Journal of Theoretical and Applied Information Technology
31st March 2022. Vol.100. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REVIEW OF TEXT BASED PASSWORD AND OTHER AUTHENTICATION METHODS FOR E-COMMERCE DATAPROTECTION

[1]AZANI CEMPAKA SARI, [2]ALSYA CARISSA ZEVANDA, [3]CHRISTIE CLAUDIA HASIANIMALAU, [4]LAURENSIA VILDA YOVIRA

Computer Science Department, School of Computer Science, Bina Nusantara University, Jl. K. H. SyahdanNo. 9 Kemanggisan, Palmerah, Jakarta 11480, Indonesia

E-mail: [1]acsari@binus.edu, [2] alysa.zevanda@binus.ac.id, [3]christie.malau@binus.ac.id, [4]laurensia.yovira@binus.ac.id

ABSTRACT

Significant development of the internet has triggered various new technologies. One of them is e-commerce.This causes the security aspect of e-commerce to be one of important factors, especially to prevent unwantedthings such as data leaks and financial losses. The authentication method is one example to provide protection,such as protection of user data and protection of transactions in e-commerce. In short, the authentication system prevents access by unauthorized parties. Authentication systems may vary from the simplest, namelythe use of passwords, to other methods. The aim of this study is to explore various authentication methods, the advantages, disadvantages, types of attacks that can occur, and the importance of using an authenticationsystem, especially in the e-commerce environment.

Keywords: *Password, Authentication, Data Protection, E-Commerce, Security*

1. INTRODUCTION

According to Wikipedia, authentication is an action or process to prove a statement or action such as the identity of a computer system user [1]. Authentication is carried out in two phases, namely identification and verification. Identification is the process of giving a user identity to a security system,usually in the form of a user ID. After the identity isrecognized, the system will look for data related to the ID to verify identity.

There are five types of authentication methods that are often used [2], namely:

1.Single-factor authentication

- Authentication method in the formof a password is created using letters, numbers, and special characters. Combinations that are created can use all three or only one (i.e. a combination of letters and numbers, a combination of numbers, etc.).

2.Multi-factor authentication

Authentication methods that usetwo or more ways to identify a user. An example is when a user wants to log in to the software on their PC, a code will be generated on their smartphone to log in.

3.Certificate-based authentication

- This authentication method uses the user's private documents to identify them. Used with electronic documents that are created based on a user's personal documents such as a passport.

4.Biometric authentication

- This authentication method uses a user's biological character such as fingerprints, facial recognition, and so on.
-

5.Token-based authentication

- This authentication method uses a unique string made of random

characters. This string will be unique for each user and will be used as a substitute for the personal information that has beeninputted so that the user does not need to re-enter it.

Apart from these several authentication methods, the one most often found in everyday life is single factor authentication, namely passwords. The first password was created in 1960 by FernandoCorbato. Since then, passwords have been widely used in various instances in human technological life to date. Over time, the requirements for a password have become more complex. Every website or application has different password requirements. According to a study by *NordPass*, one person can have 100 passwords to remember. There are passwords that only require characters, some need toadd symbols, numbers, and so on. With multiple websites that have different requirements for passwords, a single user can have multiple different combinations of passwords. As a result, users will eventually create the same password for every account they have. This is detrimental for users because having the same password for all accounts makes users vulnerable to data leakage.

Passwords are also used in various applications and websites. One of them is an e-commerce website / application. E-commerce, orwhat can be called as electronic commerce, is a business model that allows the sale and purchase of products electronically. This action is assisted by various applications / websites that help buyers and sellers to carry out their buying and selling. Like most other applications / websites, users are asked to input their personal information which will help in the business process. This information can range from full name, email, telephone number to ID number or bank account number. This information is included in information that is very personal and important to each user. Therefore, the importance ofsafeguarding this information is very important. With this, we need to learn more about the advantages and disadvantages of passwords and alsoother authentication methods that can strengthen system security in e-commerce.

There are several risks that can be faced if personal information is not properly protected and data leaks occur. One of them is identity theft. This will cause a lot of problems depending on the type ofinformation that was stolen. For example, if theaccount information from a user's mobile banking application was stolen by someone, the person who stole the information can arbitrarily use the assets and information in the mobile banking application for personal gain. As a result, the user whose personal information has been stolen might come to find that they no longer have a balance in said mobile banking application.

