Facial Recognition Authentication Adds an Extra Layer of Security to Mobile Banking Systems

Dr. Kamalakannan Machap
School of Technology
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
dr.kamalakannan@apu.edu.my

Marco
School of Technology
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
tp056778@email.apu.edu.my

***Abstract*— Due to the COVID-19 pandemic, mobile banking usage has increased significantly over the last two years. People all over the world prefer mobile banking to other banking options such as ATMs and internet banking. With more concurrent mobile banking users, hackers and cyber criminals are more likely to target mobile users. As a result, the researcher decided to conduct a study on the current mobile banking system, with the goal of developing a secure mobile banking system that uses face recognition. The research concentrated on the security of existing mobile banking applications. The researcher conducted literature reviews and comparisons of existing mobile banking applications to gain additional knowledge for a deeper understanding of the topic. The developer also researched the methodologies and technical components required for this project. After tallying the data, it was discovered that more than half of the participants stated that their current mobile banking application does not support biometrics authentication. In addition, some of the participants added that mobile banking fraud still exists and some of them have experienced it or at least know about others who were victim to such criminal act in this paper, research will be conducted on the nature of mobile banking systems provided by several well-known banks or financial institutions in terms of its security. Comparative study will also be done between the implementation of OTP as the current last-step verification and Facial Recognition as a proposed last-step verification. Finally, a proposed method on why facial recognition is better than OTP and how it should be integrated to a mobile banking system to create an in-depth layer of security will be unraveled**.

Keywords—Network security, mobile banking, payment card industry data security standard, MiTM, Face recognition, bio-metric security.

I. INTRODUCTION

Diving into the Industrial Revolution 4.0 era, Mobile Banking has been considered one of the most used inventions. Due to this discovery, bank services have been accessible anywhere and anytime with just the help of smartphones – an essential necessity in this digital era. Bank customers will no longer have to physically find an ATM (Automated Teller Machine) to access the bank services.

The bank services that can be completed via Mobile Banking are none other than Fund Transfer, Online Purchase, and Balance Checking. With Mobile Banking, completing an online payment or peer-to-peer fund transfer is just few clicks away on a smartphone.

Due to the COVID-19 pandemic, people prefer to avoid any unnecessary contact whenever possible. Consequently, the usage of Mobile Banking during the pandemic has increased significantly. In Malaysia itself, the Mobile Banking transaction volume between the year 2019 and September 2021 has increased 121% from 489.8 million transactions to 1.08 billion transactions according to Bank Negara Malaysia. This rapid surge of volume in Mobile Banking is seen due to the efficiency it has brought upon financial institutions services. Although the convenience it has provided is seamless, the types of security measure that is implemented in it is vulnerable to cyber-attacks out there.

Most Mobile Banking systems that are currently used implements passcode and OTP as their user verification and authentication method. The types of authentications are similar in a sense that both requires user input. Compared to the old-school or conventional passcode authentication (including OTP – One-Time Password), biometrics is way safer and more secure (Sane, 2021). Not only that it does not require for user to key in his or her PIN code, but the input for biometrics is also a specific trait of the human body that is unique in every human being, such as fingerprints, face, iris, etc. However, passcode authentication is ultimately required to be implemented as a security measure regardless of its flaws. As a matter of fact, every authentication method has both upsides and downsides. Therefore, combining multiple authentication methods that can complement each other's is advised instead of erasing them. To further enhance the security level within a Mobile Banking system, biometrics, especially facial recognition can be one of the authentication methods to be combined along with passcode authentication in replacement of OTP. As the name speaks for itself, facial recognition is a face-based human identification method where it recognizes human face by matching the captured face with a database of known faces (Symanovich, 2021).

This type of computer vision invention has been used in daily basis, for example in immigrations, Apple's Face ID to unlock the gadget, and even APU's temperature checking system. From a security perspective, facial recognition can act as a last-step verification prior completing an action in the mobile banking system. With an additional layer of security is created in a sense where user needs both passcode and facial identification to complete an action.

