Addressing user perception and implementing Hedera Hashgraph and voice recognition into Multi-Factor Authentication (MFA) system

Wong Jie Sheng[1], Dr. Intan Farahana Binti Kamsin[2], Salmiah Binti Amin[3], Nur Khairunnisha Binti Zainal[4]
[1, 2, 3, 4]Asia Pacific University of Technology & Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.
[1]wongjiesheng88@gmail.com, [2]intan.farahana@staffemail.apu.edu.my, [3]salmiah@staffemail.apu.edu.my,
[4]khairunnisha.zainal@staffemail.apu.edu.my

***Abstract* - Multi-Factor Authentication (MFA) has been gaining popularity in recent years for offering extra layers of protection to secure user accounts. Most of the integration of MFA today includes a One-Time Password (OTP) to be sent through a Short Message Service (SMS) identified by a user's phone number or through an MFA application. However, MFA executions like these still possess underlying vulnerabilities like phishing attacks. The aim of this research is to propose an effective Software Engineering solution to decrease the number of successful attacks on user accounts during the MFA process. The proposed system suggests a first-level authentication in the form of textbox for users to input their current location of access. This can prompt the user naturally to always pay attention to the user information provided before they continue on with the MFA process. This can help users to identify a threat and realise an attempted phishing attack before giving the full access to the attackers if proceeded with the MFA process. This paper proposes a solution that takes in voice recognition biometric alongside the traditional OTP. An improved distributed ledger technology in the form of Hedera Hashgraph is also proposed which addresses efficiency and security shortcomings of Blockchains like the Ethereum Blockchain. For this research, self-selection sampling was carried out and 5 people were chosen to attend a one-to-one online interview session. Then, a total of 50 responds by 50 people were collected through an online survey using systematic sampling to ensure the consistency of opinion of audience of a larger scale. Future research could focus on exploring a fully software-based voice recognition biometric system on MFA systems. Attacks other than phishing on MFA is also an area to be studied on to provide more security to MFA.**

Index Terms* - *Hashgraph, Multi-factor authentication, One-time password, voice recognition biometric.

1. Introduction

Multi-Factor Authentication (MFA) is a process of authentication that involves more than one authentication method in the means of security. It is used to verify user identities on top of the user credentials input by the user like a username and password in the traditional method. As long as the authentication includes a minimum of two techniques, it can be classified as MFA. The four common authentication factors are based on: What the user knows, has, is and where the user is [7]. Unfortunately, the MFA systems that are used often today are not really safe. Vulnerabilities are present and with the skills of attackers nowadays, any user might fall prey to the ill-intended hackers. According to Jensen et al. [14], the research of the team on ten MFA applications shows a worrying condition where some applications that are reputable and recommended by experts are at risk of a variety of exploits. According to Ometov et al. [21], MFA is vulnerable to a number of risks that includes data spoofing, data theft, capture of data sample and position lock. Packet pausing attacks and malicious endpoint attacks also post a risk to MFA. Phishing, a very simple form of attack is still prevalent and possible in MFA [10].

2. Research Background / Literature Review

2.1 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is the implementation of extra security in the form of adding two or more security methods supplementing the traditional login method of using only username and password [29]. MFA had existed since approximately 30 years ago. The innovative idea of MFA was patented by AT&T in the year of 1996. However, the idea has not been implemented into use in regards with the consumer security point of view until recent years. This is due to the companies' slow action to utilize this idea and put into real use [12]. Today, a single-factor authentication might not be a username and password login. With technology advancements in this day and age, a single-factor authentication can be in the form of biometrics as well. Ultimately, it has to come down to one of the three mechanisms for authentication that is: something the user knows, something the user has or something the user is. In terms of MFA, it requires more than just one of the authentication mechanisms mentioned. It can be in a form of all three mechanisms combined. For example, "something the user has" can be a physical card, "something the user knows" can be a traditional password, "something the user is" can be his/her fingerprint which cannot be altered and is completely unique to the user [27].

