Pre-thesis -I Report

Three Factor Authentication

Name and ID:

1) **Mohammad Naveed Hossain – 17201018**
2) **Sheikh FahimUzzaman – 18101597**
3) **Tazria Zerin Khan – 18101477**
4) **Sumaiya Azad Katha – 18101447**

Supervisor: Dr. Muhammad Iqbal Hossain

Co-supervisor: Mr. Md. Tawhid Anwar

Date of Submission: 1st of June 2021

Department of Computer Science and Engineering

BRAC University

Three Factor Authentication

Abstract

We live in a technological era where technology controls our lives in a good way or in a bad way. In today's digital world we can not imagine a single day without technology and for security purposes we mostly rely on single-factor authentication or two factor authentication. While using two factor authentication (2FA) our data can still be hacked. 2FA has some weaknesses and for that reason our password can be easily cracked or hacked by hackers, even when hackers do not have our OTP. To solve this weakness and make our data more secure and reliable we use three factor authentication so that any unauthorized person cannot easily access our data. We use 5 steps with 3 authentications. First one is username and password after verification, second one is OTP and if both are verified, the last and third one is biometric such as fingerprint, voice recognition etc. Through these three authentications we can protect our data, make it secure and trustworthy for every user.

I. Introduction:

The Information Technology sector is getting advanced day by day. People nowadays use the IT sector as a part and parcel of their life. As every coin has two sides people are getting what they need from this sector and also people are getting into trouble because of the vulnerability in the security of this sector. Single factor authentication is not able to keep up with the security breaches so people started to get along with the Two factor authentication which is also not enough to make sure better security. The two factor authentication uses a physical token which is easily accessible to the unauthorized person. As an OTP is sent to the user in 2FA it can be easily intercepted by the unauthorized person. Other than that social engineering attacks,password-guessing attacks, sim cloning and phishing attacks are common for the 2FA. So, to ensure the best security possible Three factor authentication 3FA is introduced which contains an extra layer of security with biometrics which is something the user possesses. So due to this Multiple layer of security it gets more complicated for the unauthorized person to get logged in with the correct credentials of the user. The main goal of 3FA is to increase the security

of the whole system and make things complicated for the unauthorized person to figure out the correct credentials of the user.

A) Research Problem

The concept of two-factor authentication was introduced on July 4, 1986. In 2011 google and Facebook introduced two-factor authentication on their software. In 2021 two-factor authentication is a common part of any communication-based software. Since it is now a very old method, it is now available in large numbers and two-factor authentication is now easily possible to hack. There are many loopholes in two step authentications. Data is not totally secured. According to 'PCIGURU' two factor authentication is 97-98% secure on the other hand three factor authentication is 99.9% secure. Two factor authentication can be hacked by different MALWARE (Virus: corrupts a particular file, Worms: Multiply the file for several times, Trojan: usually disguised as benign or useful software that you download from the Internet, but they actually carry malicious code designed to do harm). Along with malware two factor authentication can be hacked by SOCIAL ENGINEERING (Phishing emails, Physical Breaches,Pretext calling).

B) Research Objective

The goal of our research is to make the data more secure. I want to reduce the tendency of data hacking. The objectives of this research are:

1. To deeply understand the concept of three-factor authentication and how it works.
2. To deeply understand the knowledge factor, possession factor and inherence factor.
3. Ensure more security to data.
4. Ensure more privacy to private communication.

II. Literature Review:

The research work [10] Primarily this has been through the use of two-factor authentication methods. Two-factor authentication is the combination of single-factor authentication mechanisms. The focus of this research is to address and analyze the implications of using a three-factor authentication model for added security in websites and mobile apps. This paper will present an app we created which could provide a potential method for three-factor authentication that could potentially ensure added authentication assurances without loss of convenience.

This paper makes a step forward in solving this issue by proposing a generic framework for three-factor authentication to protect services and resources from unauthorized use. The analysis shows that the framework satisfies all security requirements on three-factor authentication and has several other practice-friendly properties. The future work is to fully identify the practical threats on three-factor authentication and develop concrete three factor authentication protocols with better performances.

The research work [2] Primarily this has been through the use of three-factor authentication methods. Two-factor authentication is the combination of single factor authentication mechanisms. The focus of this research is to address and analyze the implications of using a three-factor authentication model for added security in websites and mobile apps. This paper will present an app we created which could provide a potential method for three-factor authentication that could potentially ensure added authentication assurances without loss of convenience.

