Adding Knock Code Technology as a Third Authentication Element to a Global Two-factor Authentication System

Mohammad Naveed Hossain
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
naveedhossain99@gmail.com

Sheikh Fahim Uz Zaman
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
sheikh.fahim.zaman@gmail.com

Md. Shaba Sayeed
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
shaba.sayeed@gmail.com

***Abstract*—Cyber security is supported by three pillars: authentication, integrity, and confidentiality. There are a variety of consumer-accessible methods for bolstering the security of password-based login systems. Generally, two-factor authentication was utilized for this purpose. Two-factor authentication employs a mix of previously utilized techniques to assure security. In today's technological world, the desire for privacy and security has led to the widespread use of two-factor authentication. Customized, simple-to-implement security solutions are more popular and bought due to their better efficacy. This study examines the outcomes of using a three-factor authentication technique for enhanced website and mobile app security. In this post, we'll explain an app we've built that provides a possible three-factor authentication solution that is both easy and secure.**

***Index Terms*—OTP, Authentication, 2FA, 3FA, Hacked, knock code, alphanumeric password, data protection, network security, three-factor authentication.**

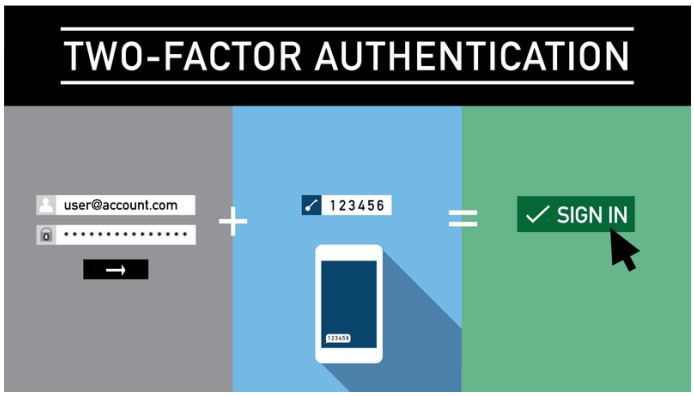

Fig. 1. Two Factor Authentication
[7]

I. Introduction

Daily, innovative breakthroughs are made in the field of information technology. The information technology industry is now deeply ingrained in people's daily lives. Individuals are able to meet their demands with the support of this sector of the economy, illustrating once again that there are two sides to every coin. In addition, individuals are getting into difficulties as a direct result of the business's many security issues. Numerous security vulnerabilities plague this business. A single element of authentication cannot keep up with the rate at which weaknesses in security are discovered. As a result, individuals were used to two-factor authentication, which is insufficient to provide significantly enhanced security. Because two-factor authentication employs a physical token, it is simpler for unauthorized individuals to get the token. When a user engages in Two-Factor Authentication, a One-Time Password (OTP) will be sent to the user through email (2FA). [2] The act of taking it requires little effort from the unauthorized individual. Use Two-Factor Authentication to prepare for social engineering, password guessing, sim cloning, and phishing attacks. To provide the highest level of security, both the three-factor authentication system and the three-factor authentication system were implemented. These systems use the user's knock code information, which the user generally has, to provide an additional degree of protection. On the market now are a variety of devices that do not permit the deployment of knock code authentication. The purpose of this project was to develop a pattern recognition system that could accommodate any knock code passwords. The purpose of the research was to describe the system. As a result of these multiple security layers, it becomes more challenging for an unauthorized user to log in using the user's credentials. The primary objective of three-factor authentication is to raise the system's overall level of security and make it more difficult for unauthorized parties to identify a user's legitimate credentials. The most important aim of three-factor authentication.

II. Existing Authentication Method

A. Connected Pieces

In an attempt to improve network safety. proposed including knock codes as one of three authentication elements in a three-factor authentication system. In this study, we suggest a three-factor authentication system, which includes a password, a smart card, and knock codes. This idea paved the

way for the development of current technology and an in-depth analysis of the drawbacks of fewer security measures, both of which contributed to the implementation of facial recognition into this application. Research on this topic has been profoundly influenced by the ongoing controversy around the efficiency and effectiveness of knock code authentication. The proposed technique was robust enough to survive many attacks while keeping hosts' media and network resources available. While multi-factor authentication has its benefits, it may become cumbersome when apps try to communicate credentials to independently running software processes. The delegation of credentials to non-contiguous software processes opens a security hole. Credentials should not be given to background programs in order to improve system security. Based on the results of this research, they should never have been distributed. According to HCPro's "two-factor authentication: cyber security for the contemporary world," two-factor authentication is crucial to even the most fundamental security program. The study and debate in this article mostly concerned prioritizing speed and ease of use above safety. This research is important to my ongoing work since it emphasizes streamlining the process as much as is practical and linking many processes with the fewest possible clicks.