In this research, we will discuss further about data protection in the e-commerce industry, three types of authentication methods (password, MFA, biometric authentication), and their advantages and disadvantages. Therefore, the aim ofthis paper is to review passwords as one of the mostfrequently used authentication methods in e- commerce, and how password's weaknesses can affect user data security. Moreover, this paper will discuss other authentication methods that can be used as alternative use of passwords.

2. LITERATURE REVIEW

2.1 Authentication

Authentication is a process for identifying and verifying the identity of a user on a system. Fromthe paper by Pawel Laka and Wojciech Mazurczyk (2018), an authentication process consists of 3 things, namely: something the user knows, something the user has, something the user is [3].

With the rapid development of the Internetand mobile devices, system authentication has been widely used in the process of accessing the internet and mobile devices to protect devices, data, and useraccounts [4]. One of the simplest and most used authentication methods is a password. However, passwords have various security holes, mainly due to limitations on human memory. Users choose passwords that are not easily forgotten, which leads to a substantial fraction, i.e. users prefer passwords that are prone to attacks such as dictionary attacks [5]

Literature [6] Categorizes the authentication method into 4, namely:

- Knowledge-based authentication
- Physiological based biometricauthentication

- Behavior-based biometric authentication
- Two / Multi-factor InformationAuthentication

2.2 Authentication Method Review

2.2.1 Knowledge-based Authentication

Knowledge-based authentication is authentication based on the user's knowledge / memory, which is usually in text or graphic form.

Examples of text, namely PIN and Password, and graphics, namely patterns. The use of text authentication is the simplest and most frequently used authentication method [6] However, it alsocauses passwords to be the most vulnerable to attacks. Passwords and PINs have the potential to receive attacks in the form of brute-force and dictionary attacks, as well as keyloggers [7].

2.2.2 Biometric Authentication

Biometrics is a technology that uses a unique pattern of physical factors or user habits in authentication or identification [8]. Biometric authentication can be divided into 2, namely Physiological Authentication and Behavioral Authentication. Biometric authentication is a method of authentication that has begun to be widely used, especially using fingerprints and faces.

Physiological Authentication performs authentication using the physical features of the user.For example, fingerprint, palmprint, hand geometry,face, eye, ear, ECG, EEG [6].

Behavioral Authentication performs authentication using the user habit feature. For example, tapping behavior, finger gesture, hand gesture, voice, gait, daily activity routine [6].

Compared to other biometric features (face, iris, and voice), the fingerprint recognition system is the most frequently used. [9] Based on a comparison made by [8] which compared 6 different biometric features, namely fingerprints, palms, iris, face, tone, and voice with 3 comparison factors namely false acceptance rate, easy to use, and counterfeit difficulty. As a result, iris has the most difficult counterfeit difficulty, followed by sound. Meanwhile, the false acceptance rate is relatively small apart from fingerprint and iris. and for convenience, the average is not much different, which is still a little [8].

Although biometric authentication is often used, biometric authentication has several problems. Compared to authentication with passwords, there are 2 biggest problems in biometric authentication systems. The first is that the biometric feature cannotbe withdrawn and re-entered or cannot be replaced, such as a password. Second, biometric features are not confidential [4]. In fact, research by literature [6] shows that almost all biometric systems lack privacy protection of the user's biological information.

Multi-factor Authentication

Authentication security can be improved by combining two or more methods, which makes it more difficult for attackers to penetrate the system. [6]

Some examples of combining authentication methods are [10]:

- Traditional (biometric-biometric,knowledge-biometric)
- Ownership (knowledge-ownership, biometric-ownership)
- Advance (knowledge-biometric-ownership)

2.3 E-Commerce and Financial Technology

E-commerce is growing rapidly which opens up opportunities to increase sales via the internet [10]. Following this development, the need for a payment system in the form of an e-payment isurgently needed. E-payment is expected not only to provide a secure payment system, but also to have various properties such as buyer

and seller authentication, transactions that are authorized by buyers, sellers and banks, as well as buyer privacy and data security [11].

