5-2023

HANDLING WORK FROM HOME SECURITY ISSUES IN SALESFORCE

Shanthi Sharanya Kode

Handling Work from Home Security Issues in Salesforce

by

Shanthi Sharanya Kode

A Starred Paper

Submitted to the Graduate Faculty

of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science in

Information Assurance

May, 2023

Starred Paper Committee:
Susantha Herath
Lynn Collen
Kasi Balasubramanian

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my research supervisor, Dr. Susantha Herath, Ph.D., for giving me the opportunity to do research and supporting me throughout my project. I am extremely grateful for what he has offered me. I would also like to thank him for his friendship, encouragement and great sense of humor which help me in completion of this project.

I am extremely grateful to my parents for their strong support, caring and sacrifices for educating me and preparing me for my future.

Finally, my thanks go to all the people who have supported me to complete the research work directly or indirectly.

ABSTRACT

"Security" is a vital component when it is identified with an endeavor record or our genuine materials. To protect our home or valuable things like gold, cash we use bank storage administrations or underground secret storage spaces at home. Similarly, IT enterprises put tremendous measure of capital in expanding security to its business and the archives. Associations use cryptography procedures to get their information utilizing progressed encryption calculations like SHA-256, SHA-512, RSA-1024, RSA-2048 pieces' key encryption and Elliptic Curve Cryptography (ECC) calculations. These industry standard calculations are difficult to break. For instance, to break RSA-2048-piece encryption key, an old-style PC needs around 300 trillion years. As indicated by the continuous examination, a quantum PC can break it in 10seconds, yet such a quantum PC doesn't yet exist. Despite the fact that these cryptographic calculations guarantee an awesome degree of safety, there will be dependably a space for breaking the security. Programmers will attempt new techniques to break the security. Thus, the association likewise should continue to utilize new strategies to build the level and nature of the security. Now it is time to check how the security aspect is taken care of when the IT employees are at work from home. The 2020 year has made many professionals work from home because of the Covid-19 pandemic. The Covid-19 has transformed almost all organizations to work from home, this has become standard advice, and technology plays an important role during work from home to monitor the employee works and provide security when the work is being carried away from their respective organization. Employees' information security awareness will become one of the most important parts of safeguarding against nefarious information security practices during this work from home. Most of the workers like the expediency of work from home and the flexibility provided for the employees. But in this situation, workers need guarantees that their privacy is secured when using company laptops and phones. Cyber security plays an important role in maintaining a secured environment when working from home. This work focusses on managing the security break attack in the course of work from home. The focus of the study is on dealing with security breaches that occur when salespeople operate from home. The problem of security isn't new. Security issues existed prior to the lockdown or pandemic, but because the staff was working from the office at the time, the system administrator was available to address them. However, how can an employee's laptop and account be secured when working from home? MFH's salesforce has leveraged a variety of innovative technologies to address security concerns during their tenure. Because the IT behemoth Salesforce has made it possible for all employees, including freshly hired ones, to seek WFH on a permanent basis. To address the security breach difficulties faced by employees, the organization used a number of new approaches, including tracking working hours, raising password difficulty, employing VPN (virtual private network), mandating video during meetings, continuously checking right to use control, and MFA (multi-factor authentication). Improvement of existing multi-factor authentication (MFA) is the focused topic discussed in the thesis. To add an additional step of protection to the login process Blockchain technology is proposed and to identify the employee identification a hybrid recognition model is proposed using face and fingerprint recognition. This leads to the

employee going through multiple processes to authenticate his or her identity in numerous ways in order to access the business laptop. This procedure entails connecting his or her laptop to his or her mobile phone or email account.
Keywords: MFA, WFH, Cyber Security, Encryption, Decryption

Table of Contents

Page

Chapter Page

List of Figures

Chapter I: Introduction

This chapter provides an overview of telecommuting, cloud computing security practices, cybersecurity, encryption, Blockchain technology, and multi-factor authentication.

Flexible hours and any professional work performed outside the organization's workplace is referred to as "work from home". The research effort's idea is to determine what are the benefits and drawbacks of working from a remote location, as well as how to protect remote workspace work. Because of the coronavirus epidemic that began in December of this year, people have been forced to labor from remote locations. On-demand has made a pitch for software that can track employees' schedules during business hours. The majority of employees spend a significant amount of time at home completing tasks that are connected to the organization's regular working hours. These tools have the capacity to enforce management when you can't see over your employee's shoulder. It may be better than nothing for a boss concerned about their employees' taking vacations. Employers must strike a tough balance between corporate needs and employee empowerment. Mann and Adkins (2017) Employee engagement is prioritized by leadership and corporate productivity. Employee engagement is becoming increasingly important to organizational leaders and stakeholders, and they expect their subordinates to go to great lengths to maintain high levels of employee engagement.

Georgiadou et al. (2021) Cyber Security center and worldwide professionals announced proposal and preventive methods that people help people avoid cybercrimes and victims of fraud. With many governments, the residents stay at home, learn,

work, and focus on cyber security. If the employee operates at the remote location, additional security is required. According to Raghav (n.d.), Cyber Criminal uses the COVID19 Coronavirus epidemic, the advantage of uninstalled technology systems, overloaded information technology (IT) experts and new employees working at home. Rawindaran et al. (n.d.) In terms of data protection and security, Cyber Security has a problem with SMEs (SMEs) and SMEs (SMEs). SME networks now have more wired and wireless connections and devices, resulting in more unplanned outages and outages. Debrosse (2019) research says that, Various aspects of cybersecurity and accounting, such as auditing and general accounting work, need to be connected to the Blockchain as soon as possible. Demairkan et al. (2020) studies says that Cloud computing, cloud security, and cybersecurity are all hot topics today. Almost all IT companies use cloud services along with cybersecurity protocols.The core technology of the cloud is encryption, which uses encryption and decryption technologies to provide security.

1.1 Introducing Cloud Computing

Buyya et al. (2011) studies says that, A cloud is used in both private and public affiliations to present a virtual perspective of the association as a single system by aggregating resources across the association, such as sensitive items, programs, informative indexes, various servers, and so on. The term "cloud computing" has become associated with the cloud. Individuals and organizations can employ scattered processing to gain access to these internet resources. Velte et al. (2010), Cloud is a pay-on-demand service that only gives organization to the attached organization. That is only to cover the costs of the previously mentioned support.

The expression "cloud" is a very common phrase that is used in both conventional and explicit areas. During stormy conditions, the cloud plays an important role in people's eyes since it stores all particles for showering the water and allowing people to save the water for future use. Furthermore, it provides a list of information-related working settings for the customer, such as information hoarding, information security, information sharing, and information protection in the future, as well as upgrading and sponsoring. Cloud is an example of a platform that allows a client to store information and applications in one location and access them at any time, regardless of where they are stored.

1.2 CyberSecurity Introduction

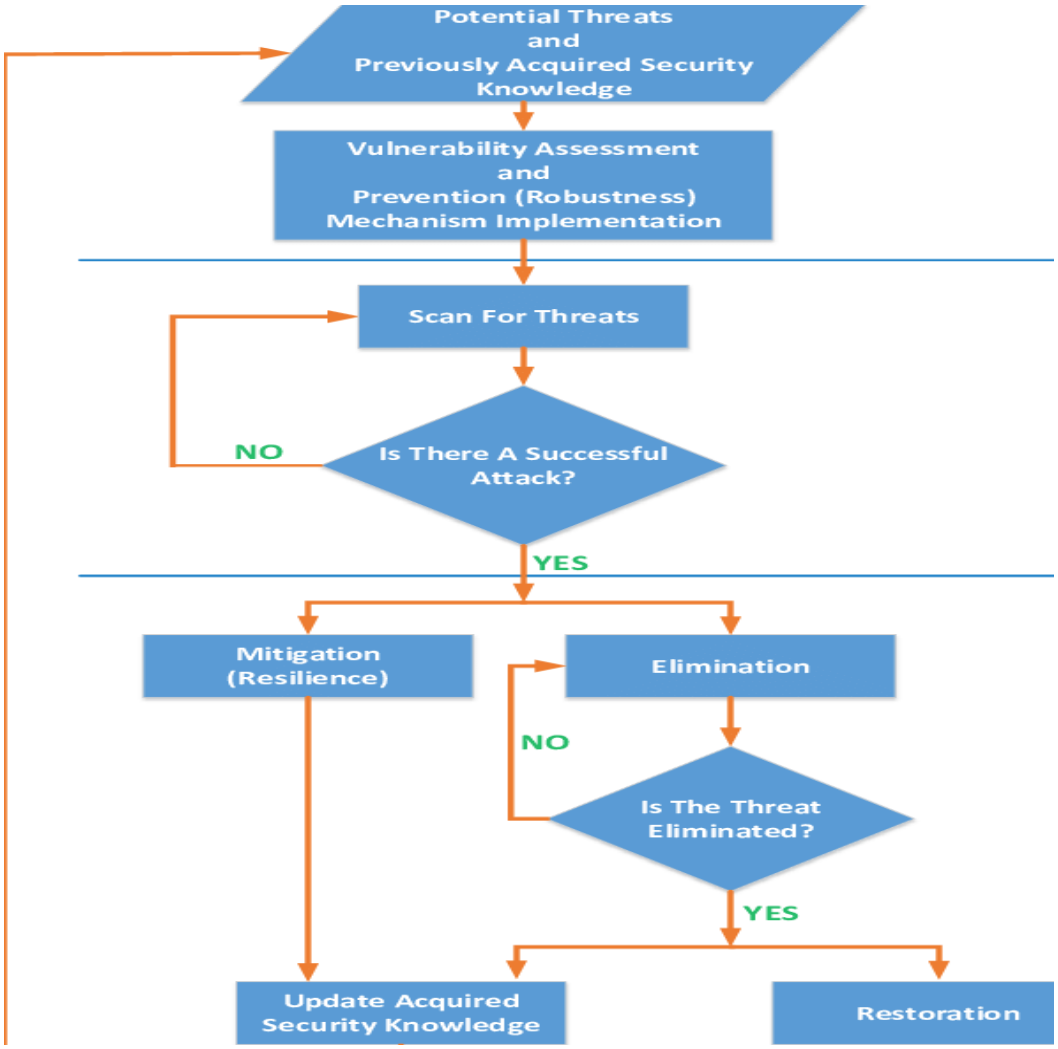
Adams-Prassl et al. (2021) says Due to the COVID-19 hidden danger, a significant rise in attack vectors is directly attributable to the number of persons freelancing or working from home. By having to open attachments, possessing more administrator privileges than necessary, downloading sensitive data onto memory sticks, forwarding emails at work to private accounts, sharing documents they shouldn't, or having access to more data than is necessary, persons are once again revealed as the weakest link in associations. The study focuses on the cybersecurity challenges faced by employees who work from home, as well as the ongoing battle to protect sensitive corporate data and individual personal information away from a normal office setting. Sajal et al. (2019) As a result, this study examines the cyberspace hazards and benefits for companies and individuals when employees work from home. It also provides strategies to stop and lessen this negative cyber influence about telecommuters and the businesses they work for.

1.3 Ensure Backup Data

Data that has been safely copied and kept apart from the original data is called a backup. Backups are useful for fending off intrusion attempts, malware, and malicious scams. To recover deleted data and emails in the event of a problem, a backup is necessary. The finest cyber security measures include routine data backups. Read about backup data procedures and the significance of doing so here.

Figure 1.1

Block Diagram of Cyber Security



1.4 Secure critical emails

Printing a paper to distribute to coworkers is a regular practice at work. Must exclusively use emails when working remotely, though. The best course of action, therefore, be to safeguard them. Email encryption is possible with cloud services, can protect the content of emails send by encrypted them.

1.5 Establish a policy for secure passwords

Passwords are frequently forgotten, even with the most advanced cyber security technologies and procedures. In no way should they be. One of the finest measures for cyber security is a robust passcode strategy. Ascertain that username and password:

- Have a minimum of 8 characters
- Numerals, and capitals in both lowercase and uppercase.
- Avoid having a keyboard, 11111, or similar appearance. In the face of a forceful assault, they will not resist.
- Each 90 days or more revised
- Internal Threats Control

Make absolutely sure the enterprise VPN service expands and can support numerous devices simultaneously. Give commercial clients access to secure video conferencing that includes both audio and video. Connection to organizational business software must only be possible through secure communication channels (SSL VPN, IPsec VPN). According to Protocol (n.d.), Software portal access should be protected using identification and authentication methods. Stop exposing remote system access

interfaces directly to the Internet (e.g., RDP). Salesforce incorporates protection into each and every action to do so that companies can concentrate on expanding and developing. Together along with customers and partners, Salesforce views cybersecurity as a team game and makes the essential investments in everybody's ability to access tools, knowledge, and assistance.