Security concerns are on the rise in all areas of industry such as banks, healthcare institutions, industry, etc. Due to the proliferation of mobile devices and the heightened interaction between mobile applications and web services, the authentication of users is more frequent for mobile devices than for desktop users. In many instances of multi-factor authentication, both a mobile device and a desktop are necessary and go hand in hand for adequate authentication.

The implementation of a future market standard of a three-factor authentication method seems all but assured with the use of biometrics and other authentication methods when used in an efficient

way. The increased reliability of a more secure platform with three-factor authentication is hard to ignore.

The research work [6] C.Lakshmi Devasena has proposed an MFA(Multi-factor Authentication) model which is a three layered approach that is able to ensure safety of the user.As most of the users have a tendency to use apparent passwords, easily guessable password , simple password and moreover same password is used in multiple accounts.Also people try to store the password in the system so that they can use it for future use which really puts them into a more hack prone zone. So, in this proposed MFA system for authentication it uses two more diverse factors in addition to the normal authentication which helps to authenticate the user with more security. The new proposed scheme consisted of an Alphanumeric password , a graphical password and a security question which the user selects and only the user knows the answer to. The scheme mainly works with the First Factor as Alphanumeric password (password that was set by the user while making the account)if the password matches than it moves to the Second Factor that is the Graphical password (such as click points, Pass faces, image and picture based data) and if it matches than it moves to the Third and Final Factor where the security question set by the user is asked if it matches than there will be successful authentication of user and that user will get logged in to the system .The author didn't used any kind of biometrics for three factor authentication because to make the scheme more cost effective and user friendly.

She also added some benefits of the scheme as it increased the privacy preservation of the user . Also as it had three layered protection so it increased the depth of security. Other than that she also highlighted some weaknesses as there are three steps to be followed to login so it's really tough to remember all of the passwords. Also as it has to store three types of data so the memory management was not that much efficient . Lastly, the author talked about the part as it is three layered so users needed to spend some additional time to get logged in.

The research work [9] Wireless sensor Network (WSN) is composed of sensor nodes that are self organizing through the application of wireless network technology. It requires higher security but

during the transmission data may get exposed. To solve this problem researchers proposed numerous security authentication protocols. The recent scheme that was proposed was by Wu et al. it is a 3FA protocol. But in this paper the authors proposed a model which is better than the 3FA proposed by Wu et al. In this paper the author described how Wu et al.'s Protocol subject to key compromises such as impersonation attack and temporary information attacks.It also highlighted how the messages passed using Wu et al.'s Protocol can be eavesdropped, intercepted and modified. Moreover, the interceptor can guess the password and identity of a user.Now in the proposed model by the authors they proved the correctness of their scheme using the BAN (Burrows–Abadi–Needham) logic. Also they used ProVerif simulation tool to ensure whether their model had any kind of vulnerabilities or not cause the ProVerif tool can simulate and return the attack sequence.Furthermore, the authors compared their scheme with Wu et al. protocol that how it failed to provide user anonymity , was more prone to temporary information attack also violated perfect forward backward security. Lastly, the authors pointed out how their proposed scheme was more efficient and secured compared to the Wu et al. protocol.

The research work [8] Authentication is considered as the first step of security requirement for any grid environment against probable threats. This paper proposes an authentication method which is based not only on the password and the user ID but also on the biometric input and the OTP .we are going to use three factor authentication for bank account transactions where in such transaction we need to have more security we are using RFid for embedded security and face recognition for biometric security and GSM communication for password security. In remote authentication schemes, the remote system gains information about the identity of the communicating Person or device. Since the introduction of Lamport's scheme [10], several new proposals and improvements on two- factor remote systems authentication [6, 7, 8, 9, 11] have been proposed. The adversary is modeled as follows: a)The adversary can tap the communication channel between the users and the server during the login and authentication phase. b)The adversary either can extract the information by obtaining the smart card or can get a user's password and Fingerprint. The adversary cannot do both, or the adversary can login the server as a legitimate user. c)Three-factor authentication method was introduced as advancement to

two-factor authentication schemes in remote authentication. The three factors used in authentication are a smart card, password and a biometric. The authentication is based on the characteristics of these three factors. To improve the security in remote authentication, biometric was introduced. Due to the uniqueness and the characteristics of biometrics, they are quite suitable for user authentication and also reduce the drawbacks inherited from passwords and smart cards.

