Implementation of One-Time Password in Online Banking System Among Malaysian Bank Users to Reduce Cyber Fraud

Poh Xin Yi[1], Intan Farahama Binti Kamsin[2], Salmiah Amin[3], Nur Khairunnisha Zainal[4]
[1'2'3'4]Asia Pacific University of Technology & Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.
[1]xypoh123@gmail.com, [2]intan.farahana@staffemail.apu.edu.my, [3]salmiah@staffemail.apu.edu.my, [4]khairunnisha.zainal@staffemail.apu.edu.my

Abstract - Security is a critical concern for online banking applications, and it may be accomplished via a variety of Internet technologies. This study suggests an application with increased security and efficiency to fight the fear of being scammed to reduce the threat of phishing and validate the user's identity. To increase security, one-time passwords (OTP) are used to circumvent the flaws of standard password-based systems. The report application employs basic random sampling and attempts to create stronger technology to improve the online banking system and give a platform for Malaysian banks and bank customers to build partnerships. A set of questionnaires is used to obtain raw data from a random sample of 200 Malaysian bank users from various backgrounds to examine their preferences and opinions on the use of the e-payment application. The community has benefited from the adoption of a new comprehensive application.

Index Terms - One-Time Password (OTP), Online Banking System, Scam Risk, Two Factor Authentication.

1. Introduction

Online banking systems have grown in popularity during the previous 10 years. It is an online payment system that allows various clients to execute financial transactions on a website. Users of an online bank may manage their accounts using their own electronic devices such as smartphones, computers, and so on, if they have an Internet connection. Online banking is also known as e-banking, virtual banking, Internet banking, and a variety of other titles [15].

Multi-factor authentication is a digital device access influence approach that a user may effectively be pass-through by displaying different authentication stages. Rather than only asking for specific pieces of information like passwords, users are asked to submit a variety of additional information, which makes it more difficult for any intruder to impersonate the genuine user [6]. OTP adds an additional layer of authentication to username and password. It is expected to continue to dominate in the next few years because of the ease of use, speed of deployment, cost-effectiveness, security, and privacy protection. To that end, SMS-based One Time Password (OTP) remains one of the most widely used multi-factor authentication and authorization mechanisms, with applications ranging from online banking to email services, social networks, financial institution transactions, online marketplaces, and online academic information applications [14]. SMS-based OTP is a way of transmitting a plaintext code known as OTP through SMS that is only valid for one session or transaction and is set to expire at a specific time. This technique significantly decreased the hazards of unauthorized access [14].

The purpose of this research is to discuss the security of the Mobile Banking and Payment Systems using SMS-based One-Time Password (OTP). This work is divided into 13 sections which are abstract, index term, introduction, literature review, problem statement, research aims, research objectives, research questions, research significance, research methodology, an overview of the proposed system, conclusion, and references.

2. Literature Review

2.1 Literature Review Matrix

Table 1.0: Literature Review Matrix

Domain	Article	Author	Year
One-Time Password	One-time Password: A Survey	Aravindhan Kurunthachalam & R.R Karthiga	2013
	An Improved Time-Based One Time Password Authentication Framework for Electronic Payments	Hassan, Md & Shukur, Zarina & Hasan, Mohammad	2020
	OTPaaS—One Time Password as a Service	Emir Erdem & Mehmet Tahir Sadikkaya	2019
	A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose?	Lumburovska & L., Dobreva, J. & Andonov, S., etc	2021

Online Banking System	e-Banking Adoption: An Opportunity for Customer Value Co-creation	Carranza, R. & Díaz, E. & Sánchez-Camacho, C. & Martín-Consuegra, D.	2021
	Analyzing the factors influencing adoption intention of internet banking: Applying DEMATEL-ANP-SEM approach.	Lin, W.-R. & Wang, Y.-H., & Hung, Y.-M.	2020
	Journal of Internet Banking and Commerce Research Trends in the Diffusion of Internet Banking in Developing Countries.	Muki, H	2014
Cyber Fraud and its impacts	Predicting susceptibility to cyber-fraud victimhood	Monica T.Whitty	2019
	A Qualitative Research on the Impact and Challenges of Cybercrimes	V Krishna Viraja & Pradnya Purandare	2021
	Top Five Cyber Frauds	Kumar Goutam, R., & Kumar Verma, D	2015
	Cyber fraud and crime	Charalampos Kyingopoulos	2019