1.6 Introducing Cryptography

Encryption and decryption are the underlying processes in cryptography. Encryption is the process of converting unreadable text material, such as text messages or email, into an unreadable format, known as "cipher textual content". Sahu and Ansari (2017) Encryption and decryption methods are widely used in the IT industry to protect data stored in the cloud. Sun (2019), Because the cloud stores and manages large amounts of data, privacy and security are two important factors. Encryption and decryption are used for this purpose.

Elprocus. (n.d.) Cryptography plays an important role in secure communication and provides an admirable way to compromise essential security against data intruders. As more people use virtual communication strategies, maintaining the confidentiality, integrity, and authenticity of records will become a major issue. There are various strategies for decrypting encryption from time to time to make data extra secure. Encryption is a type of cryptography in which messages or data are encoded and only authorized people can access them. Madhuravani et al. (2013) The word "encryption" comes from the Greek word "Krypton", meaning "hidden" or "secret". Message content can be rearranged or modified here using different numbers, letters, images, etc. to hide

the correct message. The practice of encryption dates back to 1900 BC. It happened from the beginning. Until the 1970s, encryption was widely used by governments and large corporations to share confidential information. However, over time, new methods and algorithms are being used with increasing complexity.

1.7 Introducing Blockchain Technology

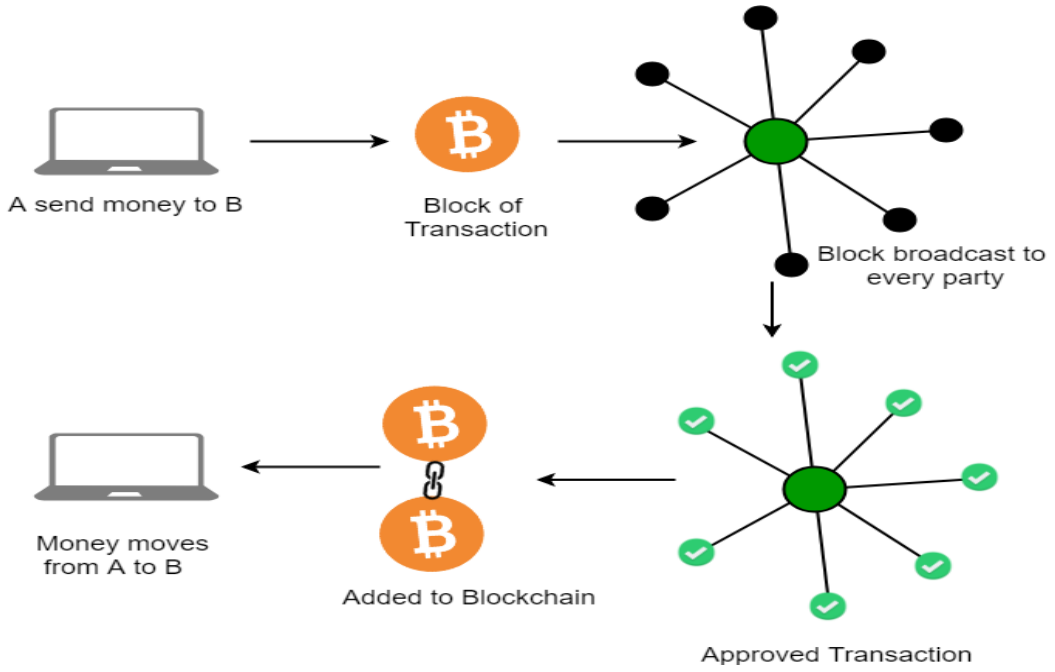
Blockchain technology has gained popularity in recent years due to its unique features such as monotony and flexibility. Radanovic and Likic (2018) The medical, education and IT industries are some of the areas where blockchain is widely used for digital transformation and security. Blockchain (BC) is a well-known public, circulating record that copies the cycle of negotiations in trade associations and subsequent capitals. An entity, be it an automobile, a currency or a terrestrial - or almost anything that can be exchanged in a protected revolution or blockchain network, such as a certificate, patent or design - can be important.

Bitcoin is one of the technologies used for Blockchain transactions. Bitcoin is based primarily on Blockchain formation, which serves as a common record for bitcoin. Consider a Blockchain as a working framework like Microsoft Windows or Mac OS and consider for example, Blockchain allows security to be achieved in minutes instead of days. It can also be used to enable manufacturers to share manufacturing logs with specialized gear manufacturers (OEMs) and controllers to help companies manage production and related installments progress or reduce product reviews. Could not. Bitcoin and black chain are not synonymous. Blockchain provides resources for recording

and storing bitcoin exchanges, but it also includes Bitcoin as well as many other applications. The most common application for Bitcoin Blockchain.

Figure 1.2

Architecture of Blockchain



1.8 Introducing Multi-Factor Authentication (MFA)

Abhishek et al. (2013) says Multi-Factor Authentication (MFA), also known as Two-Factor Authentication, strengthens login information, chance to be working remotely owing to the COVID-19 epidemic (2FA). By doing so, may avoid depending solely on a password to protect data. Credentials are no longer considered to be secure because they are simple to hack, steal, leak, rinse, and repeat; it's time to activate MFA. Having more than simply a password, so that's good. When attempting to log into bank, MFA may have been used to prompt to enter an additional passcode that was sent to

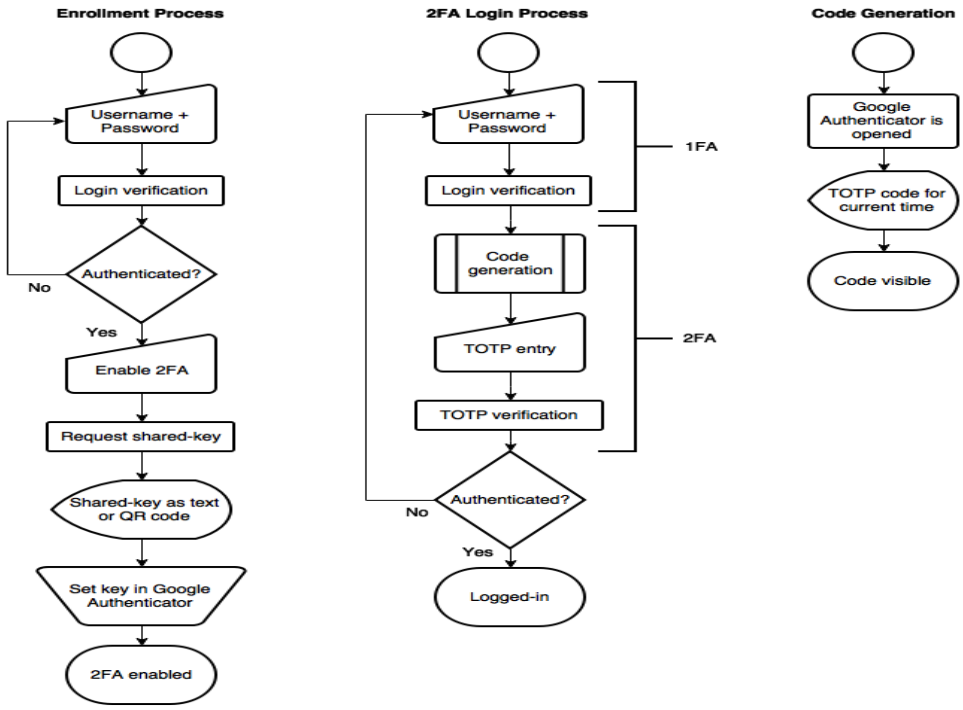
smartphones in order to confirm that were the one who was attempting to log in. It adds a step, but the difficulty for villains increases enormously. Even if they have a password that has been hacked through a breach or another way, they won't be able to login to account with it. Currently, it's likely that carry a mobile device with almost always, which is a strong justification for employing it to strengthen MFA security stance. Because it will be installed on laptops, which now can also be stolen, compromising other security protocols, be sure that whatever select has a highly secured track record. Informational responses to personal protection queries: OTP for passwords (can be both Knowledge and Possession – To know the OTP and have to have something in Possession to get it like phone).

Acquisition

- OTPs produced by smartphone applications
- OTPs delivered by text or email.

Figure 1.3

Flow Diagram of Multi Factor Authentication



- Smart Cards, USB drive, transponders or card holders for access, and cryptographic keys.
- Certifications and technology tokens

Inherence: Speech, face detection, voice commands, optic or retinal scans, or other Biometrics Observation of personality. MFA is now even more essential considering the development of cloud computing. Organizations that shift their systems into the cloud are no longer able to rely on the protection of a user literally being on the same network as a system. To make sure that malicious users are not gaining access to the systems, more security precautions must be put in effect. By requesting extra identification elements that are more challenging for cybercriminals to copy or crack using brute force

techniques, MFA can assist guarantee that individuals are who they say they are since they can connect these services from anywhere at any time. While customer use of internet platforms has considerably expanded during the epidemic, they are also more worried about just the risks of online fraud and identity theft. A most crucial factor for 71% of consumers when registering a new account is security. Thankfully, using one-time passwords is a simple technique that is generally known and approved by clients. One-time passwords are (at least) familiar to 92% of respondents, according to the report, and 86% of respondents said they are handy. Eighty-six percent of consumers (consumers) agree that OTP is reliable. Zand and Gupta (2021) According to this, consumers regard two-factor authentication as familiar, simple, and secured, with 81% of respondents saying they are accustomed with that as well. Salesforce offers straightforward, creative MFA alternatives that strike a balance between high security and user ease. To meet company and user needs, to offer a variety of secure authentication options, along with the smartphone device for Salesforce Authenticator, third-party time-based one-time passcode (TOTP) authenticator apps, and encryption keys that are Internet authentication and U2F compatible.

Research Gaps

Continuous improvement in the number of excellent contractions and related company loads has affected the versatile clothing that can be reliably delivered anywhere across the planet. In such a relevant world, regardless of authentication, the attractive effect of keeping sent data is secure. According to Venkatesh et al. (2020), The login consists of steps where "the client identifies itself by sending X to the structure; the system

accepts its role by nominating F (X) and making sure that it climbs the set of Y values". From an information development standpoint, although the term mystery is not a major part of the straightforward way of supporting clients, this definition has not changed in a long time. Authentication is the focal protection for devices or any other sensitive application, whether it is isolated or online, from unwanted permissions.

The Newyork Times (2020), Since the onset of the COVID-19 pandemic, nearly 70% of IT industry employees have been working from home for the past 3 years. To protect employees' laptops from security breaches such as hacking laptops and identity theft; Requires a solid login method. Thesis selected the case study of the sales force company, which can give employees permanent work from home based on request. Now, this is a matter of some concern to the company in terms of employee benefit and safety. Employees work remotely, so need constant monitoring and support. Multi-factor authentication (MFA) plays the first step in providing security where the employee is identified by the login method. Multi-factor authentication (MFA) is a rigorous course of certification that requires multiple verification processes that navigate the autonomous classification of verifications.

The Problem's Nature and its Importance

The proposed methods are useful for identifying the employee who has logged into the system. As an improvement on extended encrypted passwords stored in the blockchain. Block chain still provides the highest level of security in the current security market. MFA's current methods use facial recognition or fingerprint recognition or multi-

device login. The proposed work would include facial recognition, fingerprint identification and multi-device login to identify employee identities.

The objective of the proposed research work:

1. Make a comparative study of current technologies used in Multi-Factor Authentication (MFA).
2. Implement two-tier security for storing passwords using encryption and Blockchain technology.
3. Develop a hybrid recognition model using facial recognition and fingerprinting as the first step in the authentication system to create multi-factor authentication (MFA) on laptops.
4. For MFA Second Phase Design, Password Login on Laptop, One Time Password for Mobile and Face Recognition via Mobile Phone.