Based on Mello et al. [24] research, the authors proposed a solution to strengthen the single-factor authentication which in the context of the paper, propose a FIDO2 and Phone Prompt solution on top of the regular password-based authentication for the Brazillian academic federation. The password policy here is also improved to be a time-based one-time password that is vulnerable to time instead of the user defined password that stays constant. FIDO2 is an authentication method based on public key cryptography that is user friendly and preserves user

privacy. Based on Pankhuri et al. [22] proposal, the researchers suggested a pattern-based MFA system which utilises a combination of text and images. The research proposes that users are required to click on an area of the shown particular image selected during the registration process within a predefined space within it. To counter shoulder surfing in this type of graphical password setting, a key must also be inputted by the user to authenticate through the login attempt. Important attributes that the system fetches are the key, the image pixels of the clicks and the image sequence number. The proposed solutions to improve the MFA process above have different approaches to the problem. Specific types of attack have been targeted to be addressed like shoulder surfing, brute force attack and dictionary attack. An improved system would be a system that has both the front end (user end) and the back end (system's internal process) action to be addressed at multiple levels to defend against emerging attacks towards MFA. To fill in the gap of existing systems, this study takes into consideration that addresses phishing attack. That is to have the user more aware of a potential phishing attack that could have already taken ownership of the account using foreign servers from locations alien to the user. This happens primarily after the user have clicked on a suspicious website link and filled in their login credentials. The hackers could have already gained partial control over the user account and only needs the user to complete the MFA process to fully control the account.

2.2 User perception in MFA

According to Das et al. [6], user perception of MFA is faced with challenges. These include lack in motivation, unintuitive user interface and risk trade-off understanding. However, the organisation of user studies has been proved to have positive impact on improving the adoption of digital security. A mere 9.1% of studies collected on MFA have had conducted user evaluation that could help see MFA from the user's point of view. Furthermore, the study found out that aside from the lack of user evaluation, existing shortcomings also include things like lack of population diversity and the lack of expertise knowledge on the statistics collected.

Consistent with Ometov et al. [21], 68% of Europeans are willing to use biometric for payments which makes sense since biometric is a very common form of implementation of security in today's day and age. However, a single form of biometric is still considered a form of single-factor authentication. The only difference with the traditional single-factor authentication is that it goes with the "something the user is" approach instead of the password-based system where it is concerned with the "something the user knows" approach. This makes the authentication method harder to eavesdrop. A very obvious trade-off of MFA is the one between convenience and security where one side might be neglected while trying to improve the other side. An investigation also concluded that the young generation which is generally more tech savvy are able to pass authentication procedure in half the amount of time by the general audience. Another study shows that gender does not affect the efficiency of passing authentication. One study suggests pleasure as being the best way for technology adoption in a short time.

A big number of researchers go by the idea of utilising personal handheld devices like a smartphone in MFA. A solution model proposed by Michelin et al. [16] suggests the usage of the camera in the user-identified device to execute facial and iris recognition technology in MFA. The results of the scanning are then stored in the cloud for the user credential checking. Another vital problem in MFA implementation is the generalisation nature of the approaches implemented. For instance, people who have no limbs would not be able to use the fingerprint scanning authentication method. Today, most of the MFA implementations are on the hardware level [21]. Normally, anything hardware-based have a risk of it not working due to some hardware failures. Therefore, the approach that should be taken to improve MFA is making it software based. This is to improve the reliability and credibility of the authentication. It is important to give the users assurance how the MFA software stores their authentication information to ensure transparency and dispose any privacy concerns which is a topic much focused on today. In terms of MFA fatigue, there is very limited research done on it. Therefore, to approach the issue, the study takes into consideration aspects in User Interface (UI) and Human-Computer Interaction (HCI) to propose how to let the user to at least be aware to some degree if the person trying to access the account through MFA is him/herself. An attacker can use phishing attack to gain control over the targeted account once the user had inputted his/her login credentials. Although the attacker still cannot gain access to the account since there is the presence of MFA, the legitimate user's successful attempts of all the MFA mechanisms would result to the attacker gaining access after.

2.3 Voice recognition biometric

In recent years, voice recognition biometric authentication has increased popularity tremendously due to its many benefits like portability, privacy and stability. This type of authentication technology is a good option that provides high authentication accuracy while also being user-friendly and non-intrusive. Due to its portability, no other specialised proprietary tools are required to be used by a user. A smartphone is sufficient to be able to utilise voice recognition biometric since the technology can be implemented and embedded in a software used by users itself [9]. To further strengthen the importance of voice recognition biometric, many world-renowned technology companies have already started to adopt the technology into their hardware and software. Google, for example, has a service based on Android known as "Trusted Voice" that allows users to unlock their smartphones. Transactions can also be done using voice recognition biometric. An example of this is Saypay Technology's mPayment where the users utilise password in the form of voice to enable transactions. UK-based international bank HSBC Bank also mentioned they would offer biometric options for their users to access their accounts in the form of fingerprint or voice [23].