The research work [7] Using oBWNs(On body wireless networks), the vital physiological information of the patient can be gathered from the wearable sensor nodes and accessed by the authorized user like the health professional or the doctor. Since the open nature of wireless communication and the sensitivity of physiological information, secure communication has always been a vital issue in oBWNs-based systems. The proposed scheme adopts a one-time hash chain technique to ensure forward secrecy, and the pseudonym identity method is employed to provide user anonymity and resist against desynchronization attacks. There are four kinds of participants: registration authority (RA), the user, gateway node (GWN), and wearable sensor nodes. The(RA) is a trusted third party, who is in charge of generating system parameters and the registration of all the users, GWN, and wearable sensor nodes. The user, such as a health professional or the doctor , which has high computation and communication capabilities, is the critical intermediary between the user and the wearable sensor nodes. The wearable sensor nodes, such as blood pressure sensor, cardio sensor, and pulse sensor, deploy around/on the patient's body and collect vital physiological information of the target patient. Using oBWNs, it is possible to provide the continuous and real-time monitoring of the patient, regardless of the patient's location. The security of the proposed scheme is proved by rigorous formal proof using the BAN logic model. Through the heuristic, we have proven that the proposed scheme can not only provide some excellent security and functional features, but also resist various malicious attacks, such as desynchronization attack and mobile device loss attack. Compared with the state-of-the-art schemes, the low computation and communication costs as well as high security make the proposed scheme more suitable for remote patient monitoring in oBWNs-based systems.

The research work [3] Security vulnerabilities of traditional single factor authentication have become a major concern for security practitioners and researchers. Online user presence increased considerably in the last decade (Kemp 2017), where in 2018, 89% adults in the U.S. reported using the internet daily (Statistic 2018). Such exponential growth in users and data (Patil & Seshadri 2014) has warranted security practitioners to become more concerned with online data security (Al Hasib 2009) and access control issues (Cuzzocrea 2014) . Irrespective of increased data security (Labana et al. 2013), MFA tools have several usability challenges (De Cristofaro et al. 2013), such as a user's lack of motivation (Das et al. 2019.), risk trade-off understanding (Tari et al. 2006), and presence of non-intuitive user interfaces (Braz & Robert 2006). Conducting user studies (Keith et al. 2007) to provide proper risk alignment have been proven to be effective in improving digital security through adoption. Studies on the usability of authentication methods is often undervalued by security practitioners (Egelman et al. 2014). Thus, a detailed systematic literature review is imperative to understand where we can improve as a research community.

The research work [4] "Access to Network Login by Three-Factor Authentication for Effective Information Security " works on security that can protect our data, keep it trustworthy and make more trouble for unauthorized people to login and excess data. In the present world, our data is not secured and can be easily hacked by hackers even though we have single factor authentication or two factor authentication. This paper aims to secure that problem by using three factor authentication(3FA). They used three approaches. First approach is the password which is an alphanumeric password and the component is what you know. The second one is ATM cards (something the user knows) or PIN (something the user possesses) and the component is what you have. And the last and third approach is biometrics such as unique identity, retina scan, fingerprints and the component is what you are. 3FA improves our security rather than two factor or single factor authentication as the last method is biometric so every person will have a different identity which can not be easily hacked by any users and our data will be safe. But their approach has some drawbacks. The main issue is cost. Three factor authentication is more costly than other approaches as for (3FA) in the last step we need biometric fingerprint impression,

palm right, and retinal output. Apart from the cost thing, three factor authentication is very useful for security purposes and it can be more efficient if we can find a way to reduce the cost.

The research work [5] “On the (In)Security of Mobile Two-Factor Authentication” finds out drawbacks and weaknesses of two factor authentication. Facebook, Google, Twitter, Dropbox uses 2FA and this paper investigates how it can be hacked easily even if it uses 2FA. In two factor authentication first authentication is password and secondary authentication is ATM cards or PINS. Even though your ATM card or PIN is unique and only you can know and if the secondary authentication (PIN) is not in hackers control still hackers can hack it. In this paper, they present a general attack against 2FA and use both mobile phone and PC for authentication. For attacking purposes they use TAN and 2FA. Though 2FA is reasonable, easy to manage and largely usable, still lack of security is a major issue here. So, for better results we can implement three factor authentication (3FA) instead of two factor authentication (2FA) as it is a much more reliable, trustworthy and safe authentication system.