Study Questions/Hypotheses

Study Question/Hypotheses:

- Hypothesis 1: Technology plays an important role during work from home to keep track of the employee works and provides security.
- Hypothesis 2: Employee's organization laptop secured with proper monitoring tools can avoid security issues.
- Hypothesis 3: Using cyber security technologies Employees' privacy will be secured when they are using organizational resources.
- Hypothesis 4: Employees' tracking tools used during work from home is to increase work efficiency without any chance of organization economy downfall.

Definition of Terms

1. MFA (Multi-Factor Authentication)

   Multi Factor Authentication (MFA) is a validation method that requires the client to provide at least two validation variables in order to be sufficiently close to an asset such as an app, online account, or VPN. MFA is a key part of your identity and Access to Executives (IAM) strategy.

2. Encryption

   Data encryption is a technique for securing information by encrypting it in a way which can only be retrieved or decoded by someone who has the right cryptographic keys. Data that has been encrypted can seem distorted or unintelligible when someone or something reads it without authorization. Information encryption is the method of turning data from a readable format to an unintelligible string of characters. This is done to prevent snoopers from viewing sensitive data in motion. Any kind of connection across a system, including papers, data, and communications, can be encrypted. Cleartext or unencrypted refers to the information that has to be encoded. A few encryption algorithms, which are essentially theoretical computations performed on unprocessed data, must be applied to the unencrypted before it can be transmitted. Numerous encryption methods exist, and each one has a lot of different things and protection ratings. An encryption key is also necessary in addition to the techniques. The plaintext is transformed into encrypted data, generally known as encrypted message, using stated key and an appropriate encryption technique. The ciphertext is transmitted

via insecure channels of communication rather than the recipient receiving the unencrypted. The recipient can employ a decryption key to return the ciphertext to its original, plaintext-readable version once it has been delivered to them. For this decrypt key to work, must always remain confidential and could or could not be the same key used to decrypt the communication. Public key encryption demonstrates ownership of the private key by the origin server of a website, demonstrating that the servers is genuinely the owner of the SSL certificate that was issued to it. This is a crucial characteristic in a world filled with scam websites. Data encryption privacy by preventing anyone outside the intended recipient or data owner from reading messages or accessing data. With the help of this protection, personal information is shielded from thieves, hackers, internet service providers, spammers, and even official organizations. Verification and validation, Many sectors of the economy and government entities have regulations in place requiring businesses to handle user personal data to keep that data secured. HIPAA, PCI-DSS, and the GDPR are a few examples of the legal and compliance requirements that forbid cryptography. Since the ongoing coronavirus (COVID-19) outbreak, numerous businesses over the world have implemented work-from-home policies. This is the present employment reality. The use of cloud-based apps and remote logins to enterprise networks by employees has grown as a result. However, this change can also make it more prone to security attacks and online crimes. Having talked about how businesses will need to be on the lookout for hazards brought on by work-from-home policies and linked home gadgets in

one of the security predictions for 2020. Peripheral devices may become corrupted and act as jumping off sites for supply management operations, obscuring the limits of security policy. Make an arrangement for working from home in advance. Develop explicit rules for telecommuting that are in line with corporate policy after evaluating cybersecurity. Provide employees with intrusion prevention and security versus information theft and loss, particularly using corporate laptops that have IT approval. Allowing, work remotely using a business tablet. Avoid using personal computers because they can have weaker security safeguards than the technology that an organization owns. Employees should use only computers or other devices provided by their employer; may block access to homes for family and friends.

3. Blockchain Technology

According to Yang (2019), Blockchain technology is an innovator technology that is creating a great number of impacts on the current world from its spectacular contribution towards quality, decentralization, and security assets. Blockchain technology has attained reasonable level of popularity because of its primary app of Crypto values for example, Tad coin. In the upcoming years, Blockchain technology is likely to change the mode of living, cooperation, and accomplish better quality of company’s businesses. Newly, academicians, businesspeople, and scientists are massively working away at different features of Blockchain as an appearing technology. Blockchain is developed by Santoshi Nakamoto's in 2008, in the form of a digital currency called bit coin crypto currency. From then, more than 2000 digital forms of money are existing now in the market. Block chain

technology can be certainly applied in various areas because of its exceptional combination of features.

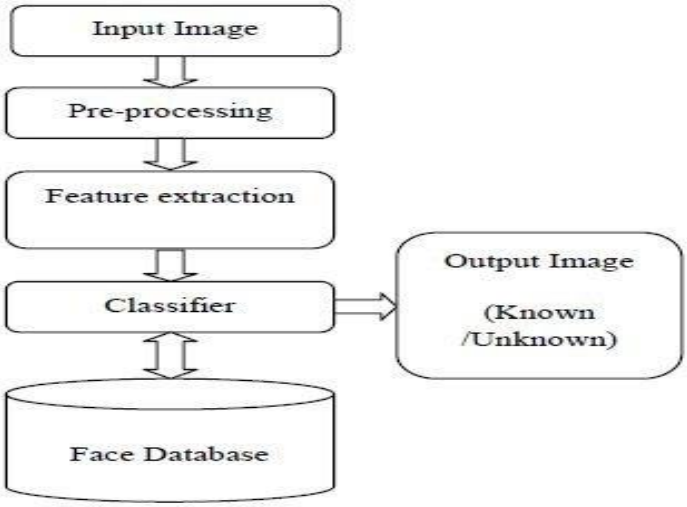
4. Face Recognition

Identification by face is the simplest way. Face recognition is one area that is receiving a lot of attention from researchers due to its many practical applications in monitoring systems, mobile payments, enhanced security, and law enforcement. The difficulty of remembering passwords and pins makes them prone to forgetting. Theft, counterfeiting, or corruption are possible with cards, tokens, or keys. Nobody can forget, lose, or steal a human face. The elements required to create a system for face recognition that is both practical and relevant.

- Accurate identification should be possible with a high degree of precision.
- The system should operate quickly from detection through recognition.
- Whatever the physical conditions—lighting, luminance, ageing, etc.—the image should still be recognizable.

Figure 1.4

Block Diagram of Face Recognition



A face's traits are recognized using a local binary pattern histogram technique in digital image processing and computer vision. In 1990, a prototype of this method was shown. LBP approach is discovered to have significant influence in texture classification. Combining the LBP and Histogram descriptor will consistently and accurately increase detection performance. In a picture, a specific function is given to every other photon. For a 3x3 pixel, a threshold value is chosen, and surrounding values are subjected to it; if they are higher, they are shown as one, otherwise as blank. A textural description is obtained from local regions that have been generated. As implied by the development's name, AI is the foundation of it. The AI application in question is a prototype. The preferred location, Salesforce Einstein Platform, is where the educated data model is kept. I set up an account there. Two APIs, notably the Visual API and the Linguistic API, are available to use with the Einstein platform at the moment. There have been several instances of

algorithmic prejudice revealed by the use of facial recognition technology, raising concerns about its legitimacy and transparency. Consider the picture detection algorithm in Cloud Storage that revealed racial biases or the face-scanning system that sparked controversy over its effectiveness and the lack of clear guidelines for handling individuals who'd been mistakenly recognized. It would seem prudent to pay attention to the following rules when developing and utilizing systems that recognize faces. And now for six essential ones: Equity, dependability and security, Discretion and safety, Egalitarianism, Accountability and Transparency.

5. Fingerprint Recognition

   The unique confirmation of the fingerprints checks the fingerprint hint in the mechanized recognition strategy or verifies the personality of personality caused by two fingerprints from the impression of your fingers is one of the most prominent biometric agents and is a wide stock of the most relevant biometric response to check the upgraded framework.

6. One-Time password

   One-time Password (OTP) is a naturally generated number or alphanumeric series that identifies the client for its own exchange or login. OTP can be used independently or as an alternative to login credentials to add another layer of security.

7. Authentication

   Validation is a term that alludes to the method involved with demonstrating that some reality or some record is veritable. In software engineering, this term is

normally connected with demonstrating a client's character. Typically, a client demonstrates their personality by giving their accreditations, that is to say, a concurred snippet of data divided among the client and the framework.

Summary

The construction of theory incorporates the Introduction, Literature Review, Methodology, Study region and Data set utilized, Results and Discussion, Conclusion and References.

Part 1 – This segment presents the foundation of the issue, inspiration for finding answer for the issue and careful issue proclamation for this undertaking theory. It further expresses the exploration goals which the theory endeavors to accomplish.

Part 2 – This section talks about the general work done by different scientists with respect to the issue articulation, for example expanding the viability of encryption, Blockchain and MFA effort.

Part 3 – The section depicts the different approaches used to accomplishing the ideal destinations and the legitimization for choosing above philosophies.

Part 4- This section covers result discussion and analysis.

Part 5- This section explains the conclusion remark.

Chapter II: Background Related to the Problem

Introduction

The literature used in this starred paper is primarily from managing, tracking, and securing the workspace, with some key concepts relating to the COVID-19 issue and critical to analyze what has been researched earlier in order to develop a sound basis for our research. The aim of this study was to fill up the gaps and add to our understanding of remote workers' workplace engagement experiences. The findings offer organizational leaders the tools and knowledge they need to better understand how to manage remote workers' levels of engagement. In this chapter literature and knowledge base on remote worker, engagement is reviewed. We focused our literature search as much as possible on peer-reviewed papers, mostly utilizing Google Scholar and the survey on related articles.

a) Review work on Block Chain Technology

Just about 10 years prior Satoshi Nakamoto (2008), the obscure individual/bunch behind Bitcoin, depicted how the blockchain innovation, an appropriated distributed connected construction, could be utilized to take care of the issue of keeping everything under control of exchanges and to stay away from the twofold spending issue. Morkunas et al. (2019) Bitcoin orders exchanges and gathers them in an obliged size structure named blocks having the equivalent timestamp. According to Zhou et al. (2020), The hubs of the organization (diggers) are answerable for connecting the squares to one another in sequential request, with each square containing the hash of the past square to make a blockchain Along these lines, the blockchain structure figures out how to contain a hearty

and auditable vault, everything being equal. Blockchains acquainted genuine disturbances with the customary business measures since the applications and exchanges, which required unified structures or confided in outsiders to check them, would now be able to work in a decentralized manner with a similar degree of assurance. The intrinsic attributes of block chain engineering and configuration give properties like straightforwardness, power, auditability, and security. A block chain can be viewed as a conveyed information base that is coordinated as a rundown of requested squares, where the serious squares are unchanging. One can see that this is ideal in the financial area as banks can collaborate under the equivalent block chain and push their clients' exchanges. Thus, past straightforwardness, block chain works with exchanges' evaluating. Organizations put resources into this innovation as they see the capability of making their designs decentralized and limiting their exchange costs as they become intrinsically more secure, straightforward and at times quicker. Thus, block chains are not simply publicity.

According to Wu and Duan (2019), the quantity of digital forms of money shows Block chain's significance, presently surpassing 1900 and developing. Kaushik et al. (2017) Such a development speed could before long make interoperability issues because of the heterogeneity of digital money applications. Xie et al. (2019) Moreover, the scene is quickly developing as block chain is being utilized in different fields past digital currencies, with Smart Contracts (SCs) assuming a focal part. SCs characterized in 1994 by Szabo as: "a mechanized exchange convention that executes the details of an agreement", permit us to make an interpretation of legally binding statements into

embeddable code hence limiting outside cooperation and dangers. Casino et al. (2019) studies say that, In this way, a SC is an arrangement between parties which, in spite of the fact that they don't believe one another, the concurred terms are consequently implemented. Accordingly, inside the block chain setting, SCs are scripts running in a decentralized way and put away in the block chain without depending on any confided in power. Specifically, block chain-based frameworks supporting SCs empower more intricate cycles and communications, so they build up another worldview with for all intents and purposes boundless applications. Accordingly, Blockchain innovation is turning out to be progressively pertinent. Very nearly 1000 (33%) of C-suite leaders pronounce that they are thinking about or have as of now been effectively drawn in with block chains. Analysts and engineers are now mindful of the abilities of the new innovation and investigate different applications across an immense range of areas. In view of the target group, three ages of block chains can be recognized: Blockchain 1.0 which incorporates applications empowering computerized cryptographic money exchanges; Blockchain 2.0 which incorporates SCs and a bunch of uses reaching out past digital currency exchanges; and Blockchain 3.0 which remembers applications for regions past the past two adaptations, like government, wellbeing, science and IoT.