Abozaid et al. [1] mentioned that using voice recognition as a biometric authentication method has several advantages. It can be seen as an intuitive and natural method since it uses the voice from an individual. The human voice gives the flexibility of which a remote authentication is possible and thus also requiring a low cost. The paper suggests two modes or operation that are training mode and recognition mode. Features excerption process is used in training mode to change voice signals into features vector. Speaker Modelling is also used for training mode by carrying out Artificial Neural Network (ANN), Support Vector Machine (SVM) and Gaussian Mixture Model (GMM). The speaker identification approach used collects speaker information through Speaker Modelling and stores them in the Speaker Model Database in training mode. Then, in the recognition mode, the goal is to match the voice from the database and come out with the decision whether to authorise and give way to the user.

In the research by Li et al. [15], an mmWave interrogation system known as VocalPrint is suggested to counter the vulnerabilities of existing voice recognition biometrics. Those vulnerabilities include replay attacks and ambient noise. VocalPrint is a low-cost, portable and energy-efficient hardware solution that works by analysing the vibration of the voice from the user for authentication purpose. It makes use of the skin-reflect radio frequency (RF) signals that is caused by the vibrations through the voice of users. The signals can be found approximately at the near-throat region of an individual. Then, by utilising resilience-aware clutter suppression that aims to preserve fine-grained vocal biometric properties, the users' ambient noise is segregated from the RF signal. An ensemble classifier acts as the technology to receive useful input such as text-independent vocal tract and vocal source features to then used for authentication. VocalPrint, although being a hardware, has the capability to allow for the transition to be used on a smartphone easily. The system records a whopping 96% accuracy from experiment that includes unfavourable conditions. The study concludes that VocalPrint is resilient against ambience and spoofing. Through the analysis, VocalPrint has the potential to be revolutionary since the approaches and technologies used are novel and emerging. A robust and improved system can aid further in achieving accurate authentication even from the audience coming from the disabled community with serious speech disorders. In order to strengthen the proposed system in this research, a voice recognition biometric system similar to VocalPrint can be introduced into the MFA system. The improvements that can be made upon the technology include improved long-distance sensing and sensing orientation. The improved voice recognition biometric technology would use text-independent recognition that provides the practicality.

2.4 Hedera Hashgraph

Hedera Hashgraph is a type of distributed ledger technology (also known as decentralised network) in the form of asynchronous byzantine fault tolerance (ABFT) atomic broadcast protocol. All decentralised networks like the popular Blockchain technology have nodes that are independent that needs to come to consensus in various aspects like the transactions to the network, the transaction orders and the state in which the network is in itself [11]. Atomic broadcast protocol is essentially the protocol that allows those nodes to reach consensus [4]. The nodes are separated in many ways in terms of geographics, virtually, ethically and so on. Based on "Byzantine General's Problem", some nodes have the potential of "betrayal" or in the nodes' context, malicious. Hackers can take over some nodes to send incorrect information purposefully. To simplify it, BFT provides the ability to have a guarantee of consensus through the use of mathematics. This means that BFT allows the nodes to come to agreement on the timing and order of transactions without having to trust other nodes. ABFT, on the other hand, further enhances BFT in a way that overcomes the challenge of timing. This is due to the fact that many BFT just suppose that a maximum threshold of message latency is present when it comes to a consensus. An ABFT network disposes this assumption and proceed to permit some messages to be lost or indefinitely delayed. It does this by only expecting messages from honest nodes to eventually pass through at some point [11].

The Blockchain technology is the traditional and an ever-popular form of distributed ledger technology first published in a white paper describing it in the year of 2008 [19]. Blockchain is being used widely nowadays but has not evolved much since its introduction. Blockchain is powerful due to the consensus system where it is pioneer at it as well as the way in which it creates immutability of data [25]. However, Blockchain is considered slow in this day and age with only 3 to 4 transactions per second [5]. One prominent strength of Blockchain is the sequentiality that it provides. A block builds upon another once approval has been confirmed by the majority of Blockchain. Then, once the next block is built upon the previous, the previous block can no longer be altered. The advantage it provides is the absence of ramifications. On the downside, it is the sequentiality that slows down the process of block building tremendously [25].

HoneyBadgerBFT, which claims to be the first practical ABFT protocol, have paved the way to be a promising transaction processing system. The protocol is able to achieve asymptotic efficiency that's optimal that can handle throughputs of tens of thousands of transactions per second and grows to over a hundred nodes on a wide area network, according to the research's implementation and test findings [17]. BEAT, a set of ABFT protocols is another project proposed by another team of researchers later in 2018. BEAT is unique in a sense where it consists of not just one, but five ABFT protocols that are flexible and versatile. The goals of the set of protocols include addressing transactions at different performance metrics as well as application scenarios. The modularity of BEAT allows for the combination of the protocols to work even better in terms of functionality and performance. Notably, BEAT surpass the previously discussed HoneyBadgerBFT which was the most efficient ABFT at the point of writing of the paper. BEAT is

able to outclass HoneyBadgerBFT in regards of latency and throughput in the experiment performed on Amazon EC2 [8].