The research work [1] the author Greg Barrow has pointed out why the two factor authentication 2FA is not possible anymore. The 2FA authentication is a two step process for the user to sign in in the first step the user inputs their password and on the second step there is a physical token such as debit card or a passcode or OTP code that is send to the the user's cell phone by a third party security system.Here , the author added this 2FA could make the user's annoyed and cut corners and take shortcuts that makes the system more vulnerable. In addition 2FA doesn't even provide identity authentication. Instead it authenticates the device under this assumption that it is under the control of the user. Moreover, the hacker can crack this 2FA only by stealing a physical token or cell phone which can be done virtually by using sim cloning that was done in 2019 with the Twitter CEO Jack Dorsey the author added.Moreover, Social Engineering attacks other than these phishing attacks are commonly seen nowadays. Lastly, other than discussing the problems of the 2FA the author also talked about some solutions to solve this problem with Biometric Authentication which only the user can possess.Though the Biometric technologies have shown a lot of vulnerabilities but at this moment it has made it more challenging for the hackers to hack into the system.

III. Work plan

The purpose of the Three Factor Authentication is to make the data more secure and increase the privacy of the software.

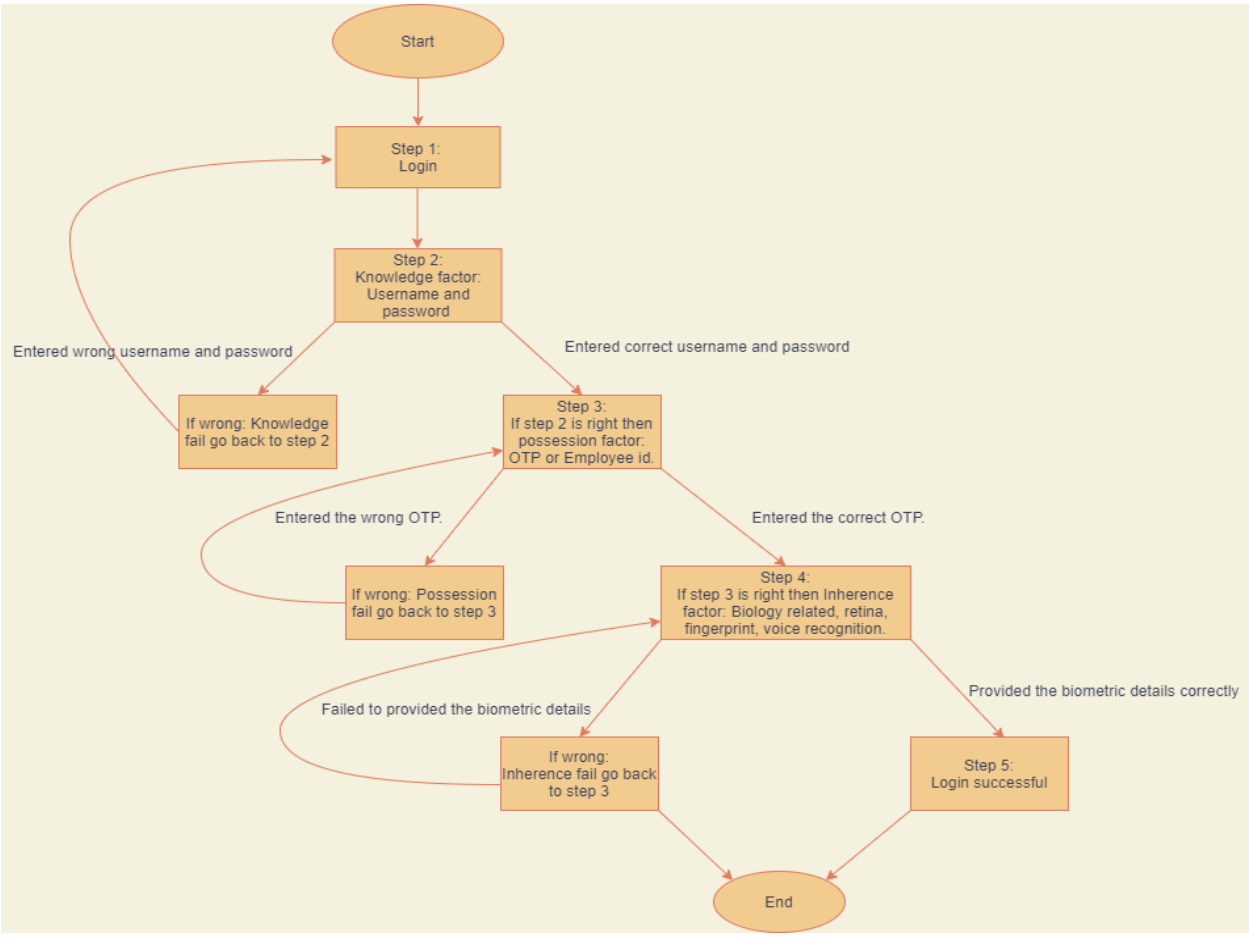

Figure 1: Flowchart of three factor authentication

Three factor authentication works step by step. Mainly it is a 5-step process.