Centralization is a cycle where the power to make choice lies in the possession of a couple. All in all, "Centralization" is the reliable and deliberate method of entrusting power to individuals who are in the focal point of the association. The world's monetary framework that utilizes public fiat monetary forms which are made and overseen by government supported national banks is a brought together method of managing

money. Though a decentralized design is autonomous of any unified power and in this manner dispenses with the requirement for a national bank. On account of bit coin, each client in the organization has a duplicate of a record/record that monitors all exchanges occurring in the bit coin network and their proprietorships. As each client in the organization has a duplicate, it is viewed as a conveyed record and in bit coin network, this is accomplished utilizing block chain. Disseminated Ledger Technology (DLT) has drawn in far and wide consideration lately. DLT is a straightforward, disseminated, secure information stockpiling and moving innovation that works with no incorporated confided in outsider. A circulated record is a decentralized data set that is kept up with by a few hubs over a distributed organization. The record is checked and reproduced by every hub. Blockchain is one type of DLT.

According to Savelyev (2018), Blockchain frameworks are regularly grouped into three classifications: public block chain, consortium block chain and private block chain. The public block chain is permission less block chain, while both consortium block chain and private block chain are permissioned block chain. In the public block chain, anybody is permitted to join the organization, take part in the agreement cycle, peruse and send exchanges, and keep up with the common record. Norton (n.d.), Most digital forms of money and some open-source block chain stages are permission less block chain frameworks. Bitcoin and Ethereum are two delegate public block chain frameworks. Bitcoin is the most well-known cryptographic money that is made by Satoshi Nakamoto in 2008. Ethereum is another delegate public block chain that upholds broad decentralized applications utilizing its Turing-complete brilliant

agreement programming dialects. The consortium block chain frameworks are by and large utilized in business space to record cross-authoritative deals. Unique in relation to public block chain frameworks, consortium block chain frameworks just permit approved substances to take an interest in the agreement cycle. The private block chain is a disseminated yet incorporated organization that is claimed by an association or substance. Permissioned block chain frameworks can be additionally separated into two classifications: public and private permissioned block chain frameworks. Both public and private permissioned block chain frameworks permit just the approved elements to partake in the agreement interaction, send exchanges, and keep up with the common record. The principal contrast between them is that public permissioned block chain frameworks permit anybody to peruse exchanges in the common record, while in the private permissioned block chain frameworks, perusing exchanges is likewise confined to the approved substances. Most block chain frameworks created for business are permissioned block chain frameworks. Hyper ledger Fabric is an agent permissioned block chain framework. Hyper ledger Fabric is a Linux Foundation project created for business. Hubs in the Hyper Ledger Fabric are partitioned into approving companions and non-approving friends. The approving friends are answerable for approving exchanges, taking part in the agreement cycle and keeping up with the record by running the Practical Byzantine Fault Tolerance (PBFT) agreement convention. Non-approving friends are permitted to peruse and confirm exchanges.

b) Review of encryption techniques

Friebel et al. (2017) Encryption is the assignment of taking irrefutable text-based substance, like a literary substance message or email, and scrambling it into a muddled organization known as "figure text-based substance". This empowers safeguard the secrecy of virtual records both saved money on pc structures and sent by means of a local area actually like the web. At the point when the implied beneficiary gets to the message, the measurements is made an interpretation of again to its bona fide structure. This is known as unscrambling. To deliver the message, each the sender and the beneficiary should utilize a “confidential" encryption key. A gathering of calculations that scramble and unscramble records again to a meaningful configuration. Encryption and unscrambling procedures are broadly utilized in IT areas for securing the information put away in mists. Security and insurance are the two vital focuses identified with the cloud information stockpiling as cloud stores and keeps an enormous amount of information. For this reason, encryption and decoding are utilized.

Cryptography plays an imperative capacity in stable verbal trade, and it gives a commendable technique to think twice about fundamental security contrary to the records gatecrashers. As the utilization virtual methodologies for conveying, it will end up being a key difficulty that the best approach to keep up with the privacy, trustworthiness and validness of records.

The intention in conveying encryption is to oversee information access from vindictive gatecrashers in the organization. A most reasonable stable security highlights are to deal with the secrecy, honesty, accessibility and openness. Having the mix of

square chain and encryption gives greater security to the information. Dai et al. (2018) studies says that, Symmetric encryption calculations can be classified into stream codes and square codes where the picture pixels are encoded individually in stream codes and utilizing squares of pieces in block figures. Even though square codes use more equipment and memory, their exhibition is ordinarily better to stream figures since they have a stage just as a replacement stage. Radwan et al. (2016) Because of the great affectability of turbulent frameworks to boundaries and beginning conditions just as the accessibility of many circuits acknowledge, bedlam-based calculations are created and concentrated as the center of encryption calculations. Bushwick (2019) says that on the opposite side, non-turbulent strategies have shown their essence and position in executing the disarray and dispersion stages. Such strategies generally increment the calculation intricacy to ensure against cryptanalysis. Albeit the two pieces of this framework are designated "keys," the public key is more similar to an opened lockbox: anybody can drop something in, or encode a mysterious message, however just the private key's holder can open the container or unscramble the message. This course of action makes such deviated cryptography safer than a symmetric framework—one that is more similar to an opened lockbox (security relies upon keeping the crate stowed away, in light of the fact that an individual who can get to it to drop in a message can likewise get to its substance). Alabdullah et al. (2021) says Consider symmetric cryptography, a more perplexing rendition of a replacement figure: if the message is encoded by moving each letter of the letters in order ahead by three spots, one can decipher the code by just moving each letter back by three. That capacity implies any

individual who realizes how to set up the code can likewise figure out it. Conversely, public-key cryptography utilizes numerical calculation to produce significantly more intricate keys so the code can't be run in reverse along these lines. Distinctive public-key frameworks can use various calculations, if they depend on numerical issues that are not difficult to institute however difficult to figure out.

c) Background related to MFA, encryption and blockchain technology.

Kebande et al. (2021) of them examine gives a Blockchain-primarily based Multi-Aspect Authentication structure for vehicular clouds and Cloud-enabled IoV that leverages an embedded digital Signature (MFBC eDS). in this paper writer has proposed MFBC eDS version includes a scheme that integrates the safety announcement Mark-up Language (SAML) with Single Sign-On (SSO) abilties. MFBC eDS makes an important contrast to Karla and Sood's cautioned baseline authentication mechanism. An embedded Probabilistic Polynomial-Time algorithm (ePPTA) and a further Hash characteristic for the Pi generated during Karla and Sood's authentication were developed and studied based totally at the foundations of Karla and Sood's scheme. the writer concludes the proposed method is higher suitable to counter big adverse attacks in some IoV-focused surroundings primarily based at the Dolev–Yao adverse model even as pleasant additives of the Confidentiality, Integrity, and Availability (CIA) triad, consistent with an early study of the proposition.

Ometov et al. (2018) examines the evolution of authentication structures from single-thing Authentication (SFA) to Multi-Component Authentication (MFA), starting with single-element Authentication (SFA) and progressing through two-issue Authentication

(TFA) (2FA). The authors are expecting biometrics is one of the essential layers with the intention to enable MFA within the destiny. While validating the user, it is assumed that combining two or greater authentication procedures will provide a better stage of protection.

Bruun et al. (2014) said that from the point of view of usability, evaluate single-issue versus multi-element authentication methods, comparing the usability of various authentication mechanisms in tabletop environments. The writer makes suggestions on which authentication tactics to utilize while growing tabletop gadgets and person interfaces. Inside the proposed paintings, best degree of usability turned into performed via combining a TUI and a PIN (TaPi). regardless of the truth that TaPi authentication became now not the fastest, participants thought it was the maximum cozy. possession-based totally TUI prototypes had been notably quicker than the expertise-based totally. The writer offers the information on MFA is conduct-based biometrics imparting totally new ways of authenticating the customers.

Kwon et al. (2019) in this study suggest a three-step method to authenticate the user using a multi-factor security framework. In this paper for secure device-server connection, technologies like Argon2 were utilized for hashing picture characteristics and physically not clonable identification. In the proposed model, the author evaluates the model's usefulness in real-world applications, analyzes the suggested model qualitatively, and compares it to existing methodologies.

Aydar et al. (2020) in this study a safe encryption process uses the owner's biometric signature to encrypt and decrypt the private key. The author discusses

Biometrics and a secret sharing technique that is used to provide an effective recovery process. Asset owners can securely store their keys on their devices and retrieve them if they are lost by using the suggested key encryption and recovery technique.

Aydar et al. (2020) This study discuss two-factor authentication and Blockchain technology to transfer 2FA by moving the centralized network into a decentralized Blockchain network. The emergence of 2FA solutions based on Blockchain technology is unavoidable as more Internet-of-Things devices require authentication credentials and consumers build their repository of usernames and passwords for accessing web services.

Pal et al. (2021) in this study talk how Public Key Infrastructure is utilized in Blockchain era to authenticate the entities and to ensure the integrity. This text discusses an outline of Blockchain, an examination of present Blockchain PKI, and key control for Blockchain wallets. a group Key control method for comfortable institution conversation is likewise offered to hold the secrecy of touchy files over the Blockchain network.

Booba et al. (2021) in this study add security features to forensic data by sending an e-mail notification for each piece of data contributed via the SMTP protocol, as well as an access key to the authorized person who can view the forensic evidence. A basic scenario has also been included to recover forensic evidence if the data has been tampered with, with the hash value in the tampered and untampered reports on the blockchain being compared.

Pise et al. (2021) in their study discuss how the security of data and storing techniques are enhanced using Blockchain technology. Also, the author discusses how

SHA-512 is used in the hashing algorithm where data security is necessary, including throughout the rest of your paper. message digest, password verification, digital certificates, and Blockchain. The author concludes to the major properties of this method; the Advanced Encryption Standard (AES) is used to encrypt and decrypt data.

Zhai et al. (2019) in their study discusses on the current state of Blockchain security is examined and future research directions are expected.

Dasgupta et al. (2016) in this paper, recommend the evaluation 3 distinctive variations of face considered. It also compared to two popular and significantly used MFA structures, FIDO and Microsoft Azure, and it became found that the recommended MFA plays far better than its competitors. This article discusses several authentication parameters to protect against fraud including PINs and passwords. This article discusses HP Client Security Manager is a software-based solution that allows administrators to boost security by requiring two authentication factors, such as a password and a fingerprint or a smartcard and a PIN.

This article gives information on how many users find it difficult to remember strong passwords, they resort to using weak or default passwords, putting their data at risk. Multi-factor authentication protects against fraudulent logins by anyone with access to one type of sensitive data. To better safeguard against identity fraud, how a variety of factors can be used, such as. What the user is aware of (passwords or PINs) Something the user possesses (Bluetooth® phones or smartcards, for example). something that the user is concerned about (facial or fingerprint recognition) HP Client Security Manager is a

software program that helps you protect your computer HP Client Security Manager, which supports two authentication methods, and allows users to manage their identities.

Yew et al. (2018) in their study show how to use cloud computation offloading to create a fast facial recognition system. Hassan and Elagazzar (2016), The author proposes before offloading the recognition to the cloud, the architecture performs preliminary image processing on mobile devices to decrease network traffic and conserve battery power. On the mobile device, preliminary results reveal a 230 percent reduction in overall response time and a 200 percent reduction in energy use.

Jarrahi and Sawyer (2013) According to many types of research, team collaboration that is actually or remotely distributed increases employee productivity. Hacker et al. (2019) As a result, an important question is, does virtual teamwork better than a face-to-face team? Several studies have summarized the input factor models and their interactions with other variables, which are divided into socio-emotional and work-based processes and their relationship to output factors.

According to the article the start of the coronavirus pandemic, 26% of HR leaders have employed some type of software or technology to follow remote workers, according to Gartner Research (2018) research released in June. This is up from 16% in April when the epidemic was only beginning to spread. Employee computer activity, employee e-mails or internal communications, employee phone usage, and employee location or movement are all monitored as part of the tracking. Because they see that remote work is here to stay, many leaders are considering using such technologies. According to

Gartner Research (2018), 47% of firms expect to allow employees to work from home full-time in the future.

Ometov et al. (2018) in this study explain that most of the people of modern smart electronic gadgets have a microphone, permitting voice recognition to be used as an issue in MFA. At the equal time, destiny technological advancements can also allow special corporations to not best understand audio system but also to duplicate their voices, inclusive of intonation, timbre, and other aspects, that is a considerable drawback of the use of voice as a major verification method additionally of their Facial popularity may be considered as a future stage. The era changed into based totally on landmark image evaluation at the start of its development, which was reasonably clean to recreate in reality providing the device with an image. The next step became to permit three-dimensional facial reputation, which required the person to transport their head in a unique way in the course of the authentication manner. Sooner or later, this gadget stepped forward to the factor where it may apprehend the consumer's real expressions [88]. it's far important to equip the system with as a minimum one output device and a digicam to allow facial reputation.