II. Literature Review and Research

The essential data, facts, and previous research undertaken to investigate and support the topic must be supplied as part of the evaluation of the chosen topic. The literature on security mechanism in mobile banking focuses on why facial recognition authentication has to be implemented in mobile banking system and how it complements the current security mechanism. To improve the limitation from prior research, all the mandatory information is collected and examined. Sources of research will be from academic publications, conference proceedings, journals, and books. As a result, the developer will be able to generate fresh solutions to the challenges and gain insights when problems or issues are encountered during the development process. Great understandings and comprehension of the project will give huge contribution to the success of the project. Therefore, in this chapter, domain research and similar systems that have already been developed and used by people all over the world will be discussed with a summary given in the later part of this chapter.

A. Mobile Banking System

In this era where industrial revolution 4.0 and COVID-19 pandemic that is happening simultaneously, the process of digitalization is accelerated as most tasks, including day-to-day activities, and business operations such as banking services, have adapted to the existence of technologies. Digitalization has driven banks to undergo the most extensive transformation in their history as clients are progressively shifting online and becoming more mobile. The presence of mobile technology is critical to the success of businesses as an innovative and competitive marketing tool for providing services and online transaction opportunities. the invention of mobile banking has helped businesses and even individuals by providing a more effective and cost-beneficial solution towards banking transactions compared to the 'traditional' way of completing banking transactions where consumers are required to go to any of the bank branches or ATM.

The convenience that is offered by mobile banking is second to none compared to other banking instruments. Due to its cost-effectiveness and accessibility, banking institutions also promote their m-banking services to encourage their customers to adopt the m-banking services. Even banking institutions prefer using mobile banking as it can reduce the company's operational and infrastructural cost at the same time (Shankar et al., 2021). Moreover, looking at the current situation, COVID-19 outbreak has spread fear in people's mind to use liquid cash and forced people to adopt mobile banking services. The mentioned advantages of mobile banking and being in a situation where 'contactless' is greatly valued and practiced, the rise of usage volume in mobile banking is inevitable. In accordance, the security feature of mobile banking has to be considered and elevated to another level to comply with the huge volume of usage.

In an investigation report of mobile banking's strategy in its features and security, stated that the PCI-DSS (Payment Card Industry-Data Security Standard) obliges any institutions or corporates that offers credit cards payment to pay attention to the security controls, otherwise they can be given penalties. Moreover, implementation of general security mechanism in mobile banking, such as encryptions, passcodes, security questions, and downloaded applications are not as robust because incidents concerning security breach still happens and consequently spreads fear to customers (Hayikader et al., 2021).

As a matter of fact, not all mobile banking applications have implemented two-factor authentication – authentication mechanism that require at least two 'factor' or different types of input, it may be what you know (passcode or PIN), In research those sensitive transactions conducted via mobile banking applications requires a more secure authentication method than just static passcode. Thus, unauthorized users could easily obtain access to sensitive information and might misuse mobile banking services if two-factor authentication is not implemented (Shuhidan et al., 2021).

In their research paper stated (Bojjagani et al., 2021), titled 'Perceived Risk towards Mobile Banking: A case study of Malaysia Young Adulthood', that there are five types of risks of mobile banking. They are performance risk, security or privacy risk, time or convenience risk, social risk, and financial risk. Looking from a cyber security perspective, security or privacy risk refers to any potential loss of assets caused by any unwanted external threats (fraud or hackers) compromising a customer's mobile banking account. An example of fraud within mobile banking is via Phishing, where hackers steal customers' confidential data, including username, password, PIN, and credit card information by disguising as a trustworthy entity in an electronic communication (Bojjagani et al., 2021). Accordingly, an in-depth security and a strong defense mechanism is required to protect against external threats. Phishing attacks can be found in diverse of places, including the online payment industry, webmail, financial institutions, file hosting and cloud storage, so on and so forth (Yi et al., 2021).

B. Analysis of Cyber Attacks on Mobile Banking System

Currently, mobile devices have become the 'pot of gold' for cyber criminals and malicious users due to the rapid increase in its capabilities and usage *(*Bojjagani et al., 2021). Looking at the brighter side, nobody has to queue at a bank counter any longer to avail banking services because mobile banking has made it incredibly convenient (Tiwari et al., 2021). However, since smartphones are used as the medium to use mobile banking, cyber criminals saw this as an opportunity to trick bank customers to have their money without getting detected or traced, or in other words, conducting social engineering to bank customers (Datta et al., 2020).