Hashgraph, despite also being a distributed ledger technology just like Blockchain and others, it works fundamentally from Blockchain and is essentially Blockchains without the blocks and the chain. The aspects of information dissemination and consensus reaching are different. Hashgraph does not need all network nodes to at all times, be in sync with all information. The nodes in Hashgraph are required to share all information with other nodes selected on random. The node receiving the information will combine the information with the information received from other nodes then finally adding information about the new transactions. This process will only stop when all nodes have knowledge of the information that was created at the very beginning. The information alongside the timestamps were to be passed on together with all the information about the previous receivers. By this ingenious implementation, all nodes are able to know each other's decision based on the information passed on without needing to vote. Because of this, Hashgraph is very efficient. The improvement is dramatic to the point where it can handle not limited to 250,000 transactions per second [25]. Compared to HoneyBadgerBFT and BEAT, Hashgraph differs in which it does not use communication to vote but only for broadcasting transactions. Through the tests performed in comparison with both HoneyBadgerBFT and BEAT, Hashgraph manage to outplay both of the previous technologies in departments of latency and throughput by a mile. An experiment was also run to test Hashgraph's handling of high-performance settings. The experiment concluded that Hashgraph is able to provide ample performance in supporting demanding applications. In the meantime, it still assures security in ABFT environment [4]. To further strengthen the legitimacy of Hedera's Hashgraph technology, the company is owned and governed by world renowned companies like Google, IBM, Boeing and more [11]. Through the study of past technologies, Hashgraph is the contemporary distributed ledger technology that provides improved efficiency and security which can be implemented into an MFA system.

2.5 Similar System

2.5.1 Hydro Raindrop MFA

The Hydro Raindrop MFA plugin has an additional layer of security while utilising Ethereum Blockchain-based authentication layer. Hydro Raindrop MFA can be integrated with websites or apps after logging in for an extra factor of authentication. The websites or apps that wishes to use Hydro MFA have to possess HTTPS (a more secure form of HTTP using SSL) connection and PHP 7.0 or higher. On the users' side, the Hydro app can be downloaded from various app stores. It is a free downloadable app that is both available on Android as well as IOS platforms. Then, the user can use the app while logging into websites or apps that have Hydro MFA added as an MFA solution optionally for users. Users first login normally by their username and password for a particular website or app. Then, on the website or app itself, the user will be prompted to input their Hydro ID which was generated using their Hydro app on their mobile device. After submitting the ID, a 6-digit OTP code (token) will be displayed on the website or app [3].

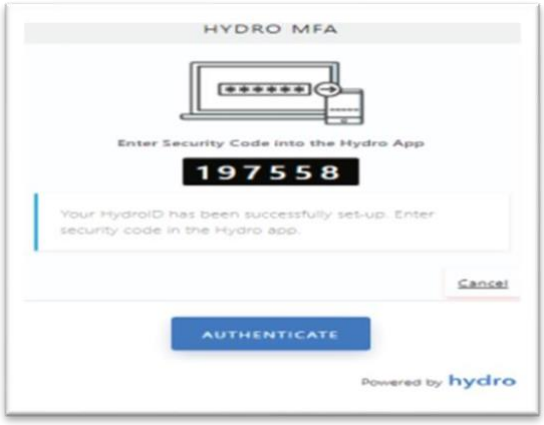

Figure 1.0 - Token generated
Source: https://doi.org/10.14488/bjopm.2019.v16.n2.a9

Users are then required to input the 6-digit code into their Hydro mobile app. The token will then be validated within the app with Hydro Blockchain. After the initial configuration, in any other attempts to login to their account in the future, the users are required to enter in a randomly generated 6-digit OTP code on top of their login credentials. Only the correct code entered will be able to authenticate into the account [3].

2.5.2 MFA through smart contracts in Ethereum Blockchain

The proposed framework is aimed in providing Two Factor Authentication (2FA) which is a type of MFA. In the example given, a user is defined as an employee within a company who wants to have access to the server's resources. A staff is an administrator level employee of that company which gives access rights to other employees. The users, staff and servers all hold a public-private key pair. Each key pair has a unique Ethereum Address assigned to it. Firstly, all servers and users are registered in the smart contract according to their Ethereum Address by the staff. Then, each user can request for access to servers that are contained in the smart contract. The staff then accepts or rejects the request based on necessity. A 6-digit OTP in numeric form can be generated from the user's side after he/she was allowed access. The OTP generated is hashed using SHA3 algorithm that will be stored in the Blockchain. After these processes, when a user attempts to access to a particular server using SSH and enters his/her assigned OTP, the server's Pluggable Authentication Modules (PAM) module will search the Blockchain for all hashed tokens matching to itself and try to find the hash of the entered OTP. If it is discovered, the user will be granted access; otherwise, the connection will be terminated. In this way, Blockchain is utilised as a distributed computing and storage platform to perform numerous 2FA-related functions. The framework was tested using Genache. The smart contracts are programmed with functions that can be accessed via DApp. A decentralised application (DApp) is a