To meet the needs and convenience in the E-payment process, the fields of Financial Technology and Fintech are also developing rapidly, especially mobile fintech. In mobile Fintech, payment service is not only done face-to-face, but also by remote internet payment, therefore, mobile devices and users must be authenticated. [11] Thereare several security issues that must be resolved for mobile Fintech payment service providers to be developed in the future, in the literature [12] these problems are classified into mutual authentication, authorization, integrity, atomicity, and availability.

Why is an authentication system in the e-commerce field so needed? As an introduction, one of the fintech e-payment methods that is often used in transactions is QR Code. But has QR Code been safe? In fact, with the widespread use of QR codes in the field of mobile payments, attacks on QR codesare more frequent and can cause financial losses [12].

2.4 E-Commerce and Data Protection

In this digital era, it's easier to count peoplewho don't use gadgets than those who do. The use of gadgets and its progress has greatly increased compared to previous years [13]. There are many types of gadgets circulating around the world. From which the most common are cellphones and computers. In this gadget, we can store our personal information through an application that we can download. Now, many industries are taking advantage of the popularity of gadgets and expanding their business with gadgets. One industry that is currently very popular is e-commerce or electronic commerce.

Due to COVID-19, the use of e-commerce is on the rise. This means that more people have entered their personal information into an application. Therefore, the security of personal data is very important to be maintained in order to reduce risks. Each country has its own regulations to guard against this. However, regulations in Indonesia regarding personal data protection are quite backward compared to other countries [14]. As a result, choosing a correct and secure authentication method is quite important.

2.5 Password in E-Commerce

Of the five authentication methods that have been mentioned, single-factor authentication is the method most often found in everyday life. One example of single-factor authentication is passwords. Password is text-based authentication that allows users to enter letters, numbers, and symbols as a form of authentication. The use of thispassword is widely used as an authentication method to the realm of e-commerce applications and websites. In e-commerce applications, users will always be asked for data such as name, email, date of birth, and bank account for transaction purposes. This data is often only protected by a password or a pin, which is single-factor authentication. Nearly 92% of all transactions that take place in the world are done online making it aninevitable part (Kumar & Cherukuri, 2018) [15].

With so many uses of passwords as an authentication method, users usually use passwords that are easy to remember and the same password for each service they have. This is very risky for user data because there are attackers and hackers who can easily get passwords without the real user'sknowledge to get important information about this user. If a pair of IDs and passwords are leaked, those IDs and passwords can be used illegally to log into any service that uses the same password (Morii, Tanioka, Ohira, Sano, Seki, Matsuura, &Ueta, 2017) [16]. The mishandling of users' personal and financial data can cause huge lossesfor individuals (Pagar & Pise, 2017) [17].

2.6 Password and Security Risk

E-commerce uses online stores to assist the buying and selling process between consumers and sellers. In this business model, users and sellers are required to input their personal information such as full name, telephone number, address, and many more. This personal information is very personal andneeds to be properly guarded. [18] Therefore, an effective authentication method is needed. One authentication method that is very often used is a password. Passwords are an example of a traditional authentication method. Password

consists of a collection of letters and / or numbers that are used to gain access to something.

However, there are some security risks thatcan be faced when using a password. Based on research conducted by Binitha Ann Scaria, Dr. Rajesh Kannan Megalingam [19], there are some security problems using passwords. These security issues are as follows:

- Surfing attack - where thieves can find out a user's account information by watching that user. Thieves can use a device such as a camera, pay attention to keys pressed by the user, or by peeking from the user's side.
- Dictionary attack - the thief will try to inputmany words, such as words in a dictionary,to try to gain access.
- Guessing attack - thieves will try to guess a user's password with that user's personal information, such as name, date of birth, petname, etc.
- Phishing - a thief will act as someone else to persuade a user to do something that could be dangerous. An example is when a user gets an email from, for example, an Apple official, to send personal information that was not sent by an Apple official. Instead, sent by someone else who goes bythe name "authorized Apple".
- Eavesdropping - where a thief eavesdrops on a user talking about their personal information.

2.7 Enhancing Password

Due to the vulnerability of passwords to data leakage, there are several innovations to strengthen passwords. One example is in research conducted by Mrs.Vasundhara R. Pagar and Mrs. Rohini G. Pise (2017) [17] using Honeywords and HoneyEncryption techniques used to support password security. Honeywords are fake passwords that are stored with the original password in the database, while the HoneyEncryption technique usesa Distribution-transformer encoder (DTE) to get theseed space which is then encrypted using a key. Thismethod can trick attackers into thinking they have the correct password, when actually what they get is honeywords.