B. Methods of Current Authentication and Their Steps

Two-factor authentication is the norm for security now more than ever. Today, Google, Facebook, Apple, and other online and mobile banking providers adopt two-factor authentication. The cornerstone of Two-Factor Authentication is One-Factor Authentication, which may be as simple as an email address or login and password. When a user properly enters their email address and passphrase, an OTP will be issued to their mobile device. Registration requires the user's phone number so the system can reach them. An OTP is only used to get access to the system, after which a password is required. According to the reports, the double-layer shielding seems to be fairly dependable and versatile. [4]

C. The Privacy and Security Risks of One-Time Password

In social software and financial websites, one-factor or single-factor authentication is unusual. It was formerly much more abundant and ubiquitous. Its utility deteriorated over time since it might be hacked in several ways. The most frequent include phishing, social engineering, malware, shoulder surfing, etc. In Phishing, a malicious link is provided to the user. If the user clicks the link and inputs the desired data, it will be sent directly to the hacker. Using this information, the individual may quickly take control of the account. In a social engineering attack, the hacker calls the user acting as a technical support agent and offers assistance. During the service, the hacker acquires all the information necessary to hack the user. Once upon a time, the CEO of a United Kingdom-based company lost 201,000 euros to a hacker who used social engineering. Malware is the most common hacking technique. Continuously, harmful files are transmitted to the sensitive information of the user. Shoulder surfing is also a cause of hacking, since nearby parties may see or guess the username and password used to access the system. Therefore, single-factor authentication may be hacked.

D. Two-factor authentication raises privacy and security issues

Rapid use of two-factor authentication has led to improved online safety. But with each passing day, it ages more and more rapidly. As the weather becomes colder, the tools to break into it become more readily available. SMS-based Attacks such as "Man in the Middle," "pass the cookie," "server-side forgery," etc. SMS man in the middle attacks include the hacker interposing himself between the server and the target. However, he uses many deceptive methods to make the user believe that he is really the server. Thus, we may make concessions on two fronts at the same time. Initially, the cookie is sent to the user's browser so they may remain logged into their apps. A hacker may get access to your account if they obtain this data. The following are many examples of 2FA in action. The list of possible, less common uses is endless.

III. Design Concept

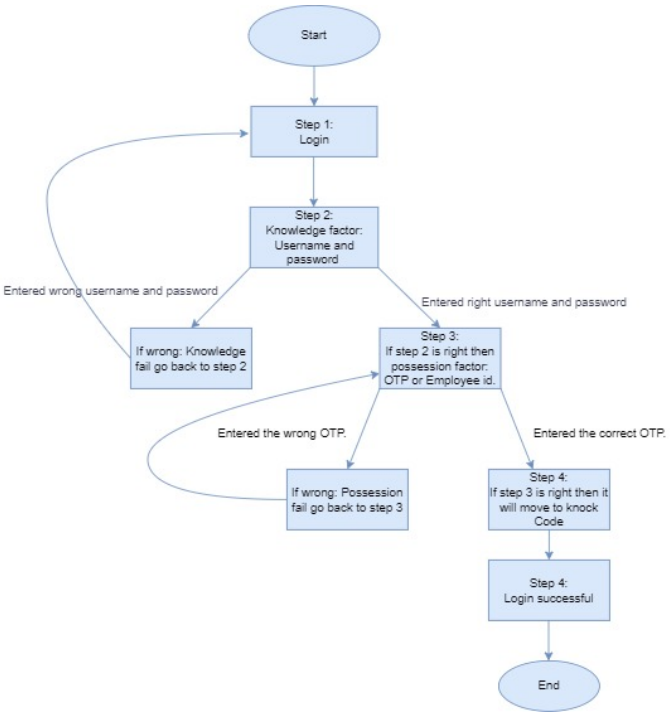

Fig. 2. Proposed Model

A. Overview of the Approach taken by the Suggested Model

Using three-factor authentication requires following a certain order of steps. This method normally consists of 5 steps. As a first step, the user logs in with their own credentials (username and password). The user must provide a valid username and strong password. Getting started with the verification process is the second stage. The user's credentials are verified against a database to see whether they match. This is known