Literature Related to the Methodology

Background study on MFA to monitor employee work from home

Ometov et al. (2018) in their paper propose and implement a multi-factor authentication system. The authors speak about evaluating the system in terms of the evaluation matrix of simplicity and performance against various types of attacks. Nakamoto (2008) In the proposed system of this paper selects two of the four stages

required for successful system login at random. In this system, the mathematical gauge is used against the brute force attack. Authentication methods such as SofToken, RFID, QR-Login, and biometric techniques are used for comparing the proposed system.

Fahim et al. (2020) in this study author proposes the security box to monitor continuously the current location and addition with this MFA identifies and ensures the documents with a biometric sensor with fingerprint and a keypad for the authentication. The author analyzes the risks associated with the proposed system and explains how extenuation increases the system's reliability. The author concludes individuals and organizations have long been concerned about security will result in significant funding being budgeted for security system reformation.

Nath and Mondal (2016) authors of this study conducted a thorough investigation on various issues and challenges that are related to the use of two-factor authentication algorithms. The authors also talked about how two-factor authentication could be standardized for industrial use biometric, OTP, salting, verification etc. The author predicts that the two-factor authentication method is easy to use because it has little software requirement. Further, the author concludes that the proposed method of authentication is more efficient allowing for simple database interaction.

Yew et al. (2018) research identifies technological flaws and proposes a method for detecting cheating. This study examines attendance fraud and proposes to change common smartphone features as a preventative measure. For attendance authentication, the proposed method requires a combination of several factors: QR code (unique event identifier), IMEI code (unique token), time stamp (time limit) and GPS location (location

limit). Hopeful ability in implementation and possibilities to take attendance have been shown. This is a very promising cost-effective approach to detect attendance irregularities automatically and in real-time, making fraud very attractive and easy to spot.

Background study on Blockchain to monitor employee work from home

Sifah et al. (2020) This study examines attendance fraud and proposes to change common smartphone features as a preventative measure. For attendance authentication, the proposed method requires a combination of several factors: QR code (unique event identifier), IMEI code (unique token), time stamp (time limit) and GPS location (location limit). Hopeful ability in implementation and possibilities to take attendance have been shown. This is a very promising cost-effective approach to detect attendance irregularities automatically and in real time, making fraud very attractive and easy to spot.

Saxena et al. (2021) This study discusses the basic concept of blockchain as well as security issues in blockchain technology. We talked about the basics and features of blockchain, and then I talked about the current security issues in blockchain technology that future researchers will use in their research. In this paper, we discuss the application areas of blockchain technology that will be used to improve technology in the future. Blockchain applications in a wide variety of industries, from finance to non-finance. Non-financial sectors include health care, education, business and industry.

Haque and Rahman (2020) predict how various security issues arise from different types of Blockchain networks, such as private Blockchain networks commonly used by businesses and large firms. The private Blockchain concept focuses on the network, which is vulnerable to cyber-attacks. The author explains the amount of power required

for hash computation leads to a more cost-effective and efficient Blockchain network than trying to develop a better consensus algorithm.

Background study on cyber security to monitor employee work from home:

Al-Mohannadi et al. (2018) in this study the author investigates all IT employees' awareness of cyber security threats, with a focus on three domains knowledge, monitoring, and prevention. The author explores that there is a knowledge gap between the Security operation team and other IT experts that needs to be bridged. SOC teams are generally capable of protecting against cyber security threats if they can identify them.

Moussa (2015), in this study explores how new technologies have not only provided organizations with reasons to monitor employees' behavior, but they have also provided new methods and techniques for performing employee monitoring. As a result, technology should be approached with caution and discretion. Employers should be aware that employees may retaliate against the organization for what they perceive to be unfair monitoring practices. As a result, when implementing new technologies to monitor employee behavior, it is critical to consider a wide range of concerns (e.g., privacy, needs, and aspirations). Educating employees about the reasons for monitoring them, developing a wide range of policies and procedures, and effectively communicating with them will be critical to success.

Michaelides (2021) in this study predicts that examining the effects of remote working on mental health, wellbeing, and cyber security behaviors reveals a complex and nuanced set of effects on employee performance and attitudes. Maurer (2020) A review of the literature on employee cyber security practices during the pandemic, based on

existing research on remote working and employee behavior, reveals a wide range of consequences, including employee fatigue, reduced productivity, inadequate risk awareness on remote working cyber security principles, and several implications for the psychological contract. Examining employee relations through the concept of the psychological contract highlights the importance of re-examining unspoken contracts and understandings between employees and organizations in the new context of remote working, as well as researching how leadership styles may need to change.

Summary

- In the review of literature, a depth survey has been carried out on encryption, Blockchain technology, and MFA as individual technologies. Recent articles published on these areas are considered to perform the survey.
- The existing underlying technology support for MFA is studied and written the recent works carried on MFA using encryption and MFA using Blockchain technology is covered.

Chapter III: Methodology

Introduction

Chapter 3 covers the methodology section of the proposed research work. It includes the designing of the objectives, definition of proposed objectives, how the objectives are implemented, tools required on each objective's coverage, information regarding data collection, hardware and software requirement details.

The objectives of the proposed research work are listed below:

1. Make a comparative study of current technologies used in Multi-Factor Authentication (MFA).
2. Implement two-tier security for storing passwords using encryption and Blockchain technology.
3. Develop a hybrid recognition model using facial recognition and fingerprinting as the first step in the authentication system to create multi-factor authentication (MFA) on laptops.
4. For MFA Second Phase Design, Password Login on Laptop, One-Time Password for Mobile and Face Recognition via Mobile Phone.

Design of the Study

The plan of the research work is listed below in a step-by-step manner:

1. Step 1: Make a comparative study of current technologies used in Multi-Factor Authentication (MFA).
   - The first step is to do a deep survey on existing underlying technologies in multi-factor authentication (MFA).

- Different organizations use different methods to implement the MFA process.
- Some MFA processes are proprietary to the IT industry, and some are open-source and available to the public to be known.
- To implement MFA the existing methods, combine the company device(laptop) login plus mobile phone login to identify the employees or laptop login linked to the email account login.
- A survey paper article will be written on this objective.

2. Step 2: Implement two-tier security for storing passwords using encryption and Blockchain technology.
    - In the second step, a two-level security model will be developed using encryption and blockchain technology to store the password of employees.
    - The existing security models of authentication mechanism stores the employee password using encryption.
    - In the proposed research work, to improve the existing authentication security model, the concept of blockchain technology is introduced.
    - In the current technology of the security market, blockchain provides the highest security.
    - Every employee of the company will be given a unique username and password.
    - This password will be encrypted, and encrypted hash id will be stored in the blockchain. From the blockchain, a unique tracker id will be issued to the employee.

- When the employee tries to log in, in the first step password will be verified through encryption and blockchain.
- In the last step, the employee has to enter the tracker id for authorization.
- The motive of storing the password in the blockchain is that no one changes the password, and it cannot be breached by anyone.

3. Step 3: Develop a hybrid recognition model using facial recognition and fingerprinting as the first step in the authentication system to create multi-factor authentication (MFA) on laptops.
    - In the third step of methodology, for the MFA process face recognition and fingerprint are combined to identify the employee.
    - If both are true, then only the employee can proceed to login into the system.
    - The photo and fingerprint of the employee will be stored in the database for cross verification.
4. Step 4: For MFA Second Phase Design, Password Login on Laptop, One-Time Password for Mobile and Face Recognition via Mobile Phone.

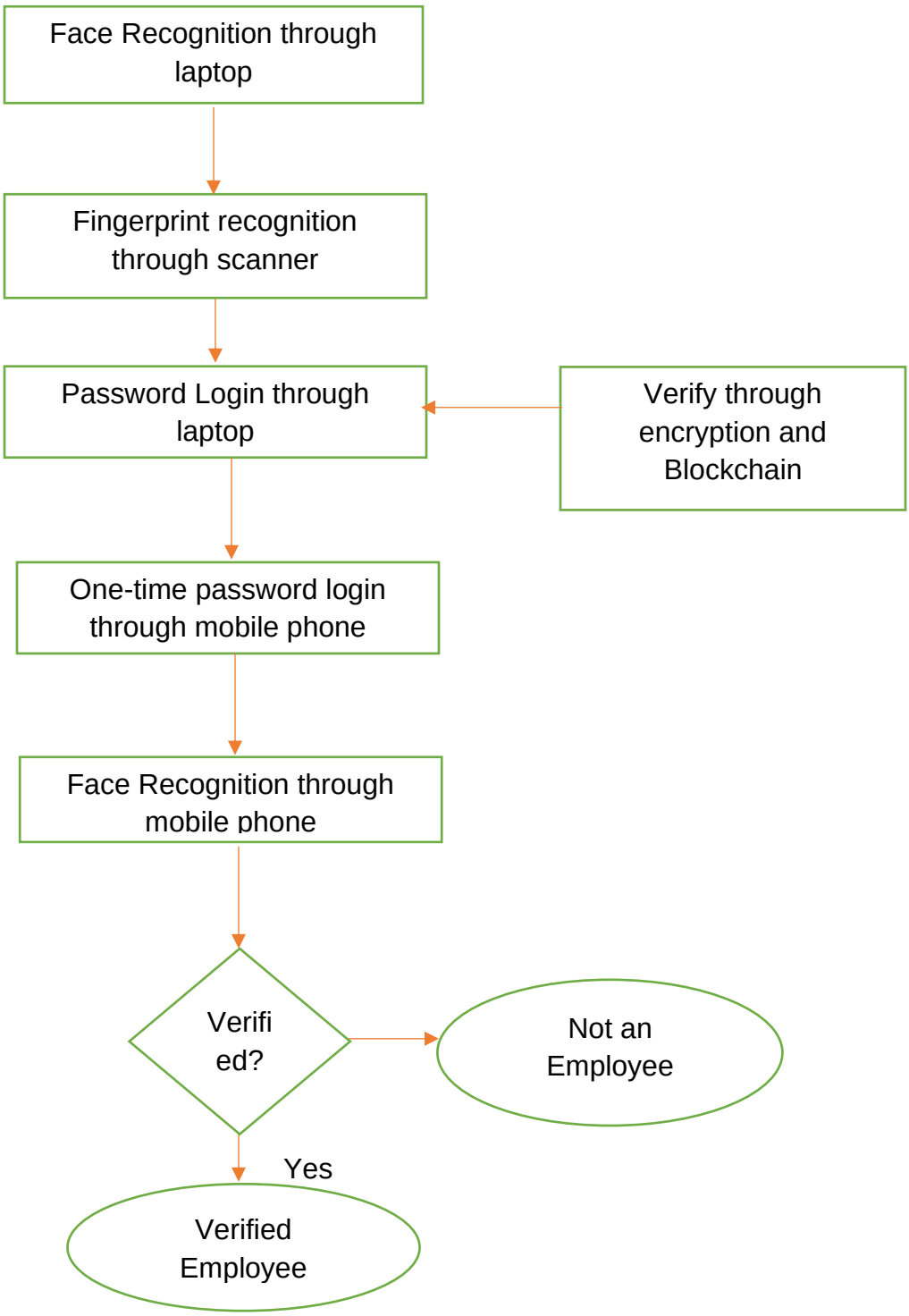
- As the second process of MFA, password login in laptop where password will be cross verified through the hybrid security model of encryption and Blockchain. If this step is true, then the employee can proceed time the step of one-time password to mobile and then again perform face recognition through mobile phone.
- The security model and the MFA are developed in hybrid in nature where multiple techniques are combined. The proposed method is expected to achieve more efficiency than the existing encryption-based MFA techniques.

The workflow of methodology is as follows:

1. Once the laptop is ON, the employee’s face will be cross checked.
2. If the face of the employee is validated correctly, then through the employee has to give the fingerprint and it will be cross validated with the database stored fingerprint.
3. Once step 2 is true, the employee can proceed with the login process in laptop by entering username and password. The password will be dross validated using the security model of encryption and Blockchain technology.
4. If step 3 is true, then a one-time password is sent to the employee’s mobile.
5. If the one-time password entered is correct, then through mobile camera once again the face of the employee is validated with the database stored photo.
6. If step 5 is true, the employee is the true employee and allowed to login into the laptop or else the login will be declined. The manager of the employee will be intimated if the login is declined.