In addition, there is also an idea from Zheng& Jia (2017) [20] which was inspired by keystroke dynamics to add several blank characters or certain characters in a password as a code that is checked toverify valid users.

The two ideas mentioned above use text- based passwords which are still vulnerable to errors and offline attacks such as dictionary attacks, shoulder surfing, and eavesdropping. Literature review and survey conducted by Asmat, & Qasirrf (2019) [21] proposed the idea of a picture passwordthat can provide better security than using a text- based password. The method proposed is a picture password which integrates the idea of randomizing the images to reduce infiltration attacks such asshoulder surfing and eavesdropping.

2.8 Alternative to Password: MFA

To replace the password, another authntication method can be used. One of them is MF, namely Two-Factor Authentication. 2FA is done by a user inputting a password which will then be authenticated via, for example, their cellphone. One example of using 2FA is SMS, where after a user enters a password, he will receive an SMS containing a code or PIN that will be used to gain access. However, opinions regarding 2FA are still divided because 2FA can be interpreted as entering two passwords, which means that there are still people who can guess it. There are others who are of the opinion that 2FA is good to implement because it can increase the security of the applications they use. Then there are those who only want to use 2FA based on the importance / usefulness of the applications they use [22]. Not only that, because 2FA requires two stages, the time used will be longerthan using one stage.

There is a lot of research being done on MFA. Through these studies, MFA is considered to have helped improve security and increase the login success rate. However, the majority of this research was conducted through experiments but rather surveys [23]. With this, it is possible that the research being carried out does not adequately consider user opinions. So, the results obtained will not necessarily be received well by people.

2.9 Alternative to Password: Biometric Authentication

Apart from MFA, there is another authentication method that can be used, namely biometric authentication. Biometric authentication is a measurement of physiological characteristics (eg, eyes, face, DNA, fingerprints) and behavior (eg, signature, voice) [24]. One example of its use is witha smartphone. When users want to use their smartphone, they must first scan their fingerprint in order to gain access to use the smartphone.

Based on a survey by Spolaor, Li, Monaro,Conti, Gamberini and Giuseppe Sartori (2016) [25] biometric authentication is categorized into 2, namely physiological and behavioral. Physiological biometrics depend on the characteristics of the user's body, while behavioral biometrics depend on the user's behavior with their mobile device. Examples of physiological biometrics are found in research andexperiments conducted by Wu, L., Yang, J., Zhou, M., Chen, Y., & Wang, Q. (2019) who use LVID, a multimodal biometric authentication. based on lip movements or voice [26]. An example of behavioral biometrics is the experiment by Laghari, A., Waheed-ur-Rehman, & Memon, Z. A. (2016) who proposed a method whereby a user uses a smartphone to show his signature on the air [27].

Biometric authentication has good potential because human physical characteristics are difficult to imitate, so the security risk is lower than using traditional authentication methods such as PIN and password [28]. Not only that, in the case of fingerprints or face scans, users don't need to remember passwords or PINs and only need to scanthem. If the user uses a card that needs to be carried,the physical card has a high chance of being lost or

misplaced. Biometric authentication will be very helpful in saving time and hassle [29].

E-commerce is a business model that uses online stores to carry out the buying and selling process between consumers and sellers. The COVID-19 pandemic which has caused many people to stay at home is one of the reasons for the rise of e-commerce. E-commerce applications / websites store a lot of personal information that needs to be stored properly. Traditional authentication methods such as passwords and PINs are considered to have security risks that can be solved using other authentication methods. MFA is a good authentication method, but it is time consuming and more complicated because it requiresseveral steps. Biometric authentication is an authentication method that is developing and after testing, it was found that it can maintain better data security because the physical characteristics of eachperson are different, so it will be more difficult to imitate.

2.10 Future of Authentication Method

From the discussion above, it can be concluded that each authentication method has its own problems that make each of them unbelievable, for example, knowledge-based is prone to public information on social media which can lead to leaks in passwords and security questions. Biometric- based is prone to 3D modeling such as face or fingerprint models. And ownership-based is prone touser negligence such as losing tokens / etc. [7] It canalso be seen that multi-factor authentication has great potential, by combining various authentication methods. However, it should be noted that not all authentication methods are appropriate to be used atthe same time.