Fig 1: User Credentials Seen in plist File

Thus, new attack techniques and vectors are also developed to comply with the advancement of technologies and also to take advantage of any discovered vulnerabilities within the mobile banking applications.

A Threat Model for Vulnerability Assessment and Penetration Testing of Android and iOS Mobile Banking

Apps', (Bojjagani et al., 2021), it was found out that several m-Banking applications are still employing a simple HTTP protocol to send user data without regard for security requirements. As a result of their penetration testing attempt, it was found out that most m-Banking applications were receiving self-signed or fake certificates. Since those certificates were blindly considered as sound and valid by the banks, chances of the banks being attacked via SSL/TLS Man-in-the-Middle attacks will be there.

IOS mobile banking applications where local data in the form of Core Data, XML and plist, NSUserDefaults class, Keychain Data, Log Files, and SQLite files were analyzed, it was discovered that user's credentials are stored in a plain text in plist files. The plist files, which are commonly used to store integers, floats, and strings, also stores user's credentials. Besides the plist file, SQLite databases and NSUserDefaults also stores information regarding user's credential. However, the information stored in SQLite database is usually encrypted (Bojjagani et al., 2021). On the other hand, information stored in NSUserDefaults is in a plain-text form.

On the other side of the coin also conducted a dynamic analysis of both Android and iOS mobile banking applications. In their analysis, it is discovered that adversaries can intercept user's OTP. An OTP is sent to the user's registered phone number to authenticate the user at the server side (Bojjagani et al., 2021). OTP can be seen in a plain-text format which can lead to another cyberattack, such as session hijacking. This emphasizes that MitM is possible to be performed on mobile banking applications.

```
POST/D3-BANK_3/servelt/NativeServlet01?ts=164672 HTTP/1.1
Content-Length: 164
Content-Type: application/x-www-form-urlencoded
Host: D3-BANK_3
Connection: close
Expect: 100-continue
Cookie: JSESSIONID=E6FB22137117580EED05A723C558ED45; LS
NONCEID=41e7a68b7e999af42f274724e9e2d343e28a0fb8dbdb1fe13fbf0a5868178872
Cookie2: $Version=1
BUILD_VERSION=14& USER_ID=215075231
&MOBILE_PIN=&FRM_OS=ANDROID&MOBILE_NUMBER=&METHOD_NAME=validateOTP&IMEI_NUM
BER=353327052273281&UNO=04785781714214074375&OTP=184176
```

Fig 2: OTP Intercepted in a Plain text

Basic security features such as encryption and the implementation of HTTPS as a secure connectivity between end device and server is sometimes absent in mobile banking applications due to the insufficient knowledge on the security aspect of a mobile application. Burp Proxy of Burp Suite is used to attempt MitM attack to the target. Based on the attack result, among the 19 India's Android mobile banking applications, Man-in-the-Middle attack can be launched with ease on 90% of the mobile banking applications even with HTTPS implemented within the system. Despite having HTTPS, OTPs can also be intercepted and decrypted by hackers which can result in another associated attacks to MitM, such as Denial of Service (DoS), Session Prediction, and Account Lockout Attack. This emphasizes that even a system with an advanced security defense implemented, it is still possible for hackers to successfully launch their attacks, let alone those with minimum security features.

Apart from MitM attacks, Keylogging can also threaten mobile banking users. Hackers are able to view user's ID and password that was keyed in during the login process. This information is usually stored in the key.log file that is automatically generated whenever keyboard strokes inputs are read (Tiwari et al., 2021). However, the keylogger file must be downloaded beforehand. The user input is recorded letter by letter and finally potential credentials are shown. Combined with another cyberattack, such as session hijacking and MitM attacks, hackers will be able to steal user's money as the credentials are already captured and it is also possible for them to capture the OTP sent by the server by using the Burp Proxy (Bojjagani et al., 2021).