2.2 Research Domain

2.2.1 One-Time Password

One-time password is a method of logging into a network or service that uses a unique password that can only be used once. It prevents many sorts of identity theft by ensuring that a login or password combination cannot be used again [2]. The most significant downside of one-time password solutions is that they are less subject to replay attacks, phishing attacks, and other attacks on basic conventional passwords than static passwords. This implies that if a prospective intruder successfully logs an OTP that has already been used to log in to a service or execute a transaction, he will be unable to exploit it since it will no longer be valid (Aravindhan Kurunthachalam & R R Karthiga, 2013). Transferring the same password over the network each time a user authenticates makes it easy to eavesdrop on the network. People devised one-time passwords to address these issues. Other benefits include anonymity, portability and extensibility, and the ability to avoid information leaks, among others [2]. There are two types of One-Time Password (OTP) which are HMAC-based One-time Password (HOTP) and Time-based One-time Password (TOTP). HMAC-based One-Time Password is an acronym that stands for Hash-based Message Authentication Code (HMAC). The HOTP is an event-based OTP with a counter as the moving component in each code [10]. The movement factor is increased based on a counter each time the HOTP is requested and verified. The generated code is valid until the user requests another one and is validated by the authentication server. When the code is verified and the user receives access, the OTP generator and the server are synchronized [10]. Another of the primary criteria for a one-time password is Time-based One-Time Password (TOTP) [6]. In TOTP, the token generates a numeric code, which is generally six or eight digits long. TOTP makes use of incremental time, often known as a timely action, which is commonly 30 or 60 seconds. This indicates that during important time activities, each OTP is lawful. TOTP is regarded as a more secure one-time password solution [6].

2.2.2 Online Banking

Internet banking is a financial service that has been developed over time by bank operators [9]. It is an electronic payment system that is also known as internet banking, e-banking, or virtual banking [3]. It offers real-time, quick, and convenient services. Consumers may use several banking services after registering for their own set of accounts and passwords, including online money transfers, bill payments, currency exchange services, account data inquiries, financial investments, and more. Consumers may avoid banks' business hours by using internet banking, which reduces the amount of time they must wait for counter services [9]. Consumers can clearly perceive the difference nowadays when comparing the quality and substance of services supplied by bank websites. The fast rise of online banking has the potential to provide significant benefits to banking operators when compared to traditional brick-and-mortar bank branches, as well as a fierce horizontal rivalry. It is critical for bank operators to grasp the experts' Internet banking business plans as well as the foundation for consumers' use of Internet banking [9].

This method of service delivery is a subset of electronic banking (EB). This comprises all types of electronic banking channels, such as ATMs, IB, mobile banking (MB), credit and debit card transactions, and so on [11]. Customers can perform banking transactions through the Internet at any time and from any location if they have an Internet connection. The introduction of these new distribution channels has not only enabled the adoption of multichannel strategies by existing institutions but has also resulted in the emergence of new financial services such as "virtual banking" [11]. Both financial firms and clients have benefited from IB. For example, bank customers may do their personal and business banking operations quickly, effectively, and easily by utilizing the bank's online banking website without leaving the comfort of their home or workplace, saving them the

expense and time of driving to a bank branch to execute the needed transactions. This also allows banks to duplicate the same services historically supplied in bank branches to their online consumers at a cheaper operational cost [11].

2.2.3 Cyber Fraud and its impacts

In terms of criminal growth, cybercrime is the world's largest industry [17]. Cybercrime refers to any illegal behavior involving computers, internet-connected devices, or networks. Some cybercrimes entail physically causing harm to or disabling computers, while others involve the use of computers or networks to transmit malware, unlawful messages, pictures, or other information [17]. One example of cybercrime is cyber fraud. Cyber fraud (also known as internet fraud) is any sort of deception that involves the use of e-mail, instant messaging, or social networking sites to defraud the public of money. Even though crime is on the rise, it has given rise to innovative means of solving and even reducing issues. To be more specific, cyber fraud helps to improve Internet security by providing critical protections [4]. Furthermore, user networks have been established with the goal of keeping attackers away from their systems, allowing governments to respond more rapidly in times of crisis. Finally, a computer network security mechanism must be established to prevent hostile crackers and hackers from gaining access to the system [4].