as the ”possession factor.” The third step will be entered if the entered credentials check out in the database. A new session will be started if an incorrect username or password is used. [1] The possession phase of the second verification step is kicked off in stage three. Here, we'll use a one-time password (OTP) or other employee id for verification purposes. In OTP systems, the user will get a 4- to 6-digit PIN by text message. If the wrong PIN is entered, the procedure will begin again at Step 3 to ask for a new OTP. In step 4, if the user has enabled three-factor authentication, they will have access to the public platform. Once a user chooses they don't wish to utilize three-factor authentication, the sequence terminates and they may begin logging in at step 4 on their next service usage. When a user selects three-factor authentication, they are given a choice between two options. Users with a sophisticated smartphone may choose for the knock code password, while those with an older device can use the knock code option. Note that if the user chooses the knock code password, steps 1-3 will continue to work as usual, but step 5 will change. Step 7 will be reached if the correct knock code password has been supplied. The user will be successfully signed in if their knock code password was input, and the procedure will begin again at Step 5 otherwise. If the user choose to use a knock code password, the first six stages will operate normally. If a knock code password is entered successfully, the login procedure will go to step 7; otherwise, it will return to step 6 to ask for a new password. Users will be able to log in securely using three different authentication methods after completing the aforementioned five steps. subsectionImplementation and Proposed Model

1) The Login Window : In the initial stage, you'll see the login screen. There, you'll be prompted to log in using a user name and password. If the user gives a legitimate login, complete name, and password, our first layer of authentication will take effect. The page will stay untouched if the user enters an invalid username or password. When the problem has been resolved, it will go on to the OTP sender phase. [2]

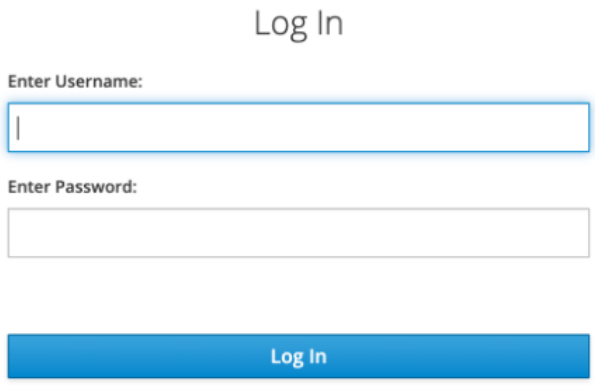

Fig. 3. Login Page
[3]

2) One-Time Password Transmission Authentication Service Provider : The OTP provider stands in for a second layer of authentication. If our first authentication is successful, we will proceed to the OTP step, where the user will get a four-digit PIN via text message. After correctly inserting the nail, the user moves on to the next step, which involves a third authentication factor if one was selected. If this is the last message, then the user's two-factor authentication login was successful.

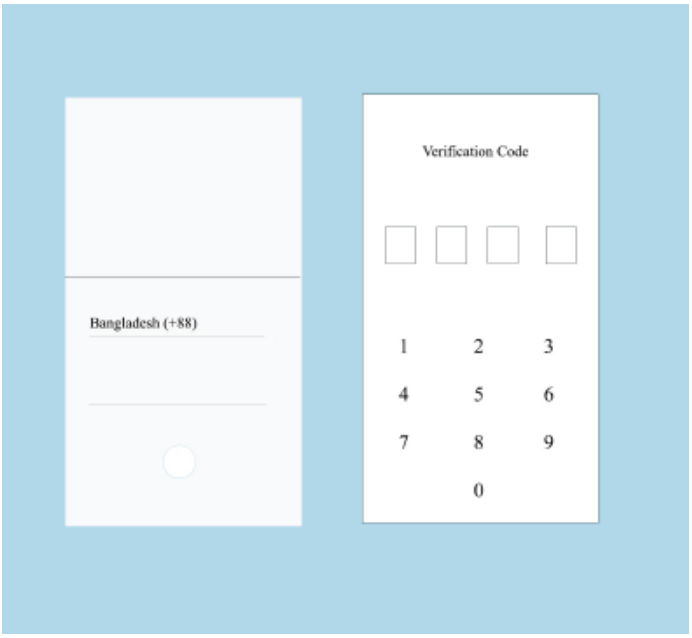

Fig. 4. OTP
[5]

3) Knock code : Knock Code is a specialized kind of security code used to protect the user. It may stand in for pattern in several contexts. Not only that, but it offers more security than patterns do. The matrix used in the processing of the tap code will be three by three, for a total of nine cells. The user will then touch the cells to train the knock code. More than one tap will be recorded for each cell. Therefore, the knock code will be required the next time the user attempts to log in. You'll need to knock those cells in order, just like you did when you learned the knock code. If someone shoulders surfs the pattern, they can crack the code since it's drawn in full on the screen. However, if the user instead enters a knock code, no one will be able to tell where the knocks came from or how many times they were repeated.

