Signature or Anomaly detection, which needs less time and resources. It describes a collection of the network's earlier anomalous behaviour. Then it searches for assaults that the approach has previously outlined. As a consequence, since the approach only understands the behaviour of assaults that it has already specified, signature-based detection was unable to identify new attacks. On the other hand, the anomaly detection approach builds a model for typical network events by learning the behaviour of the regular environment. The data and occurrences that differ from the usual are referred to as anomalies. A specified set of typical data or occurrences is used in the anomaly detection to identify abnormalities. This kind of variation detection may thus identify assaults that are unknown. Even though anomaly detection has a high detection rate, it often generates false alarms. The tactics used in anomaly detection techniques encompass statistical, clustering, categorization, and artificial intelligence based ones. Naive Bayes, Bayesian Network, Support Vector Machine (SVM), single class Principal Component Classifier, Self-Organizing Map founded on Neural Networks, and Bayesian Network are some of the methods for machine learning utilised so far to lower the false alarm rate to some degree. All of the aforementioned techniques, however, collapse when additional training data are added since the results are drastically altered.

Robust Anomaly Detection

Computer system connection and accessibility have rapidly increased, creating several options for invasions and assaults. Two common methods for detecting computer intrusions are anomaly detection and abuse detection. Anomaly detection, as opposed to abuse detection, which raises an alert if a known attack fingerprint is matched, discovers behaviors that differ from the monitored system's (or users') typical behaviour and hence has the potential to spot new attacks. To record a system or user's typical use pattern and categories new activity as either normal or abnormal, several anomaly detection approaches, including as neural networks (NNs), support vector machines (SVMs), and data mining, have been presented throughout the last decade. These methods may also be divided into generative and discriminative techniques. A model is created using only typical training instances in a generative manner, and each testing case is assessed to see how well it matches the model. On the other side, a discriminative method makes an effort to identify the differences between the abnormal and normal classifications. In training for discriminative methods, both normal and attack examples (attack instances are often uncommon) are used.

Bibliography

[1] S. Rajendran, W. Meert, V. Lenders, and S. Pollin, “Unsupervised wireless spectrum anomaly detection with interpretable features,” *IEEE Trans. Cogn. Commun. Netw.*, 2019, doi: 10.1109/TCCN.2019.2911524.

[2] H. Alipour, Y. B. Al-Nashif, P. Satam, and S. Hariri, “Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis,” *IEEE Trans. Inf. Forensics Secur.*, 2015, doi: 10.1109/TIFS.2015.2433898.

[3] I. G. A. Poornima and B. Paramasivan, “Anomaly detection in wireless sensor network using machine learning algorithm,” *Comput. Commun.*, 2020, doi: 10.1016/j.comcom.2020.01.005.

[4] M. S. Alsahli, M. M. Almasri, M. Al-Akhras, A. I. Al-Issa, and M. Alawairdhi, “Evaluation of Machine Learning Algorithms for Intrusion Detection System in WSN,” *Int. J. Adv. Comput. Sci. Appl.*, 2021, doi: 10.14569/IJACSA.2021.0120574.

[5] A. Ali, Y. Ming, S. Chakraborty, and S. Iram, “A comprehensive survey on real-time applications of WSN,” *Future Internet*. 2017. doi: 10.3390/fi9040077.

[6] P. S. Mehra, M. N. Doja, and B. Alam, “Fuzzy based enhanced cluster head selection (FBECS) for WSN,” *J. King Saud Univ. - Sci.*, 2020, doi: 10.1016/j.jksus.2018.04.031.