There are five types of cybercrimes which are tax refund fraud, corporate account takeover, identity theft, theft of sensitive data, and theft of intellectual property [8]. First, tax refund fraud is a recently created technique of network crime that has appeared in recent years. Tax refund fraud begins with cybercriminals targeting persons who fail to submit tax forms and then attempting to gain legitimate personal information about that person, such as name, social security number, ID card, and so on. This information is available not just via email phishing and social networking sites, but also on the black market. Following that, the invader would advocate for the tax to be paid in a more appealing manner. Customers frequently donate their tax money to scammers in this manner. Tax refund fraud may also be accomplished using off-the-shelf software [8]. The second type of cybercrimes is corporate account takeover. Corporate account takeovers are highlighted as another sort of cybercrime in 2008. Financial fraudsters frequently utilize technological techniques to conduct financial fraud or move funds from legitimate accounts to their own. Few years ago, corporate accounts have hijacked by producing new ACH files, but the situation has altered and is now influenced by account information previously supplied to the bank. The organization's finances and reputation would suffer irreversible harm because of this. The entire cost of business account purchases, on the other hand, is impossible to measure, with the FBI alone estimating losses of around $100 million in 2011. It demonstrates how deadly these kinds of cybercrimes may be [8].

The third is a different type of cybercrime in which a person illegally uses someone else's identity for financial gain, called identity theft. Cybercriminals are quite skilled at impersonating civilians or celebrities in order to carry out their nefarious operations. Therefore, the offender harms both the person who gave the information on the individual and the other party who has utilized to swindle the incorrect party. The attacker can use the stolen personal and financial information to get access to the victim's bank account, start a new account, transfer bank balances, or make purchases, among other things. In 2012, around 12.6 million Americans are estimated to have committed identity fraud [8]. The fourth of the cybercrime is the theft of intellectual property. It is an invention of ideas, including creative and cultural works, slogans, formulae, algorithms, and so on. It has monetary worth and is suited for commercial application. If someone else exploits your intellectual property for profit without your knowledge or consent, that person is committing intellectual property theft. Patents for new discoveries or creations, copyrights for music, films, graphics, logos, and textual materials, and trademarks for branded items are commonly used to protect and preserve intellectual property rights from theft [8].

Finally, the type of cybercrimes is the theft of sensitive data. It contains a wide range of information, such as information about persons, political opinions, religious beliefs, social connections, and so on. A person has the full right to access and use his personal information and the right to know how others are doing the same. There is a distinction to be made between personal sensitive data and identity theft. Identity theft is the illegal acquisition of your identity or availability by others, as well as access to personally sensitive information about your past and conduct [8].

2.3 Similar System

2.3.1 Google Authenticator

Google Authenticator is a mobile application that uses the TOTP or HOTP algorithms outlined in the Request for Comments (RFC) [5]. It is a free security application that can help you safeguard your accounts against password theft. It's simple to set up and may be utilized in a procedure known as two-factor authentication (2FA), which is available on major sites such as Gmail, Facebook, Twitter, Instagram, and others [7].

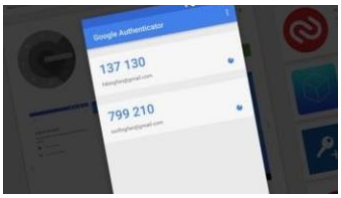

Figure 1.0: Overview of Google Authenticator
Source: https://www.pcmag.com/news/android-malware-can-steal-2fa-codes-from-google-authenticator-app

When you log into multiple services, the app, either iOS or Android, creates a random code that is used to authenticate your identity. Although the code may be provided to your phone through text message every time, the Google Authenticator application adds an extra layer of protection. The Google Authenticator software prevents SMS-based attacks by employing algorithms to create codes on your phone [7].

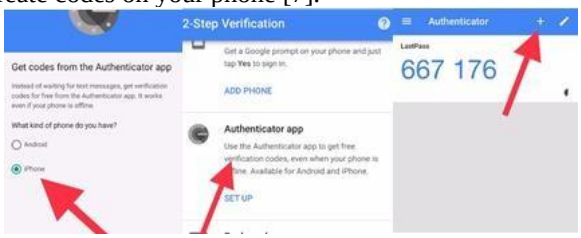

Figure 2.0: Set up the two-step verification & Select Device & Tap the button on top
Source: https://mashable.com/article/how-to-set-up-google-authenticator

First, the user can download a free Google Authenticator from either the Android Google Play Store or the Apple App Store. After completing the download, set up two-step verification on your Google account. According to the figure above, go through the “Security and Sign-In” section and choose the “Two-Step Verification” and click on the “Authenticator App” option [7]. Based on the figure 2, since the users select what kind of phone do, they have, it will restart the Google Authenticator App on your phone and press on the “+” button [7].