The biggest problem with the authentication method is security and user privacy, therefore, in the future, the development of the authentication method can focus on these things.

3. QUESTIONNAIRE RESULTS

3.1 Introduction

We conducted a Questionnaire during the month of May in 2021. The questionnaire we conducted collected data and opinion from 35 participants. The goal for of this questionnaire is to understand the thoughts, understanding, and preferences of these participants.

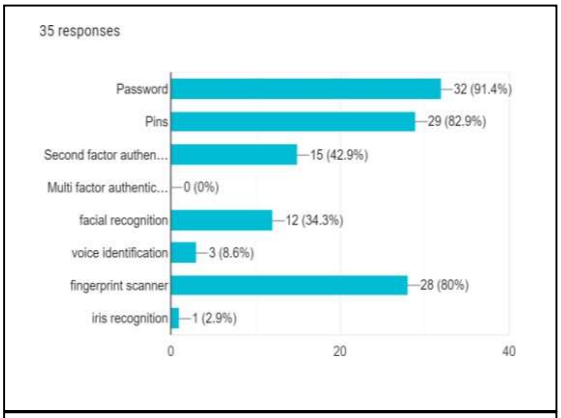
3.2 Results.

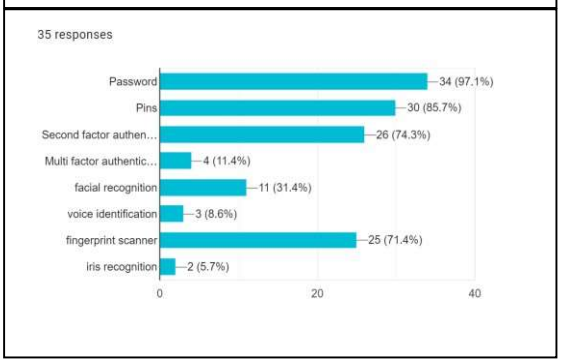
One of the questions we asked to the participants was about the meaning of an authentication method. The participants answered it all correctly which is the process to verify the truth

or integrity relating to an identity.

Another question we asked to theparticipants is about what kind of authentication method they most often come across while they wereusing an e-commerce application/website.

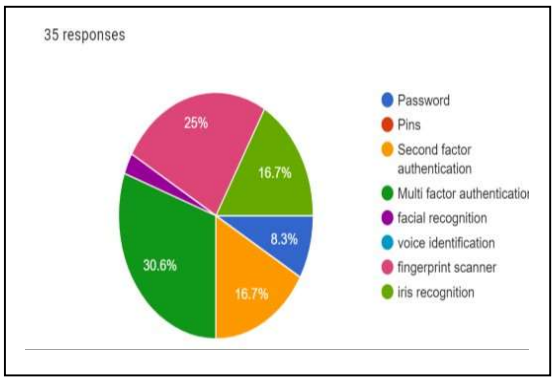
The answer which we received was not at all surprising as we see that Password holds the highest spot with 97.1%, followed by PINs with 85.7%, Second Factor Authentication with 74.3%, followed by Fingerprint Scanner with 71.4%, to which it is followed by the other options. Here, we understand how popular Text-based Authentication Methods are as they dominated the results of this question's results as seen in this picture below.Moving onto the next question, since the previous question was to understand which authentication method is the most popular within e- commerce applications/websites, this next question was made in order for us to know which authentication methods are most popular in their daily lives.





As seen from the picture above, yet again the Text-based Authentication Methods (Password and PINs) dominated the question results. However,in this question, the Fingerprint Scanner with 80% took over third place which is followed by Second Factor Authentication with 42%. Here, we can see that the participants use Biometric Authentication Method in their daily lives more than they did in e- commerce application/website.

The next question we asked was to know the opinions of our participants. We asked them which authentication method was safest according to them.