service that allows users to engage with smart contracts in a user-friendly way. The DApp was developed using HTML and Javascript using libraries to result in a user-friendly interface. The Metamask browser plugin was used to interact with the Ethereum node and allowing DApp to have communication with the nodes. It also gives users the ability to load and unload their Ethereum keys into DApp. This plugin may be set up to digitally sign all Web3 transactions and transmit them to a single gateway, where they are all added to a pool and processed by miners [2].

Figure 2.0 - OTP generated at user's side
Source: https://doi.org/10.14488/bjopm.2019.v16.n2.a9

Table 1.0 - Comparison table of the two similar systems.

Similar system / Component	Hydro Raindrop MFA	MFA through smart contracts in Ethereum Blockchain
Levels of authentication	2	2
Ledger technology	Distributed	Distributed
Distributed ledger technology	Ethereum Blockchain	Ethereum Blockchain
Smart contract	✓	✓
User location confirmation	×	×
OTP	✓	✓
Voice recognition biometric	×	×
SHA3 hashing	×	✓
Audience	Anyone	Within organisation

The comparison table shows that both systems above only provide one more level of authentication on top of the user credentials like username and password. The 2FA approach in MFA can definitely be improved to come up with a system with a more secured mechanism with more levels of authentication. Both systems above utilised distributed ledger technology in the form of Ethereum Blockchain with smart contracts which is a public open source Blockchain platform launched in the year of 2015 [3]. However, both systems do not have the functionality of providing user location for user confirmation and absent of voice recognition biometric. The authentication offered by both systems discussed are in the form of 6-digit OTP code. Furthermore, MFA through smart contracts in Ethereum Blockchain has SHA3 hashing functionality that hashes the OTP code received when storing it in the Blockchain to be used for internal comparing for authentication purpose [3]. In terms of audience groups, Hydro Raindrop MFA can be used for anyone with access to a particular website or app that utilises the technology. On the other hand, MFA through smart contracts in Ethereum Blockchain has been recommended for use within an organisation which focuses on protecting an organisation's confidential data accessibility.

To conclude, both the systems discussed above are lacking in terms of protecting users from phishing attacks. Aside from that, an MFA system should add more complexity and levels of authentication. Hackers today are getting more and more skilful and difficult to deal with. Therefore, the least an MFA system can do is to increase its level of security to decrease the risk of exploitation on user accounts. Thus, this research will propose the necessary additional features to fill in the gap and overcome the weaknesses on the discussed systems to come out with a more secured MFA solution.

3. Problem Statement

Based on a survey conducted in 2017, 30% of enterprises have plans on the deployment of Multi-Factor Authentication (MFA) while 51% have already implemented it within their enterprises. Furthermore, another 38% stated that there are implementations of MFA already in "some areas" of operation in their respective enterprises [28]. It can be widely agreed upon that MFA provides extra protection compared to the traditional Single-Factor Authentication (SFA). However, there are caveats surrounding MFA addressing that MFA is not a perfect security mechanism. The modern MFA today still has its underlying threats discussed earlier. This means that current technologies used in MFA is not secure enough. Another problem regarding this is circulated at a term known as MFA fatigue that results in many phishing attacks. This occurs when the users have gotten so used to the same process of MFA that they no longer pay attention to the outcome of their actions if they were to authenticate into their accounts while under a form of security risk. By logging in without being meticulous, they are not able to identify the legitimacy of the login attempts [13]. As a result of this, their accounts might be exploited by attackers with bad intentions and can be sold to the dark web.

4. Aim and Objectives

4.1 Aim

The aim of this research is to propose an effective Software Engineering solution to decrease the number of successful phishing attacks on user accounts during the MFA process.

4.2 Objectives

- To design a system that displays the exact location, IP address and other useful information of a login attempt in proper font design and size as well as other Human Computer Interaction (HCI) principles that captures users' attention.
- To implement a text field in the User Interface (UI) for the users to input the access location for confirmation and legitimacy of login attempt.
- To enable voice recognition by the implementation of the call function within the authentication system.
- To enable distributed ledger technology in the form of Hedera Hashgraph to improve the security and efficiency of MFA.