1. At step 1 the user has to login with username and password. User has to enter a valid username and a strong password.

2. At step 2 the verification will be started and the system will match the username and the password with the database. This step is known as the possession factor. If the username and the password match with the database the system will forward to step-3. If the user enters the wrong

username or password the system will loop to step-1 again and will ask the user to enter username and password correctly.

3. At step 3 the second step verification will be started which is known as possession factor. In this step OTP or similar kind of employee id will be used to verify. In the OTP system the user will receive a 4-to-6-digit pin in their personal phone number. If they fail to enter the pin number correctly it will be looped to step 3 again and will ask for the new OTP. If the user entered the OTP, then it will move to step 4.

4. At step 4 the last verification will be started and it is the most important step of verification and our main purpose of the research. This step verification is known as Inherence factor. In this step the users have to verify themselves via biometric. In this step there can be fingerprint verification, face recognition or voice recognition. If the fingerprint matches with the user, then the system will move forward to step 5 and if the match fails then the system will be looped to step 4 again and have to put the fingerprint again.

5. Step 5 is the final step if users verify themselves in step 2,3 and 4 they will successfully login to the software and they can use the software.

IV. Conclusion

Advancement in validation technique has to look into the authentication inequalities in the coming times not for the present time. At this moment, one needs to invest more to get a prominent standard of security. preserving the standard of security will be tougher and more frightening with time. Some challenges can be predicted and estimated just like reformation in computation that are making it systematically easier to dictionary-attack a password database. Some challenges are harder to forecast, for example, the exposure of new "day-zero" vulnerabilities in the software being used. Therefore, security preconditions are not altered, yet increment with time. Three-factor authorization can be habitually being Three-factor authorization can be habitually being utilized to work around the basic inadequacies in password administration. Integrated three-factor authentication gives the best expediency for better security. As the confirm mechanism for authentication, the proposed view can be suitably used in many secure-critical applications/areas especially in the web oriented applications. The absolute goal is that the proposed three-factor authentication will evoke more vital security.

References

[1] Barrow, G. (2020, November 17). *What's Wrong with Two-Factor Authentication?* Retrieved from Security Scorecard: https://securityscorecard.com/blog/whats-wrong-with-two-factor-authentication

[2] Contributor, T. T. (2014, December). *three-factor authentication (3FA)*. Retrieved from Tech Target: https://searchsecurity.techtarget.com/definition/three-factor-authentication-3FA

[3] Garska, K. (2017, September 28). *Why SMS 2-Step Verification Won't Keep You Safe*. Retrieved from Identity Automation: https://blog.identityautomation.com/why-sms-2-step-verification-wont-keep-you-safe

[4] S. Vaithyasubramanian, A. Christy, D. Saravanan, "Access to Network Login by Three-Factor Authentication for Effective Information Security", The Scientific World Journal, vol. 2016, Article ID 6105053, 5 pages, 2016. https://doi.org/10.1155/2016/6105053

[5] Dmitrienko A., Liebchen C., Rossow C., Sadeghi AR. (2014) On the (In)Security of Mobile Two-Factor Authentication. In: Christin N., Safavi-Naini R. (eds) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science, vol 8437. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_24

[6] A Three-Factor Authentication Scheme in ATM Volume 13, Number 10 (2018) pp. 7576-7579 © Research India Publications. http://www.ripublication.co

[7] Mengxia Shuai, Bin Liu, Nenghai Yu, Ling Xiong, "Lightweight and Secure Three-Factor Authentication Scheme for Remote Patient Monitoring Using On-Body Wireless Networks", Security and Communication Networks, vol. 2019, Article ID 8145087, 14 pages, 2019. https://doi.org/10.1155/2019/8145087

[8] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," Electron. Lett., vol. 38, no.12, pp. 554–555, 2002.

[9] Tsu-Yang Wu, Lei Yang, Zhiyuan Lee, Shu-Chuan Chu, Saru Kumari, Sachin Kumar, "A Provably Secure Three-Factor Authentication Protocol for Wireless Sensor Networks", Wireless Communications and Mobile Computing, vol. 2021, Article ID 5537018, 15 pages, 2021. https://doi.org/10.1155/2021/5537018

[10] Edward F. Gehringer "Choosing passwords: Security and Human factors" IEEE 2002 international symposium on Technology and Society, (ISTAS'02), ISBN 0-7803-7284-0, pp. 369 - 373, 2002.