Figure 3.1

Block diagram of the proposed work



Data Collection

For the data collection need an organization's employee personal details. After receiving the employee names, a set of credentials will be created. Then an encryption and Blockchain based security model will be developed. Using the hybrid model of encryption and Blockchain the credentials of the employees will be stored and tested.

Tools and Techniques

Tools required:

- Open-source Blockchain tool
- Laptop with front camera
- Touch screen Mobile phone with front camera
- Tools will be added as per the requirement during the implementation.

Techniques used:

- Multi-Factor Technology
- Encryption Technique
- Blockchain technology
- Face recognition
- Techniques will be added as per the requirement during the implementation.

Hardware and Software Environment

Software requirements:

- Windows operating system with minimum 8 GB RAM. Code for encryption algorithms and open-source code of Blockchain to create blocks for each employee. Software components will be added as per the requirement during the implementation.

Hardware Requirements

- Laptop with front camera
- Touch screen Mobile phone with front camera
- Hardware components will be added as per the requirement during the implementation.

Work in Progress

As of now, the work is on learning and studying the underlying technologies required to implement MFA. On the learning process of encryption and blockchain technology. Even working on a survey article paper on the analysis of existing methods and technologies used in multi-factor authentication (MFA).

Timeline

The total estimated timeline required is estimated to be 4 years. The initial 6 months are for surveys and survey articles. Next 6 months for objective 1 and one research article. In next year's objective, 2 and one more research article will be written. It's next year's objectives 3 and 4 with another research article will be written.in the last planned thesis on the research work will be written.

Chapter IV: Data Presentation and Analysis

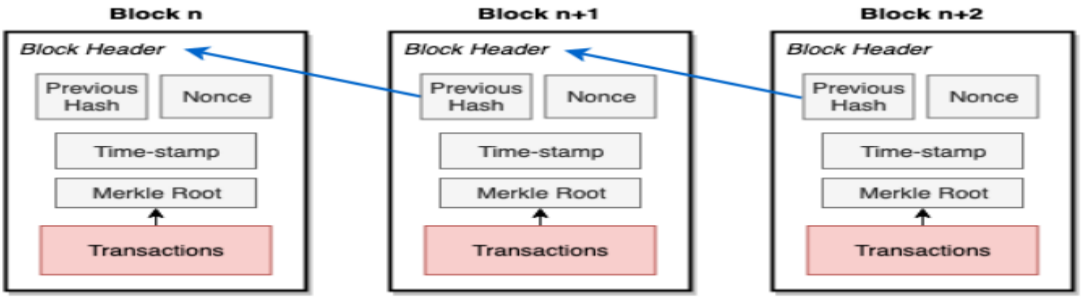
Implement two-tier security for storing passwords using encryption and Blockchain technology.

A decentralized, securely shared data ledger is what the term "blockchain" refers to. Data sharing is made possible by blockchain technology among a small set of people. Transactional data from many sources may be quickly gathered, integrated, and shared through blockchain cloud services. Cryptographic hashes are used to create distinct identities that are used to chain together shared blocks of data. Blockchain eliminates data duplication and boosts security by providing data integrity with a single source of truth.

The primary use case for blockchain technology was to enable cryptocurrencies, with Bitcoin serving as its first notable success. A set of nodes, known as miners, maintain a trustless, decentralized transaction database, also known as a ledger, called the blockchain. Each node executes a consensus process. All transactions are stored in this database in blocks that are arranged chronologically. Any type of data can be transferred through transactions, which are not just used for monetary transfers.

Figure 4.1

Architecture of Blockchain



A reference (hash) to the previous block is included in each block along with a set of transactions, their Merkle representation, a time stamp, the solution to a challenging mathematical puzzle that is used to validate the data included in that block, and a series of transactions. After the entire block has been hashed, the hash also known as the block header is appended to the following block, forming a chain of blocks hence the name "blockchain."(Figure 4.1)

A key component of information security is digital identity management. It serves as the foundation for most forms of online accountability and access restriction. By lowering the chances of unauthorized access to personal information and data breaches, it helps to preserve privacy. Digital identity is the starting point for any identity management system. Electronic data includes digital uniqueness. A person’s particular characteristics that are linked with them are recognizable within a certain situation.

Digital uniqueness Contains three different types of data:

Identifiers: Identification numbers, such as those found on a passport, email address, social security number (SSN), or employee number, are examples of identifiers.

Credentials: a collection of information serving as proof for identity claims, such as digital certificates, SAML assertions, and Kerberos tickets.

Attributes: information on the subject's traits, such as name, age, birthdate, job title, and residence.

Authentication using Blockchain technology

Proposed Methodology

Blockchain technology is regularly described as an impenetrable technology as it gains acceptance in many different industries. Many believe that information held in a blockchain is, and will always be, safe because of decentralization and encryption. This chapter looks at various security concerns relating to blockchain technology to provide readers with a better understanding of all the dangers that may be posed to the most popular blockchain platforms.

Since the creation of bitcoin, blockchain technology has found numerous uses in industry as a less expensive and more secure method of managing a distributed database for Security level.

The main objective is to propose an artifact of MFA that uses text- and image-based authentication elements to protect the authentication process of an entity in the AUTH coin protocol. The AUTH coin protocol's security is built on blockchain technology, which maintains the challenge requests and responses on the ledger and keeps them transparent and undamaged so that other entities can examine authentication-related information. The initial binding is more trustworthy between an entity and her/his claimed domain, email, or other belongings since MFA may employ four types of evidence

(knowledge, possession, inherence, and context of an authentication candidate) to authenticate the user.

Figure 4.2

The design-science research framework

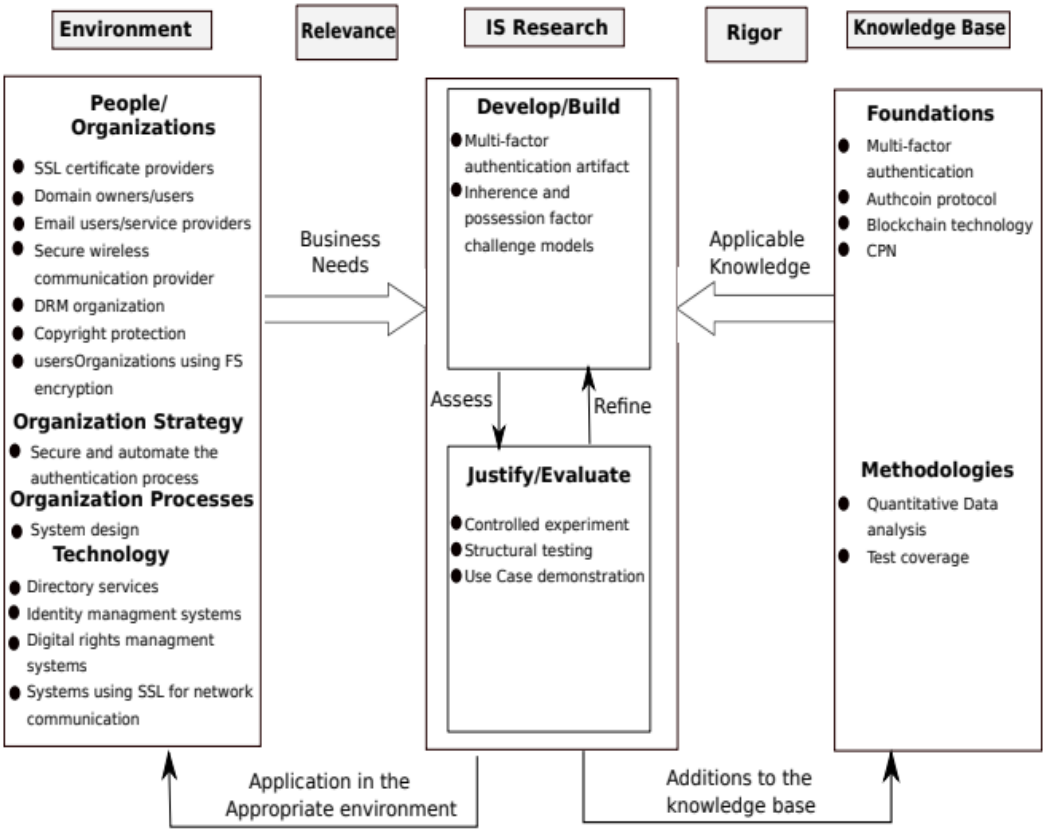
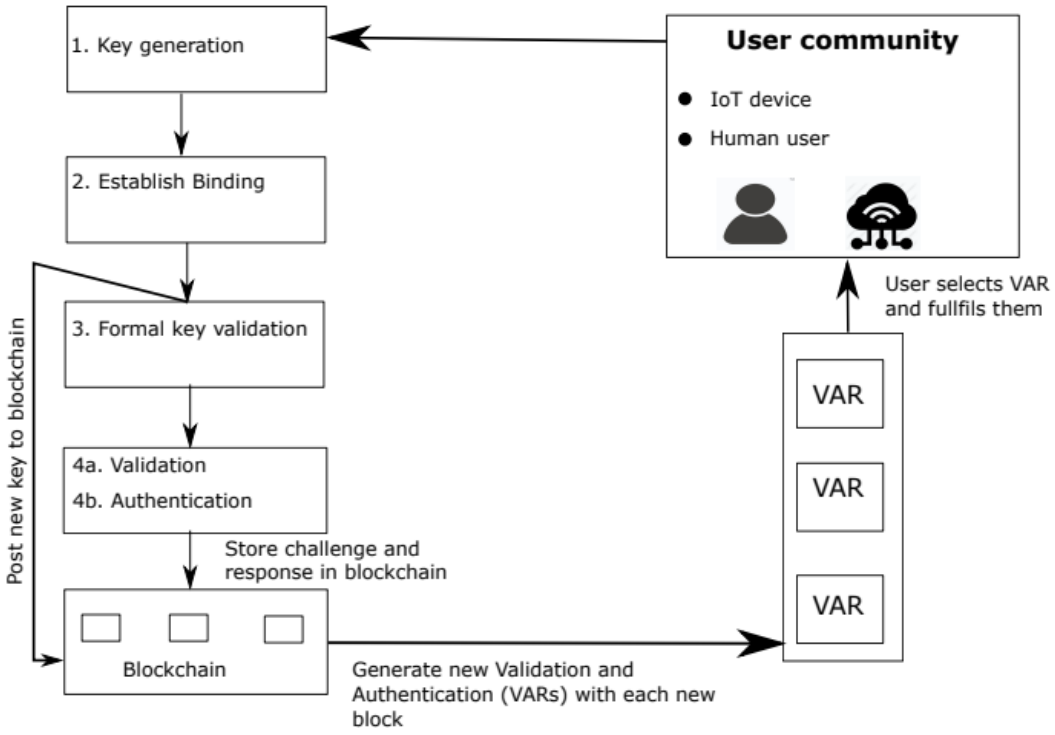


Figure 4.2 shows the design framework of the proposed model. The environmental needs are represented by the left column in the artefact. People, organizations, technology, organizational processes, and strategy all make up the surroundings. The foundations and methods employed in the creation of the item are provided in the knowledge base column on the right. By being applied to the environment, the generated artefact serves the initial requirement while also adding to the body of knowledge.

MFA technology may employ four different types of factors: You have (token, OTP, or encryption key), someone has (username, password, passphrase, or PIN), someone is (biometrics or the user's behavior), and someone's context (location, time or IP address)

Figure 4.3

Workflow of using Blockchain using AUTH coin Protocol.



Blockchain is the storage technology that AUTH coin employs, and the transactions inside the blocks are the real data that must be saved, including challenges, keys, signatures, responses, and other pertinent data. Blockchain is made up of blocks that are chronologically connected and cannot be altered once data has been added. Each block has a header, which contains any metadata, and content, which stores any transactions. The network must come to an agreement when a new block is added to the

blockchain for the addition to be successful. The most popular procedures for reaching consensus are proof-of-work, which is used by Bitcoin, and proof-of-stake, which is used by Ethereum. Since the hash of each block is based on the hashes of earlier blocks, altering a block is not conceivable because it would never be recognized as authentic by other miners.