5. Research Significance

The findings of this research can help in the implementation of a more secure MFA mechanism. MFA used today are mostly in the form of 2FA and are susceptible to various vulnerabilities. The proposed system framework takes into consideration security measures starting from the very beginning of MFA – what the user can do at the frontend. Multiple MFA methods are added into the system and the backend distributed ledger technology used is of an improved version of the traditional Blockchain technology. The research on this paper can also serve as a catalyst in future research and development works in MFA.

6. Methodology

The research uses qualitative research in the form of online interview through self-selection sampling which is a type of non-probability purposive sampling. The use of it is to get an idea on what are the respondents' perception towards the research before stepping into quantitative research. Self-selection sampling can reduce the time required to find for respondents and respondents are likely to be more committed since it is based on their willingness to join the interview at the first place [26]. For this research, the research idea is publicised through various social media platforms like WhatsApp and Instagram to look for voluntary respondents. The target number of respondents for the online interview session is 5. The form of online interview the research takes is one-to-one online interviews through Microsoft Teams. The structure of interview is semi-structured to ensure that core and important questions are answered alongside the possibility of the respondents giving more information during the interview as some other areas within the research scope could be touched upon.

Aside from qualitative research, quantitative research in the form of online survey through systematic sampling is also used. Systematic sampling is a type of probability sampling which is classified as complex probability sampling. Firstly, a list of respondents that is unknown to the researcher is listed and chosen at random by fixed intervals of a total of 100 respondents. The survey questionnaire has gone through expert validation by the research supervisor, pre-test that involved 3 respondents answering the questionnaire, pilot testing (with amended questions based on pre-test feedback) that involved 20 respondents. Then, emails are sent to the potential respondents with an online survey Microsoft Forms link with the final questionnaire using multiple choice questions and Likert scale as the answering format. Likert scale is the most often used form of tool for evaluating affective variables like motivation and self-efficacy [20]. Therefore, Likert scale is useful to ask opinion-based quantitative questions like to what degree the respondent agree to or disagree of something. This online survey serves as a mean to ensure that the larger audience's perspectives align with the ideas given by a smaller audience from the online interview. This is because non-probability sampling is typically carried out before probability sampling since it involves a smaller sample size. Email reminders are sent to follow up with the potential respondents near to the deadline. The online survey looks forward to at least 50 responds of fully answered online survey form. Quantitative research is adopted to have an overall view on user perception of a larger population. Systematic sampling is suitable for this particular research because the research is not based on any particular audience. However, it is based on addressing the issues that users commonly share to propose a viable solution. When explicit or implicit stratification is included in the sample frame, systematic sampling can offer more precise estimators than other quantitative sampling methods like simple random sampling [18]. Thus, to ensure there is no bias and inaccurate results, respondents are chosen at intervals.

7. Overview of the Proposed System

The proposed system covers authentication methods across various spectrums. This paper proposes a solution that includes a suite of authentication methods and technologies to increase the security of MFA. A user will be directed to the MFA system once his/her user credentials have been authenticated on the service website or application that uses the MFA system. The solution suggested is in the form of an MFA system or application in which it starts out with displaying of information useful for users like the location of their login attempt, IP address, time with the correct time zone and device model to the user and confirmation of location by the user as the first layer of security that tackles phishing attacks. When the user is required to input in a textbox his/her location for confirmation, it will force the user to check out on the information displayed for them that might help them identify an attack attempt on their accounts at the very beginning. Once the user has got his/her location filled in and matches with what it is displayed and, in the database, a 6-digit OTP will be provided as the second level of MFA. Then, a voice recognition biometric prompt using VocalPrint technology with better long-distance sensing and sensing orientation will be enabled if the OTP keyed in is indeed correct. The voice authentication is done through a call function within the application. The user is required to speak certain random words or sentences in English as requested by the system. After the user have been authenticated through it, he/she will be able to access his/her account. In the meantime, at the background of all these, a Hedera Hashgraph distributed

ledger technology is managing all the processes for increased efficiency and security. Without a single point of failure, it can provide the service with low-cost and high-performance. Hashgraph also does not require a lot of processing power or electricity. The perks of using Hashgraph overweighs the traditional Blockchain technology by a distance.