C. Concept of Face Recognition

The human face is regarded as the most important feature of the body. According to studies, even a face can communicate and has different words for different emotions. Humans use vision to adapt and understand the environments in which they live, whereas computer vision works to duplicate human vision but in an electronic format to perceive and interpret an image (Teoh et al., 2021). The computer vision does not only operate as an eye to view, but it also must react. It must be capable of detecting, identifying, and processing pictures in the same way as human vision does it. Since the world is in three-dimensional but visual sensors typically provide two-dimensional images, it is more challenging for a computer to assess an object in three dimensions (Teoh et al., 2021).

Nonetheless, face recognition can be used as a key for security solutions in many businesses because it conveys people's identities. The facial recognition system is becoming increasingly popular around the world as a highly secure and dependable security tool. Because of its high level of security and reliability, it is acquiring major importance and attention from hundreds of corporate and government entities (Salama et al., 2021).

9911	23.24.20	>net.myinfosys.muamalat.activity>adampray690
9912	23.24.20	>net.myinfosys.muamalat.activity>adampray6902
9913	23.24.24	>net.myinfosys.muamalat.activity>P
9914	23.24.24	>net.myinfosys.muamalat.activity>Pa
9915	23.24.25	>net.myinfosys.muamalat.activity>Pas
9916	23.24.25	>net.myinfosys.muamalat.activity>Pasc
9917	23.24.25	>net.myinfosys.muamalat.activity>Pasca
9918	23.24.25	>net.myinfosys.muamalat.activity>Pascas
9919	23.24.26	>net.myinfosys.muamalat.activity>Pascasa
9920	23.24.26	>net.myinfosys.muamalat.activity>Pascasar
9921	23.24.26	>net.myinfosys.muamalat.activity>Pascasarj
9922	23.24.26	>net.myinfosys.muamalat.activity>Pascasarja
9923	23.24.27	>net.myinfosys.muamalat.activity>Pascasarjan
9924	23.24.27	>net.myinfosys.muamalat.activity>Pascasarjan4
9925	23.24.35	>net.myinfosys.muamalat.activity>0
9926	23.24.35	>net.myinfosys.muamalat.activity>15/12/2016
9927	23.24.35	>net.myinfosys.muamalat.activity>1
9928	23.24.36	>net.myinfosys.muamalat.activity>15/12/2016

Fig 3: Digital Evidence of User ID and Password by Keylogging

The application of facial recognition in mobile banking can improve the security on the current existing system and also help the society to go 'cash-less'. In order for people to believe in the possibility of going cashless, a system with a strong and in-depth security is compulsory so that users will feel safe which in result, will then discourage the use of cash (Adesuyi et al., 2021).

In recent research on the security issues of electronic and mobile banking, it is said that biometrics-based security mechanism can further improve the functionality and efficiency to mobile banking as it is nearly impossible to bypass the authentication. The reason is because biometric features (fingerprints, facial image, palm vein, iris, etc.) are more difficult to obtain compared to passcode (Wodo et al., 2021).

However, regardless of its secure mechanism, an individual's biometric traits can still be captured by hackers, especially faces. Most of the times, people tend to post their pictures on social media, which then will be used by hackers to bypass the face recognition authentication in any of the victim's gadget or account.

III. IMPLEMENTATION OF METHODS

System development methodologies are defined as a procedure of improving software development process' management and control, structuring and disentangling the process, and standardizing the development approach and product by defining actions to be performed and techniques to be applied (Saravanan et al., 2021).

The employment of a system development methodology is frequently thought to improve system development productivity and quality. In this section, there are two main system development methodologies that will be discussed and compared, which is the Waterfall Methodology and Rapid Application Development (RAD) Methodology. The merits and disadvantages of each methodology will be discussed and analyzed. Then, the most suitable methodology will be selected as this project's development methodology.

In the Requirements Planning and Analysis phase of the RAD model that is chosen for this project, minimum requirements of the final year project are necessary to be studied. In addition, a thorough research is required to be conducted for the developer to gain insights and the sufficient knowledge to develop the system. Assistance and guidance from supervisor and experts are required for the developer to create a fully functional system.

Online survey is also necessary to provide the developer with data to support the idea of the project. After all requirements are analyzed, it will be easy for the developer to set the goal and checkpoints of the project. the User Design phase, the developer will firstly design the interface, and continued by the functionalities of the secure mobile banking system. The prototype will be given to the supervisor for checking and if changes are required to be made, a new prototype will be created based on the feedback given by the supervisor. This phase will be repeated until the developer and supervisor are satisfied with the prototype. Once the created prototype has fulfilled the requirements and expectations, the developer can proceed to the next phase.