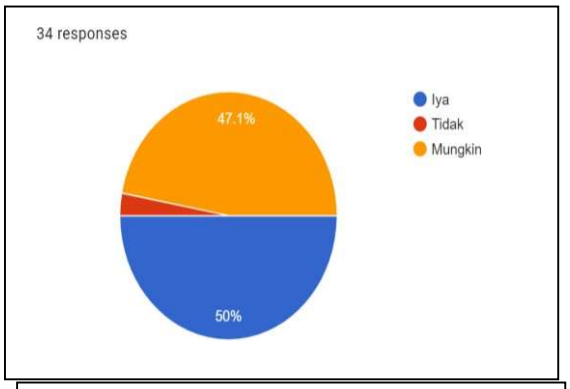


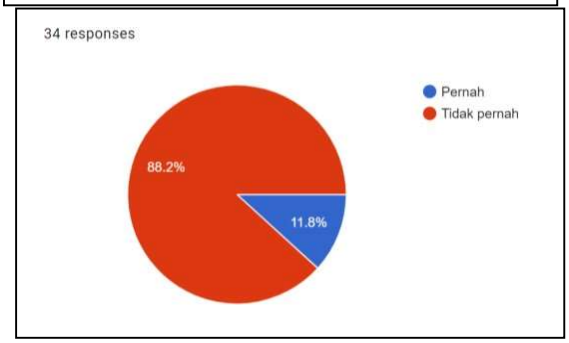
Through this question, we found out that most of our participants chose Multi Factor Authentication to be the safest out of all the choiceswe provided. It is then followed by Fingerprint Scanner, which is a Biometric AuthenticationMethod. With which it is followed by a draw between Second Factor Authentication Method and Iris Recognition, which is also a Biometric

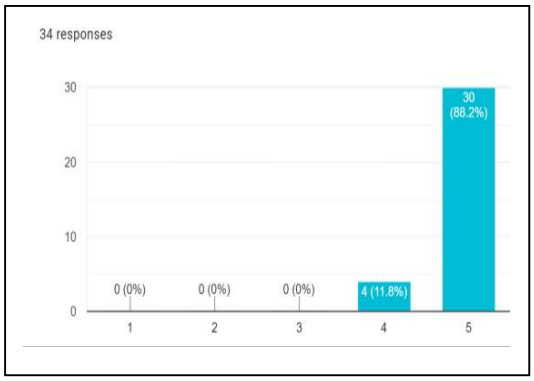
Authentication. Password, the Text-based Authentication Method that kept dominating the firstfew questions fell to 4th place and followed by Facial Recognition, another Biometric Authentication Method, who took last place.

Through this question, we found out that the participants prefer MFA and Biometric Authentication Methods to be safer than usual Text-based Authentication Methods which is, ironically, the most prevalent authentication method as of now.

Moving on, we needed to understand up towhat point was the severity of the risk of losing our personal data through unsafe authentication methods. Hence, we asked our participants to tell us whether or not they have ever had their personal datastolen.







Through this question, we found out that four of our participants have ever had their personaldata stolen. Even though it is a small number, it is still concerning that the risk of getting our personal data stolen is always going to be present.

Previously, we have been asking ourparticipants about the various authenticationmethods that are currently present and widely available. Which of those methods are the safest to them and which of those are widely encountered by our participants? These next few questions will now be pertaining to the importance of Personal Data andits safety.

We asked our participants to choose on a scale of one to five, with one being the least important to five being the most important, how important is the safety of their personal data in e- commerce.

produces several more steps than the usual, moreinstant, and simple authentication methods.

4. CONCLUSION

As seen from the image above, most of our participants picked the number five to indicate that they agree that the safety of their personal data in e-commerce is very important. Although the rest of ourparticipants chose the number four, it is still quite high in the scale as it still counts as them agreeing that their personal data's safety is important even though it might not be the most important.

Our last question towards our participants was to know whether or not they were willing to go through extra steps in order to gain access to their personal data. Extra steps here is pointing to the factthat they would be using Multiple Factor Authentication.

Here, we can notice the uncertainty from our participants as half of them chose yes, that they would be willing to use MFA in order to protet theirpersonal data, followed by quite a bit of participants who chose maybe resulting in a percentage that is not far behind from the majority. And then the minority of the participants chose no, indicating that they arenot willing to use MFA.

The results from these few questions tells us that even though their personal data's safety is important, the ease in order to access it is also quite an important factor. Hence, the participants became unsure whether or not they would use MFA, which

Through this research, we can conclude thatText-based Authentication Methods are commonly used in our daily lives especially in the e-commerce industry. However, it is not the safest authenticationmethod, which was taken from the opinions of our questionnaire participants and also proven through reviewing multiple literature analysis.