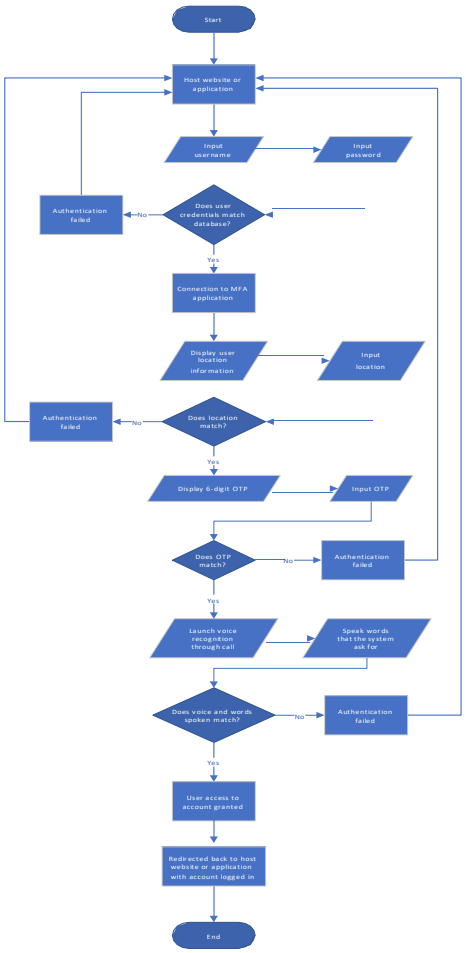

Figure 3.0 - Flowchart of the proposed system.

The figure above displays the flowchart that illustrates the flow of the proposed MFA system. Each failed authentication from the MFA process would send the user back to the host website or application. This is due to the security measure that is applied to prevent an interception from attackers when a user accidentally or intentionally tries to fail an authentication. This MFA framework uses an "AND" approach in which all authentication process has to be completed flawlessly to achieve the end goal of granting access through user identification to the user account.

8. Conclusion

All in all, phishing attacks in MFA are possible when users click on fraudulent links to the login page of a website or application. For the websites or applications that require MFA to be authenticated to gain access, the attacker can stay in the process of login until all the MFA process have been successfully authenticated. Then, once the MFA is authenticated, the attacker can have full access to the user account and can proceed to do whatever he/she wants like changing the account password and more. The proposed system attempts to curb this by implementing the first layer security on the user's side to "force" them to verify on their location of access. This addresses the MFA fatigue issue that is present in many users' perspective on MFA. Additional security measures using secure voice recognition biometric technology and an improved version of Blockchain under the hood are also enforced in the proposed system. The proposed system also functions as a mean that can help increase user awareness of phishing attacks in the MFA process. One limitation to the proposed system is that it primarily addresses phishing attack only. There are many other attacks that could be done by attackers that also requires a solution. Future research could dive deep into the investigations on other attacks on MFA. Last but not least, improvements could be done on the voice recognition biometric system where a fully software-based system can be introduced. Fully software-based voice recognition biometric can offer better reliability since it is less vulnerable to physical damage which can cause problems on the system. It is also cheaper and more easily used by companies that are interested since the configuration process could potentially be enhanced with more customisations.

References

[1] Abozaid, A., Haggag, A., Kasban, H., & Eltokhy, M. (2018). Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion. *Multimedia Tools and Applications*, *78*(12). https://doi.org/10.1007/s11042-018-7012-3

[2] Amrutiya, V., Jhamb, S., Priyadarshi, P., & Bhatia, A. (2019). Trustless two-factor authentication using smart contracts in blockchains. *2019 International Conference on Information Networking (ICOIN)*. https://doi.org/10.1109/icoin.2019.8718198

[3] Aparecido Cardoso, J. A., Ishizu, F. T., de Lima, J. T., & Pinto, J. D. S. (2019). Blockchain Based MFA Solution: the use of hydro raindrop MFA for information security on WordPress websites. *Brazilian Journal of Operations & Production Management*, *16*(2), 281–293. https://doi.org/10.14488/bjopm.2019.v16.n2.a9

[4] Baird, L., & Luykx, A. (2020). The Hashgraph protocol: Efficient asynchronous BFT for high-throughput distributed ledgers. *2020 International Conference on Omni-layer Intelligent Systems (COINS)*. https://doi.org/10.1109/coins49042.2020.9191430

[5] Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D., Wattenhofer, R. (2016). On scaling decentralized blockchains. *Paper presented at the International Conference on Financial*

Cryptography and Data Security. https://doi.org/10.1007/978-3-662-53357-4_8

[6] Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019). Evaluating User Perception of Multi-Factor Authentication: A Systematic Review. https://arxiv.org/abs/1908.05901

[7] Dasgupta, D., Roy, A., & Nag, A. (2017). Multi-Factor Authentication. *Infosys Science Foundation Series*, 185–233. https://doi.org/10.1007/978-3-319-58808-7_5