In the construction phase, the developer will create a more refined and cleaner version of the final prototype. In this phase, final testing is conducted before the project is finally released and submitted. Any minor defects, errors, or bugs can be fixed immediately by the developer. As major defects or issues are addressed in the prototyping or user design phase, the developer will be able to progress into the next phase to finally deploy the product. Once the developed system is deployed, the developer must make sure that it functions well and always update the system whenever required or when future enhancements happen.

In the maintenance phase, future bugs or errors that are encountered should immediately be patched by the developer before to ensure user's satisfaction and security of the system.

IV CONCLUSION AND REFLECTIONS

Overall, in the first leg of the research, the developer can complete the work to fulfilment the requirement. In depth research was conducted by the developer to gain knowledge and insights related to the topic. Starting from reading online journals, academic report, and several websites to conducting survey, the developer has gathered necessary information and data regarding people's comprehension on current mobile banking system. The developer is able to identify the drawbacks of current mobile banking system that is used by people and will take that as a reference to create a better and more secure system. Moreover, the developer has also done thorough reading and watched enough videos to decide the technical components to be used in developing the project, including the methodology, programming language, IDE, libraries, and tools to help achieve the project goal. However, the developer has yet to decide on the specific plugin that will be used later to develop the system.

REFERENCES

Adesuyi, F. A., Oluwafemi, O., Oludare, A. I., & Rick, A. V. (2013). Secure authentication for mobile banking using facial recognition.

Bojjagani, S., & Sastry, V. N. (2017, October). VAPTAi: a threat model for vulnerability assessment and penetration testing of android and iOS mobile banking apps. In 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC) (pp. 77-86). IEEE.

Hayikader, S., Hadi, F. N., & Ibrahim, J. (2016). Issues and security measures of mobile banking Apps. International Journal of Scientific and Research Publications, 6(1), 36-41.

Kuncoro, A. P., & Kusuma, B. A. (2018, November). Keylogger is a hacking technique that allows threatening information on mobile banking user. In 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE) (pp. 141-145). IEEE.

Lee, H., Zhang, Y., & Chen, K. L. (2013). An investigation of features and security in mobile banking strategy. Journal of International Technology and Information Management, 22(4), 2.

Salama AbdELminaam, D., Almansori, A. M., Taha, M., & Badr, E. (2020). A deep facial recognition system using computational intelligent algorithms. Plos one, 15(12), e0242269.

Saravanan, K., Floyd, R. W., Mcllroy, D., Morris, C., Boehm, B., Methodo, C., & North, D. (2017). Systems development methodologies: Conceptual study. Indian Journal of Scientific Research, 14(1), 27-37.

Shankar, A., & Rishi, B. (2020). Convenience matter in mobile banking adoption intention?. Australasian Marketing Journal (AMJ), 28(4), 273-285.

Shuhidan, S. M., Hamidi, S. R., & Saleh, I. S. (2017, August). Perceived risk towards mobile banking: A case study of Malaysia young adulthood. In IOP Conference Series: Materials Science and Engineering (Vol. 226, No. 1, p. 012115). IOP Publishing.

Symanovich, S. *What is facial recognition? How facial recognition works*. November 20, 2021.

Teoh, K. H., Ismail, R. C., Naziri, S. Z. M., Hussin, R., Isa, M. N. M., & Basir, M. S. S. M. (2021, February). Face recognition and identification using deep learning approach. In Journal of Physics: Conference Series (Vol. 1755, No. 1, p. 012006). IOP Publishing.

Tiwari, E., Sardar, P., & Jain, S. (2020). 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO).

Wodo, W., Stygar, D., & Blaskiewicz, P. (2021). Security Issues of Electronic and Mobile Banking. In SECRYPT (pp. 631-638).

Yi, C. X., & Kamsin, D. I. F. B. (2022) Research of Detection and Prevention of Phishing and Proposal of Phishing Detector Solution. Journal of Applied Technology and Innovation, 6(3), 1–5.