A smart contract on the Ethereum blockchain is an executable piece of code that is put to the blockchain, where it remains unchanged after that. The agreements have the code, account balance, and storage and are designed to coordinate and enforce the terms of negotiations between two parties.

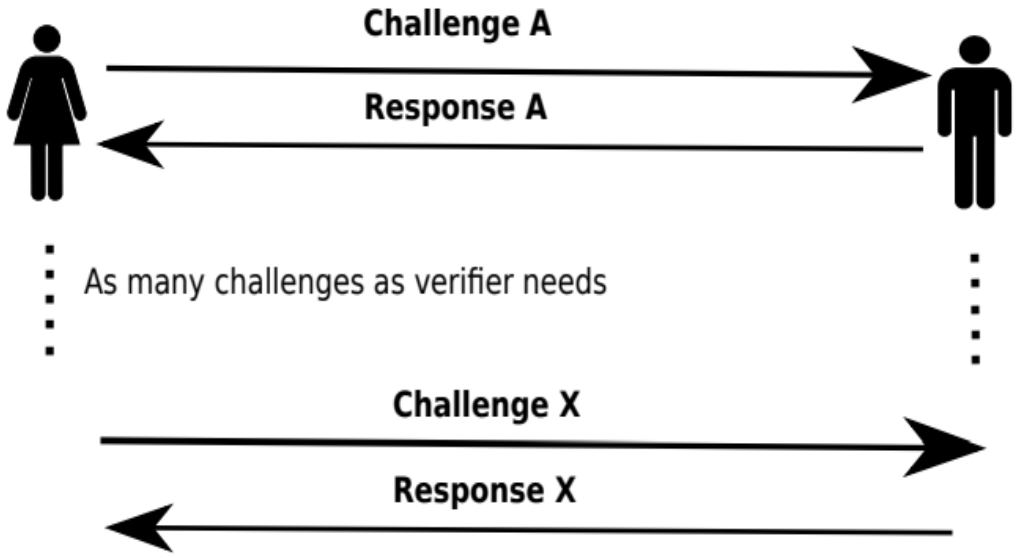
In order to read from or write to storage, the code may be used when a message is received. The account balance can be used to send and receive money through contracts. Additionally, contracts have a gas that is required to run code, preventing the use of endless loops. Contracts are compiled to bytecode before being uploaded to the blockchain.

AUTH coin protocol's MFA process in action

Automatic VARs and normal authentication via challenge-response between two entities are the two situations in which authentication is employed in the AUTH coin protocol. In the figure that is shown, it is assumed that the verifier does not have access to the digital versions of earlier responses, making it impossible for him or her to compare the response that was received to anything. In Figure 4.5, the only person who can independently verify the received response is the verifier.

Figure 4.4

Verification between two persons



In the context of AUTH coin, this chapter discussed user authentication security levels and how to select a user authentication method. A straightforward MFA procedure between entities was also provided. However, the risk assessment and instructions offered for selecting user authentication are only meant to serve as general recommendations and do not ensure that authentication will be secure. The workflow for MFA is also made simpler due to reliance on the context in which Authcoin is used, as numerous variables, including the user, the authentication factor, and business and technological constraints, may change.

Summary

To produce, manage, distribute, store, cancel, and generally use their digital certificates, AUTH coin users can use MFA. Since the user can be either a human or a machine and in-person registration may not always be possible for them, level three

authentication, which typically allows using MFA with biometric and password, is the best option for AUTH coin, according to the results of the risk assessment 8 that was conducted.

Depending on the verifier's trust, we concluded that the MFA procedure can involve numerous rounds of challenge-response messages between two AUTH coin users.

Chapter V: Results, Conclusion and Recommendations

Cryptography application in Blockchain with results and discussions

The blockchain's fundamental cryptography technologies are discussed in this subsection. They are the Merkle tree, hash pointer, digital signature, and cryptographic hash function.

Hash Function: A mathematical operation known as a cryptographic hash function produces fixed-length alphanumeric strings from any input string (data) regardless of length. The output string is also known as a checksum, digest, hash value, or digital fingerprint. Additionally, the output is both set in length and singular. Regardless matter how many times it is recalculated; the function always generates the same hash from the same data. Since the hash cannot be used to recover the input data, it can be used to verify the accuracy of data.

Collision-free, hidden, and puzzle-friendly are the hash function's three key characteristics. It is highly unlikely to find two messages with the same hash that are collision free. For instance, no matter how many times the hash of a string x is calculated, the hash of a string y is always different. Puzzle-friendly refers to the ease with which a hash of given data can be calculated, while hiding refers to the impossibility of finding x from a given hash of x.

Hash Pointer: The term "hash pointer" refers to a pointer that points to a location where data and its digest are stored. It is merely a hash that is used to refer to a different piece of known data that may be used to validate the data digest, in other words (data has changed or not). The hash pointer can be used to create data structures such as the

blockchain, which is a linked list of hash pointers, and the Merkle tree, which is a binary tree of hash pointers.

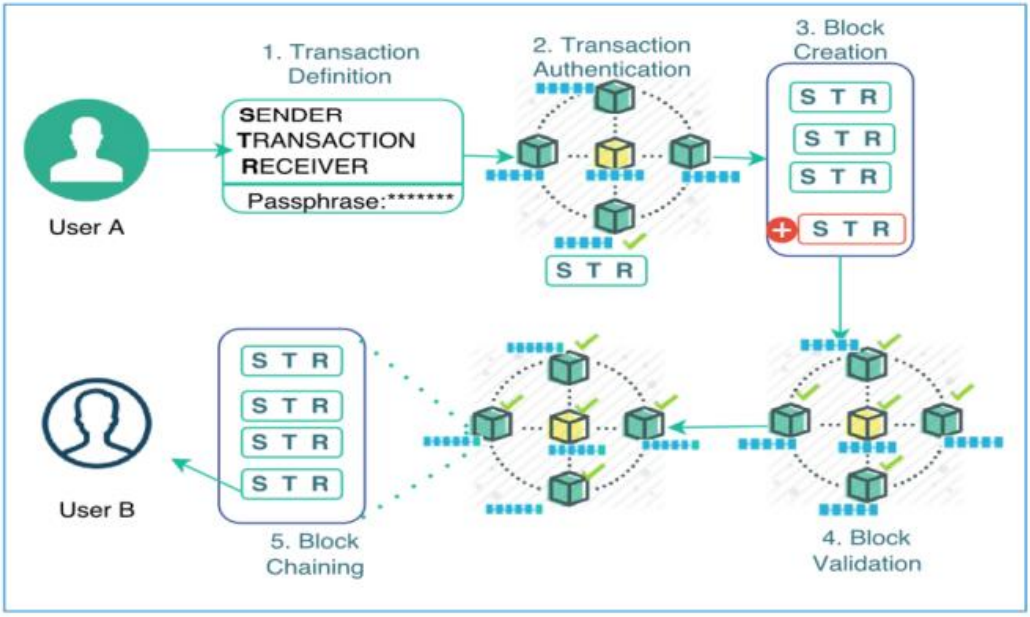
Digital Signature: A further component of the blockchain is the digital signature. It employs public-key cryptography to ensure the authenticity, integrity, and nonrepudiation of a message and its source. Nonrepudiation is the obligation of a message transmitted and received by the parties. Similar to a manual signature, which can only be issued by the signer and is valid for other users, it has these characteristics. Users can verify a message that has a digital signature attached to it, but only the owner of the signature can sign the message. Additionally, digital signatures are produced by means of public key cryptography. A combination of a public and private key is used as the key in public key cryptography or asymmetric cryptography.

Merkle Tree: With a peer-to-peer (P2P) network, fresh data must be propagated and validated throughout the network while each peer must have the same copy of the data. Data propagation and verification across P2P networks need time and money to compute. Therefore, the Merkle tree is utilized, which enables for the secure and effective verification of larger data structures while still guaranteeing data integrity. Instead of sending actual data, only its hash is provided, and the receiving peer checks the hash against the Merkle tree's root. Merkle trees, also known as hash trees or binary trees of hash pointers, are used to ensure that all peers and nodes share the same, authentic, undamaged data and that any changes to that data must be communicated to all other nodes.

Blockchain working Process: Transaction definition, transaction authentication, block creation, block validation, and block chaining are the five phases that make up the blockchain workflow. The transaction model that the blockchain network has already developed is known as a transaction definition. The recipient's public key is cryptographically signed with the sender's passphrase-protected digital key, together with the transaction payload and sender's digital signature. The procedure by which the nodes determine if the A is authorized to move the asset and has the necessary funds and assets is known as transaction authentication. Block creation is the process through which a node from the transaction pool creates a block where transactions are categorized according to when they were created. Block confirmation is the process of verifying the block's validity by seeing if it contains the preceding hash and nonce that offers the evidence of the work. Adding a block to a chain is a technique called block chaining once the nodes have reached a consensus in the blockchain.

Figure 5.1

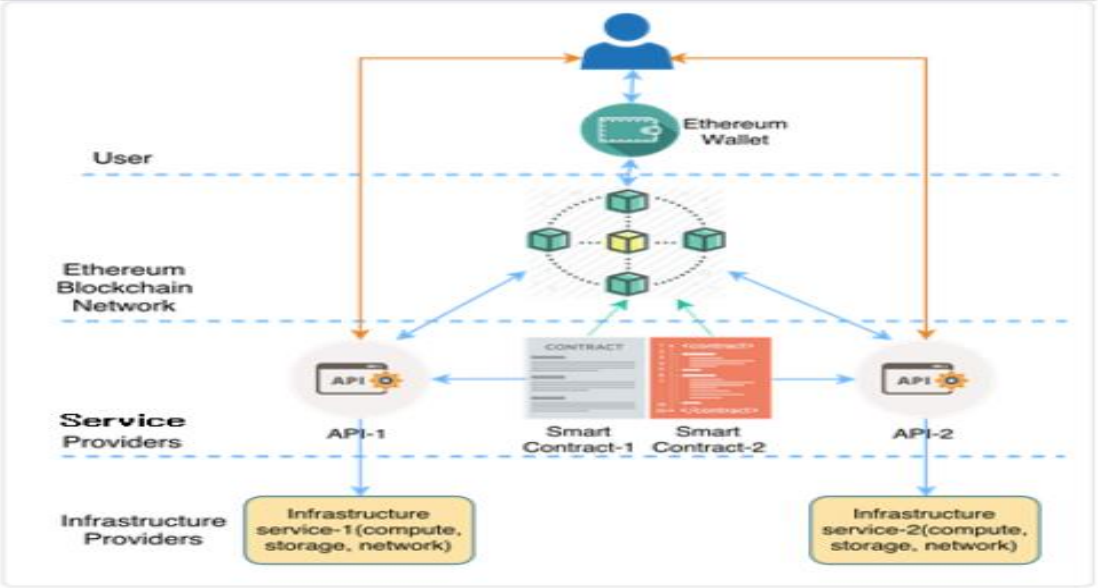
Working of Blockchain Architecture



Software Implementation of Blockchain

Figure 5.2

A Blockchain Architecture Implementation

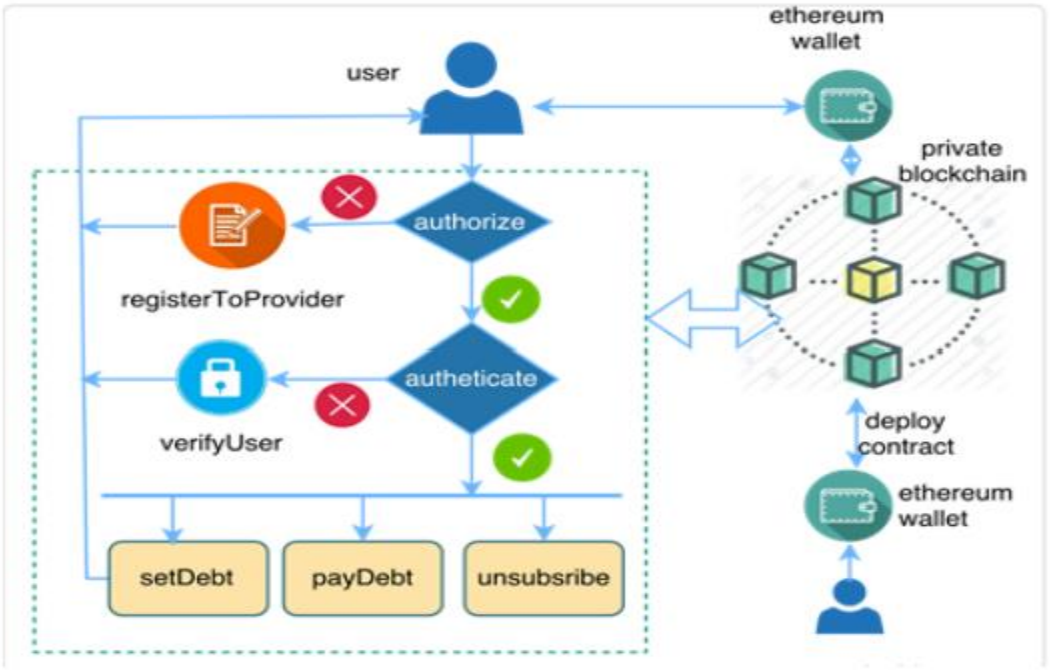


The comprehensive answer on how the service providers could use Ethereum blockchain technology for a shared identification backend is shown in the software architecture given in the next Figure. The solution also demonstrates how users can pay their bills and own data using blockchain technology without disclosing their personal financial information. The most important components were the implementation of smart contracts on the blockchain network and the detailed explanation of the relationship between providers, the blockchain, smart contracts, and users. As indicated in Figure 5.2, there are four different types of participants in the software architecture: users, infrastructure providers, service providers, and the Ethereum Blockchain network.