IV. Result Analysis

Single-factor authentication relies on a password, which might be compromised in a very short amount of time. Single Fig. 8's complexity. Correctly Sequenced Image Passwords T=2 log2 [AN/(109 3600)] is a suitable example factor, where A is the list of all authorized characters and N is the length of the password. The XNOR gate has complexity O(A XNOR B), the AND gate has complexity O(A AND B), and the difficulty

Fig. 5. Knock Code

of two-factor authentication is T = 2 log2[AN/(109 3600)]. (A.B). T = 2 log2[AN/(109 3600)] Complication Level = + O(A XNOR B) + O(A XNOR B) (A.B) Two-factor authentication, like any other security mechanism, may be defeated, however doing so requires more time and effort owing to the intricacy of the attack routes. Three-factor authentication also includes the use of passphrases, pattern locks, PINs, and secret questions. The difficulty of a secret question or PIN is roughly the same as that of a password; the complexity of a 33 pattern lock system is 9P3 = 504; whereas the complexity of a 44 pattern lock system is 4P3 = 43680, both of which can be cracked in under an hour. Our suggested model for pictorial passwords ensures a complexity of T = 2log2[AN/(1093600)]. Where Vy is the Horizontal Complexity of the knock code matrix, Vx is the Vertical Complexity of the knock code matrix, and I is the Identity Matrix, then + O(A XNOR B) + (A.B) + O(i, j) = 0.5 tan1 (Vy(i, j)/Vx(i, j)). Data security is strengthened mathematically with the employment of both knock code passwords and knock code factors over the present manner. Our proposed paradigm has advantages, but it also has some potential downsides. In contrast to laptops, desktop PCs and feature phones are not well-suited for use with knock code passwords. Our solution especially shines on high-end mobile devices and the most recent, expensive laptop models.

V. Discussion and Prospects for Further Study

The progressive invalidation approach will need to be studied in the future to discover the causes of the authentication discrepancies. Enhanced security now comes at a heftier price. It will be more difficult to maintain the existing degree of security. Protection of the security protocol is getting increasingly complex. Due to the fact that certain problems, such as computation reformation, may be easily estimated and predicted, dictionary attacks on password databases are sometimes possible. However, there are certain challenges that are impossible to predict, including the emergence of brand-new ”day-zero” bugs in the software. Thus, security measures must not be altered, but rather must evolve to keep up with evolving threats. Since this is a security problem, three-factor authentication might be a great solution. Using a three-factor authentication system is the most time- and labor-effective approach to improving safety. It also provides a wide range of customization options to suit the needs and preferences of users of varying experience and expertise. So, 3FA might be helpful in a variety of situations. Online banking, online shopping, and online money transfers are just a few examples of the many useful applications of the internet. When using three-factor authentication, users have a few of options. For those who have expensive handsets and limitless data plans, using a knock code password as the third authentication method is a breeze. Biological methods of recognition may also be used, such as those that use a person’s fingerprints, eyes, or voice. Third-party authentication (3FA) may be an option for users that require additional protection but have limited financial resources or inferior mobile devices. Third, people may prefer a knock code password over a knock code one. In this case, we’re talking about a pattern-based password generator. Therefore, a straightforward solution to the cost problem is to provide customers a choice between two different three-factor authentication options. The user is given a few of easy choices for establishing authentication. Taking these precautions will make our database much more secure [7]. We’ve previously demonstrated that our solution offers much improved performance on state-of-the-art mobile devices and desktops. Our objective should be to boost performance for all platforms and users. Our plan was to use this approach with industry leaders like IBM and SOPHOS. We have shown that there are many ways in which the security of 2FA may be breached; however, the strong security measures of 3FA more than make up for this. We also want to create a beta version of our software for use by local companies. Furthermore, we will release a beta version of the app to observe user behavior as they adapt to the new 3FA. Additionally, there is the potential for problems with the visual password. There is much opportunity for improvement in the spatial and temporal complexity of the whole model when it is put into reality [6].

References

[1] Abraham Bookstein, Vladimir A Kulyukin, and Timo Raita. Generalized hamming distance. Information Retrieval, 5(4):353–375, 2002

[2] NevonProjects. Smart android knock code password strategy. 2018

[3] ADEO. Why you should activate two-factor authentication. 2020

[4] K. Garska. Why sms 2-step verification won’t keep you safe. 09 2017.

[5] Hossain, M. N., Zaman, S. F. U., Khan, T. Z., Katha, S. A., Anwar, M. T., Hossain, M. I. (2022, July). Implementing knock code or knock code Password Authentication in a Universal Three-Factor Authentication System. In 2022 4th International Conference on Computer Communication and the Internet (ICCCI) (pp. 72-77). IEEE.

[6] Soumitra Sudip Bhuyan, Umar Y Kabir, Jessica M Escareno, Kenya Ector, Sandeep Palakodeti, David Wyant, Sajeesh Kumar, Marian Levy, Satish Kedia, Dipankar Dasgupta, et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. Journal of medical systems, 44(5):1–9, 2020.

[7] Mr.Jadhav Rajesh S., Chandole Durgesh K., and Mr.Wani Milind D. Graphi- cal password authentication system. knock code Password Authentication System, 3(4):353–375, 2014.