Each year, the usage of e-commerce platforms rise. More and more people are selling and buying things online. Of course, these platforms will ask for the user's personal information. Some of which are quite sensitive to the owner, such as, address, ID number, social security number, bank credentials, and so much more.

In order to solve this issue, we reviewed other authentication methods to substitute the Text-based Authentication Methods. The authentication method we deemed the most appropriate, in terms ofease and security, to substiture Text-basedAuthentication Methods are Biometric Authentication Methods and Multiple Factor Authentication.

Biometric Authentication Methods uses a person's own unique biometrical identity which includes our fingerprints, face, iris, and many more.These are things unique only to the owner and is quite difficult to replicate. Hence, not only is it easyto use, it also has quite a formidable security level.

Aside from Biometric AuthenticationMethods, we also chose Multiple Factor Authentication as a worthy substitute for Text-based Authentication Methods. True to its name, it uses multiple authentication methods that needs to, in order, be successfully authenticated for the user to beable to gain access to their personal data. This method is quite safe to use as there are, in a sense, multiple walls that protects the access to a person's personal data. However, the process could be quite tedious to some as its not an instant process like the Biometric Authentication Methods or Text-basedAuthentication Methods.

In summary, there are multiple authentication methods that are currently available. They are used in order to guard our personal data from thieves who might want to steal our personal data in order for their own personal gain which is, ofcourse, done illegally. Which is why, choosing the right authentication method is important as it is the barrier between those thieves and your personal data.

REFRENCES:

[1] Wikipedia contributors. (2021, April 9). *Authentication*.Wikipedia. https://en.wikipedia.org/wiki/Authentication

[2] Maayan, G. D. (2021, March 10). *5 Authentication Methods that Can Preventthe Next Breach*. https://www.idrnd.ai/5-authentication-methods-that-can-prevent- the-next-breach/

[3] Laka, P., & Mazurczyk, W. (2018). User perspective and security of a new mobile authentication method. *Telecommunication Systems*, *69*(3), 365–379. https://doi.org/10.1007/s11235-018-0437- 1

[4] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," in IEEEAccess, vol. 7, pp. 5994-6009, 2019, doi: 10.1109/ACCESS.2018.2889996.

[5] Ammar Hameed Shnain and Sarah Hadi Shaheed , "The use of graphical password to improve authentication problems in e-commerce" , AIP Conference Proceedings 2016, 020133 (2018) https://doi.org/10.1063/1.5055535

[6] Chen Wang, Yan Wang, Yingying Chen, Hongbo Liu, Jian Liu, User authenticationon mobile devices: Approaches, threats andtrends, Computer Networks, Volume 170, 2020, 107118,ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2020.107 118.

[7] Mohammadreza Hazhirpasand Barkadehi, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi, Sarminah Samad, Authentication systems: A literature reviewand classification, Telematics and Informatics, Volume 35, Issue 5, 2018, Pages 1491-1511, ISSN 0736-5853, https://doi.org/10.1016/j.tele.2018.03.018.

[8] ang, W.; Wang, S.; Hu, J.; Zheng, G.; Valli, C. Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry 2019, 11, 141. https://doi.org/10.3390/sym11020141

[9] Huichao Ye et al 2020 J. Phys.: Conf. Ser. 1607 012120

[10] S Fatonah et al 2018 J. Phys.: Conf. Ser. 1140 012033

[11] Kang, J. Mobile payment in Fintech environment: trends, security challenges, and services. Hum. Cent. Comput. Inf. Sci. 8, 32 (2018). https://doi.org/10.1186/s13673-018-0155- 4

[12] Yang, Ching-Nung; Lu, Jianfeng;Yang, Zaorang;Li, Lina;Yuan, Wenqiang;Li, Li;Chang, Chin-Chen. Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography. 2017.https://doi.org/10.1155/2017/435603 8

[13] Fan, K., Li, H., Jiang, W., Xiao, C., & Yang, Y. (2018). Secure authentication protocol for mobile payment. Tsinghua Science and Technology, 23(5), 610-620. https://sci-

hub.se/https://ieeexplore.ieee.org/abstract/document/8450873

[14] Haganta, R. (2020). Legal Protection of Personal Data As Privacy Rights Of E-Commerce Consumers Amid The Covid-19 Pandemic. Lex Scientia Law Review, 4(2), 77-90. https://journal.unnes.ac.id/sju/index.php/lslr/article/view/40904/17466