Figure 3.0: Scan Barcode & Manual Entry & Set up Authentication using Scan Barcode & Manual Entry
Source: https://mashable.com/article/how-to-set-up-google-authenticator

Next, according to figure 3, the system will ask the user to choose either “Scan Barcode” or “Manual Entry”. If the users select "Scan Barcode," they must first download a QR scanner from the app store. The QR code will then show on the computer screen, and users will need to validate a Google authenticator using their phone in order to log in to their account. This procedure takes a long time [7]. However, if the user selects the "Manual Entry" option, Google will merely send a 16-bit code to the user's email address. The code must then be entered to complete the validation procedure. Before finishing the application, make sure the time-based option is turned on to confirm that the code given by the user matches the freshly created password of the verifier [7].

Figure 4.0: Six-digit Verification Number
Source: https://mashable.com/article/how-to-set-up-google-authenticator

According to figure 4, when a user sign in to a Google authenticator-connected account, the account will now prompt the user to provide a six-digit verification number. Simply launch the Google Validator app, and it will produce a fresh random code for the user to input [7].

2.3.2 Twilio Authy

Twilio Authy is a multi-device 2FA application that can be used to secure any account, as long as that account supports 2FA via applications. Authy also provides a powerful API and app that assists the users in securing users and future-proofing their organizations [16]. It provides backup capabilities through its cloud and explains an extremely secure mechanism for handling it, with only a backup password being able to decrypt it. It has a user-friendly layout where the user can view the icons for each of the accounts that the user has set up.
In addition, Authy also has multiple authentication channels such as SMS/Voice/Email one-time password (OTP), API Soft Tokens (TOTP), Google Authenticator soft tokens, and Push Authentication.

Figure 5.0: Push Authentication
Source: https://mashable.com/article/how-to-set-up-google-authenticator

Push authentication improves user security while also improving the user experience. Push authentication is more powerful than passwords. It provides users with an unprecedented new experience right away, helping them to feel more confident while signing in [16].

Figure 6.0: Soft Tokens
Source: https://mashable.com/article/how-to-set-up-google-authenticator

Furthermore, soft tokens enable authentication everywhere, so it enables users to add a multi-functional experience. If customers are unable to receive SMS or push authentication on mobile or desktop due to being offline or having no data, they can still log in using a time-based one-time password (TOTP). A device-specific shared secret is used to generate the TOTP token. Unlike device-independent authentication methods like SMS and Voice, users can make risk decisions on a per-device basis [16].

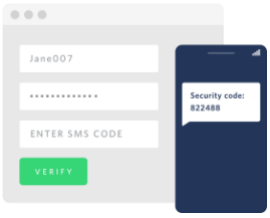

Figure 7.0: SMS, Voice, Email
Source: https://mashable.com/article/how-to-set-up-google-authenticator

SMS, phone, and E-mail are the most frequent ways of communication and authentication, allowing users to reach a huge audience with minimal effort [16]. Authy overcomes security issues that the common person does not notice. Authy is capable of easily resolving difficulties that appear to be complex. Passwords are insufficient to safeguard all of the data that consumers require. Authy works across all platforms and operating systems, authenticating logins with context data that bad actors cannot fabricate.

Table 2.0: Comparison of Google Authenticator and Twilio Authy

Characteristic	Google Authenticator	Twilio Authy
Operating System	Android, iOS, BlackBerry OS	Android, iOS, Mac, Windows, Linux, Apple Watch
Recovery Backup	No	Yes
Token safe	Less secure	More Secure (Backup Password, Master Password, and PIN Protection)
Multiple-device Support	No	Yes
Push Authentication	No	Yes

Table above clearly showed how Authy is more capable compared to Google Authenticator.