Infrastructure service providers give service providers access to infrastructure services like computation, storage, and networks.

Figure 5.3

System overall workflow



The flow diagram Figure 5.3 shows how a user interacts with a smart contract for a service provider that has been installed on the blockchain network. We presume that services resources are used for simplicity's sake. The user who can conduct transactions using the smart contract in the blockchain network and the smart contracts implemented by the services provider are the main elements in the diagram.

Results and Discussions

The hardware and software elements needed to implement the prototype are described in this section. The setup of the prototype environment, the smart contracts,

and the execution of the prototype are also covered. The key concept is that you might set up the development environment and run the prototype after reading this part.

Hardware Components The prototype was developed, and the tested computer has 2,4 GHz Intel Core 2 Duo processor, 8 GB memory and operating system Windows OS Sierra version. Software Components This section describes the software components used for prototype development and testing. The components are entity platform, API gateway and E-pass platform

Conclusion

Three primary parts make up the architecture of the suggested solution: an Ethereum wallet, smart contracts, and an Ethereum blockchain. By generating a private-public key, the Ethereum wallet is in charge of authenticating the user against the Ethereum blockchain. The private key is kept confidential with the user and is password-protected while the public key is dispersed throughout the blockchain network. With the help of the user's public key, the network can confirm and validate the user's identity using this key pair. The primary logic of smart contracts consists of user permission, while the supporting logic includes authentication, accounting, and de-registration of users. The cloud service providers that create and implement it on the blockchain are in control of the contracts.

References

Abhishek, K., Roshan, S., Kumar, P., & Ranjan, R. (2013). A Comprehensive Study on Multifactor Authentication Schemes. *Advances in Computing and Information Technology, 568.*

Adams-Prassl, A., Boneva, T., Golin, M., & Rauh, C. (2021). Work that can be done from home: Evidence on variation within and across occupations and industries. *Science Direct.*

Alabdullah, B., Beloff, N., & White, M. (2021). E-ART: A New Encryption Algorithm Based on the Reflection of Binary Search Tree. *Cryptography.*

AL-Mohannadi, H., Awan, I., Hamar, J. A., Hamar, Y. A., Shah, M., & Musa, A. (2018). Understanding awareness of cyber security threat among IT employees. *2018 6th International Conference on Future Internet of Things and Cloud Workshops.*

Aydar, M., Cetin, S. C., Ayvaz, S., & Aygun, B. (2020). Private Key encryption and recovery in blockchain. *arXiv.*

Bruun, A., Jensen, K., & Kristensen, D. (2014). Usability of Single and Multi Factor Authentication on Tabletops: A Comparative Study. *International Conference on Human Centred Software Engineering, 306.*

Bushwick, S. (2019). New Encryption System Protects Data from Quantum Computers,. *Scientific American.*

Buyya, R., Broberg, J., & Goscinski, A. (2011). Cloud Computing - Principles and Paradigms. *John Wiley & Sons.*

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 81.*

Dai, M., Zhang, S., Wang, H., & Jin, S. (2018). A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain. *IEEE Access.*

Dasgupta, D., Roy, A., & Nag, A. (2016). Toward the design of adaptive selection strategies for multi-factor authentication. *Computers & Security, 116.*

Debrosse, J. (2019). Cybersecurity Review. Cybersecurity Review White Paper.

Demairkan, S., Demirkan, I., & Mckee, A. (2020). Blockchain technology in the future of business cyber security. *Journal of Management Analytics.*

Elprocus. (n.d.). What is an Encryption Process : Definition, Types and Uses. https://www.elprocus.com/what-is-an-encryption-process-definition-types-and-uses/

Fahim, S. R., Shahriar, S., Islam, O. K., Rahman, M. I., Sarker, S. K., & Akter, S. (2020). Development of a remote tracking security box with multi-factor authentication system incorporates with a biometric sensing device. *2019 IEEE International WIE Conference on Electrical and Computer Engineering.*

Friebel, G., Heinz, M., Krueger, M., & Zubanov, N. (2017). Team Incentives and Performance: Evidence from a Retail chain. *American Economic Review.*

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Security Journal, 35.*

Hacker, J. V., Johnson, M., Saunders, C., & Thayer, A. L. (2019). Trust in Virtual Teams: A Multidisciplinary Review and Integration. *Australasian Journal of Information Systems, 23.*

Haque, A. B., & Rahman, M. (2020). Blockchain technology: Methodology, application and security issues. *International Journal of Computer Science and Network Security, 20(2).*

Zand, M & Gupta, R (2021, 02 01). How two factor authentication works with blockchain. *Retrieved from Security*: https://www.securitymagazine.com/articles/94479-how-two-factor-authentication-works-with-blockchain

Jarrahi, M. H., & Sawyer, S. (2013). Social Technologies, Informal Knowledge Practices, and the Enterprise. *Journal of Organizational Computing and Electronic Commerce, 137.*

Kaushik, A., Choudhary, A., Ektare, C., Thomas, D., & Akram, S. (2017). Blockchain - Literature Survey. *2017 2nd IEEE International Conference on Recent trends in Electronics, Information & Communication Technology.*

Kebande, V. R., Awaysheh, F. M., Ikuesan, R. A., Alawadi, S. A., & Alshehri, M. D. (2021). A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles. *MDPI.*

Kwon, B. W., Sharma, P. K., & Park, J. H. (2019). CCTV Based Multi Factor Authentication System. *Journal of Information Processing Systems, 919.*

Madhuravani, B., Reddy, P. B., & Reddy, P. L. (2013). A Comprehensive Study on Different Authentication Factors. *International Journal of Engineering Research & Technology.*

Mann, A., & Adkins, A. (2017, 03 22). Gallup. *Retrieved from Engaged Remote workforce:* http://www.gallup.com/businessjournal/206180/engaged-remote-workforce.aspx

Maurer, R. (2020, 03 26). How to Maintain Cybersecurity for your Remote Workers. *Retrieved from SHRM:* https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/how-to-maintain-cybersecurity-for-your-remote-workers.aspx

Michaelides, N. (2021). Remote Working and Cyber Security Literature Review. *Retrieved from ResearchGate:* https://www.researchgate.net/publication/349396561_Remote_Working_and_Cyber_Security_Literature_Review

Morkunas, V., Paschen, J., & Boon, E. (2019). How block chain technologies impact your business model. *Business Horizons.*

Moussa, M. (2015). Monitoring employee behavior through the use of technology and issues of employee privacy in America. *SAGE Open.*

Multi factor Authentication. (n.d.). *Retrieved from HP:* https://www.hp.com/in-en/shop/buying-guide-multi-factor-authentication

Szabo, N. (1994). Smart Contracts.

Szabo, N. (1997). The idea of smart contracts.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Nath, A., & Mondal, T. (2016). Issues and Challenges in Two Factor Authentication Algorithms. *International Journal of Latest trends in Engineering and Technology, 327.*

Ometov, A., Bezzateev, S., Makitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi Factor Authentication: A Survey. *cryptography.*

Pal, O., Alam, B., Thakur, V., & Singh, S. (2021). Key Management for Block chain technology. *ICT Express, 80.*

Pise, R., & Patil, S. (2021). Enhancing Security of Data in Cloud Storage using Decentralized Blockchain . *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks.*

Protocol. (n.d.). *Retrieved from remote work boss tracking tools:* https://www.protocol.com/remote-work-boss-tracking-tools

Radanovic, I., & Likic, R. (2018). Opportunities for Use of Blockchain Technology in Medicine. *Applied Health Economics and Health Policy, 590.*

Radwan, A. G., AbdElHaleem, S. H., & Abd-El-Hafiz, S. K. (2016). Symmetric encryption algorithms using chaotic and non-chaotic generators: A review. *Journal of Advanced Research, 208.*

Research, G. (2018, January 16). Gartner Research. *Retrieved from Gartner:* https://www.gartner.com/en/documents/3845967

Raghav, C. S. (n.d.). Cyber security in india's counter terrorism strategy.

Rawindaran, N., jayal, A., Prakash, E., & Hewage, C. (n.d.). Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). *Future Internet.*

Renuka, P., & Booba, B. (2021). A Correlation Blockchain Matrix Factorization to Enhance the Disease Prediction Accuracy and Security in IoT Medical Data. *Cyber Security and Digital Forensics, 369.*

Sahu, M. K., & Ansari, M. S. (2017). A Survey on Encryption Techniques. *International Journal of science and Research, 1189.*

Sajal, S. Z., Jahan, I., & Nygard, K. E. (2019). A Survey on Cyber Security Threats and Challenges in Modern Society. *2019 IEEE International Conference on Electro Information Technology (EIT).*

Savel*yev, A. (2018). Copyright in the blockchain era: Promises and challenges. Computer Law & Security Review, 561.*

Saxena, s., Gupta, U. K., & Dwivedi, R. &. (2021). Security Issues and Application of Blockchain. Machine Learning, Advances in Computing, *Renewable Energy and Communication, 541.*

Sifah, E. B., Xia, H., Cobblah, C. N., Xia, Q., Gao, J., & Du, X. (2020). BEMPAS: a decentralized employee performance assessment system based on blockchain for smart city governance. *IEEE Access.*

Sun, P. J. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. *IEEE Access, 147452.*

Hassan, G., Elagazzar, K., (2016). The case of face recognition on Mobile Devices. *2016 IEEE Wireless Communications and Networking Conference.*

The Newyork Times. (2020, 05 06). *Retrieved from Employee monitoring work from home:* https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html

Velte, T., Velte, A., & Elsenpeter, R. C. (2010). Cloud Computing, A Practical Approach. *McGraw-Hill Companies.*

Venkatesh, V., Thong, j. Y., Chan, F. K., Hoehle, H., & Spohrer, K. (2020). How agile software development methods reduce work exhaustion: Insights on role perceptions and organizational skills . *Information Systems Journal.*

Norton (n.d.). What is Encryption and how does it protect your data. *Retrieved from Norton:* https://us.norton.com/internetsecurity-privacy-what-is-encryption.html#:~:text=Encryption%20is%20the%20process%20of,a%20network%20like%20the%20internet.

Wu, B., & Duan, T. (2019). The Advantages of Blockchain Technology in Commercial Bank Operation and Management. ICMLT 2019: *Proceedings of the 2019 4th International Conference on Machine Learning Technologies, 87.*

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A Survey of Blockchain technology applied to smart cities: *Research issues and challenges. IEEE Communications Surveys & Tutorials.*

Yang, L. (2019). The Blockchain: State-of-the-Art and Research Challenges. *Journal of Industrial Information Integration, 90.*

Yew, K. H., Kalid, K. S., & Tachmammedov, S. (2018). Multi-factor attendance authentication system. *International Journal of Computer Systems & Software Engineering, 79.*

Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019). Research on the Application of Cryptography on the Blockchain. *Journal of Physics: Conference Series.*

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: A Survey. *IEEE Access, 16455.*