[8] Duan, S., Reiter, M. K., & Zhang, H. (2018). Beat. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3243734.3243812

[9] Duraibi, S., T. Sheldon, F., & Alhamdani, W. (2020). Voice Biometric Identity Authentication Model for IoT Devices. *International Journal of Security, Privacy and Trust Management*, *9*(2), 1–10. https://doi.org/10.5121/ijsptm.2020.9201

[10] Grimes, R. (2019). The many ways to hack 2FA. *Network Security*, *2019*(9), 8–13. https://doi.org/10.1016/s1353-4858(19)30107-2

[11] Hedera. (2018). *What is asynchronous byzantine fault tolerance (ABFT)?* https://hedera.com/learning/what-is-asynchronous-byzantine-fault-tolerance-abft

[12] Henricks, A, & Kettani, H. (2019). On Data Protection Using Multi-Factor Authentication. *Proceedings of the International Conference on Information System and System Management (ISSM)*, 1. https://doi.org/10.1145/3394788.3394789

[13] Hess, E., Tolbert, M., & Nascimento, M. (2021). *Vulnerabilities of Multi-factor Authentication in Modern Computer Networks.* : Worcester Polytechnic Institute.

[14] Jensen, K., Tazi, F., & Das, S. (2021). Multi-Factor Authentication Application Assessment: Risk Assessment of Expert-Recommended MFA Mobile Applications. https://ssrn.com/abstract=3878387

[15] Li, H., Xu, C., Rathore, A. S., Li, Z., Zhang, H., Song, C., Wang, K., Su, L., Lin, F., Ren, K., & Xu, W. (2021). VocalPrint: A mmWave-based Unmediated Vocal Sensing System for Secure Authentication. *IEEE Transactions on Mobile Computing*. https://doi.org/10.1109/tmc.2021.3084971

[16] Michelin, R. A., Zorzo, A. F., Campos, M. B., Neu, C. V., & Orozco, A. M. (2016). Smartphone as a biometric service for web authentication. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. https://doi.org/10.1109/icitst.2016.7856740

[17] Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The honey badger of BFT protocols. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/2976749.2978399

[18] Mostafa, S. A., & Ahmad, I. A. (2017). Recent developments in systematic sampling: A review. *Journal of Statistical Theory and Practice*, *12*(2), 290–310. https://doi.org/10.1080/15598608.2017.1353456

[19] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

[20] Nemoto, T., & Beglar, D. (2014). Developing Likert-scale questionnaires. In N. Sonda & A. Krause (Eds.), JALT2013 Conference Proceedings. Tokyo: JALT.

[21] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

[22] Pankhuri., Sinha, A., Shrivastava, G., & Kumar, P. (2019). A Pattern-Based Multi-Factor Authentication System. *Scalable Computing: Practice and Experience*, *20*(1), 101–112. https://doi.org/10.12694/scpe.v20i1.1460

[23] Ren, Y., Fang, Z., Liu, D., & Chen, C. (2018). Replay attack detection based on distortion by loudspeaker for voice authentication. *Multimedia Tools and Applications*, *78*(7), 8383–8396. https://doi.org/10.1007/s11042-018-6834-3

[24] Ribeiro De Mello, E., Silva Wangham, M., Bristot Loli, S., da Silva, C. E., Cavalcanti Da Silva, G., de Chaves, S. A., & Bristot Loli, B. (2020). Multi-factor authentication for shibboleth identity providers. *Journal of Internet Services and Applications*, *11*(1). https://doi.org/10.1186/s13174-020-00128-1

[25] Schueffel, P. (2017). Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph - A High-Level Overview and Comparison -. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3144241

[26] Sharma, G. (2017). Pros and cons of different sampling techniques. *International Journal of Applied Research*, *3*(7), 749-752. https://www.allresearchjournal.com/archives/2017/vol3issue7/PartK/3-7-69-542.pdf

[27] Sheklashvili, G. (2020). *Multi-Factor Authentication (MFA) on a Blockchain-based Decentralised Trust Network With Customizable Challenges* (thesis). ResearchGate, Tallinn.

[28] Umar Iftikhar, E., Kashif Asrar, Waqas, M., Syed, E., & Ali, A. (2021). Access Management Using Knowledge Based Multi Factor Authentication In Information Security. *IJCSNS International Journal of Computer Science and Network Security*, *21*(7), 119. https://doi.org/10.22937/IJCSNS.2021.21.7.15

[29] Williamson, J., & Curran, K. (2021). The Role of Multi-factor Authentication for Modern Day Security. *Semiconductor Science and Information Devices*, *03*(01), 16. https://ojs.bilpublishing.com/index.php/ssid/article/view/3152