[15] Pradeep Kumar, K., & Cherukuri, R. C. (2018). Secured Electronic Transactions Using Visual Encryption: An E-Commerce Instance. *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*. https://doi.org/10.1109/icirca.2018.859732 4

[16] Morii, M., Tanioka, H., Ohira, K., Sano, M., Seki, Y., Matsuura, K., & Ueta, T. (2017). Research on Integrated Authentication Using Passwordless Authentication Method. *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*. https://doi.org/10.1109/compsac.2017.198

[17] Pagar, V. R., & Pise, R. G. (2017). Strengthening password security through honeyword and Honeyencryption technique. *2017 International Conference on Trends in Electronics and Informatics(ICEI)*. https://doi.org/10.1109/icoei.2017.830081 9

[18] González Briones, A., Chamoso Santos, P., & López Barriuso, A. (2016). Review ofthe main security problems with multi-agent systems used in e-commerce applications. https://gredos.usal.es/bitstream/handle/10366/132092/Review_of_the_Main_Security_Problems_wit.pdf?sequence=1&isAllowed=y

[19] Scaria, B. A., & Megalingam, R. K. (2018,June). Enhanced E-commerce application security using three-factor authentication. In 2018 Second International Conferenceon Intelligent Computing and ControlSystems (ICICCS) (pp. 1588-1591). IEEE. https://sci-hub.se/https://ieeexplore.ieee.org/abstract/document/8662831

[20] Zheng, W., & Jia, C. (2017). CombinedPWD: A New Password Authentication Mechanism Using Separators Between Keystrokes. *2017 13th International Conference on Computational Intelligence and Security (CIS)*. https://doi.org/10.1109/cis.2017.00129

[21] Asmat, N., & Qasim, H. S. A. (2019). Conundrum-Pass: A New Graphical Password Approach. *2019 2nd International Conferenceon Communication, Computing and Digital Systems (C-CODE)*. https://doi.org/10.1109/c-code.2019.8680989

[22] Reese, K., Smith, T., Dutson, J.,Armknecht, J., Cameron, J., & Seamons, K.

(2019). A usability study of five two-factor authentication methods. In FifteenthSymposium on Usable Privacy and Security {SOUPS} 2019). https://www.usenix.org/system/files/soups2019-reese.pdf

[23] Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019). Evaluating user perception of multi-factor authentication: a systematic review. arXiv preprint arXiv:1908.05901. https://arxiv.org/ftp/arxiv/papers/1908/1908.05901.pdf

[24] Sabhanayagam, T., Venkatesan, V. P., & Senthamaraikannan, K. (2018). Acomprehensive survey on various biometric systems. International Journal of Applied Engineering Research, 13(5), 2276-2297. http://www.ripublication.com/ijaer18/ijaerv13n5_28.pdf

[25] Spolaor, R., Li, Q., Monaro, M., Conti, M., Gamberini, L., & Sartori, G. (2016). Biometric Authentication Methods on Smartphones: A Survey. *PsychNology Journal, 14,* 87–98. http://www.psychnology.org/File/PNJ14(2-3)/PSYCHNOLOGY_JOURNAL_14_2_3_SPOLAOR.pdf

[26] Wu, L., Yang, J., Zhou, M., Chen, Y., & Wang, Q. (2020). LVID: A Multimodal Biometrics Authentication System on Smartphones. *IEEE Transactions on Information Forensics and Security*, *15*, 1572–1585. https://doi.org/10.1109/tifs.2019.2944058

[27] Laghari, A., Waheed-ur-Rehman, & Memon, Z. A. (2016). Biometric authentication technique using smartphonesensor. *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*. https://doi.org/10.1109/ibcast.2016.7429906

[28] Bhartiya, N., Jangid, N., & Jannu, S. (2018, April). Biometric authentication systems: security concerns and solutions. In 2018 3rd international conference for convergence in technology (I2CT) (pp. 1- 6). IEEE.https://scihub.se/https://ieeexplore.ieee.org/abstract/ document/8529435

[29] Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decision Support Systems, 106, 1-14. https://scihub.se/https://www.sciencedirect.com/science/article/abs/pii/S0167923617302154