3. Problem Statement

In recent years, cybercrime is becoming more common, hazardous, and sophisticated every day. The global growth of the internet has raised concerns about the security of banking transactions. To trick internet users, phishers try to imitate the visual design of a webpage, and the false webpage contains identity keywords and hyperlinks that connect to the corresponding authentic webpage. The most popular scenario is when the users doing their e-banking payments, they will be required to enter the Password Authentication Code (PAC) by SMS [12] [13]. However, using SMS to get the PAC has some vulnerabilities. Many banks and companies rely on SMS as an additional layer of security for two-factor authentication (2FA). To help verify that a user is who they say they are, the company sends a text message with a single-use additional passcode. Then the user must enter the passcode that the company sent by SMS.

In this case, the phishers have learned how to use open-source software for writing code that interacts with SS7, to intercept SMS messages intended for others. Armed with an SMS verification code sent out by a bank and the target's username and password, a hacker could log into a victim's account to transfer money to themselves. In response to this problem, the researchers propose to implement a security application for the bank users so that when they are required to enter the SMS PAC, they can just go to the new security application and take the One-Time Password.

4. Research Aims and Objectives

The aim of this research project is to develop a more powerful technology to improve the online bank system. The research also identifies the security enhancements that would make an online bank system more secure.

5. Research Objectives

- To investigate the effect of brand credibility on consumer happiness in mobile banking.
- To investigate the effect of service quality on customer satisfaction in mobile banking.
- To investigate the influence of security on consumer happiness in mobile banking.

- To look at ways to safeguard bank customers from identity theft and provide reliable authentication.
- To consider how authentication will improve the online banking system and how it will assist banks in improving payment security.

6. Research Question

- Are the characteristics of mobile banking services influencing individuals to utilize them?
- Is people's distrust about mobile banking security keeping them from using the services?
- Does the bank's brand influence consumer satisfaction with mobile banking?
- What are the ways to safeguard bank customers from identity theft and provide reliable authentication?
- How will authentication improve the online banking system and how it will assist banks in improving payment security?

7. Research Significance

The purpose of this study is to look at the importance of having a more secure online banking system for all bank users. With the advancement of technology, the existing online banking system is experiencing several issues since many hackers are eyeing all the data of bank users. To avoid this, we must constantly improve the security of the online banking system. As a result, all stakeholders would gain from the establishment of a more safe and systematic online banking system for all banks. The benefit is that all bank users' data can be protected. In addition, with a more secure and systematic system, bank users may feel more confident while doing online transactions.

8. Methodology

8.1 Respondents

In this study, at least 200 bank users from different regions will be selected as the investigation objects through random sampling. According to Roscoe's Rules of Thumb, it is necessary to collect feedback from at least 100 respondents to reduce margin error to 10%, increase confidence to 85%-95%, and ensure a response rate of 50% [18].

8.2 Sampling

In this investigation, the researcher has uses simple random method. Simple random sampling is a random pick from a vast quantity of data after determining whether the selected data is available. The goal of the study is to figure out what elements are impacting the continuous theft of bank users' information. To understand and determine this factor, this study will need to consult data from other countries or regions. This sampling strategy helps researchers to swiftly locate information, saving both time and money.

8.3 Data Collection

There are two types of qualitative surveys which are paper surveys and online surveys. Respondents to paper surveys usually provide qualitative information. The survey consisted of a series of brief questions with an infinite number of participants. The questionnaire's goal is to collect standardized data. These questions are based on the interviewees' expressions in order to collect data. As a result, it may be used to gather information from a population or a bigger sample. An online survey is one that is done via the use of the software. The software can conduct an online survey by uploading it to a website or sending it to respondents via email. It can also share or send the data that needs to be surveyed. This is for the purpose of gathering reliable online data. Instead of penning the response on paper, the responder uses a computer and a keyboard to type in the concept you wish to communicate, then sends it again. Online surveys are more detailed, and respondents can respond at any time. Respondents simply need a phone, tablet, or other mobile devices to complete the online survey. This facilitates the collection of qualitative data from online questionnaires. This study primarily employs an online survey to collect data from others, further explore and comprehend the research questions, and indirectly comprehend the factors that influence bank user data theft.

9. Overview of the Proposed System

SecureKey is developed for the targeted users which are the banks and bank users. SecureKey will allow bank users to take the One-Time Password (OTP) when they are doing e-payment transactions. However, SecureKey will help the banks to make sure that there are no hackers are trying to phish. After the analysis of similar systems in 2.3, the proposed system references one of the more comprehensive systems, which is Twilio Authy.

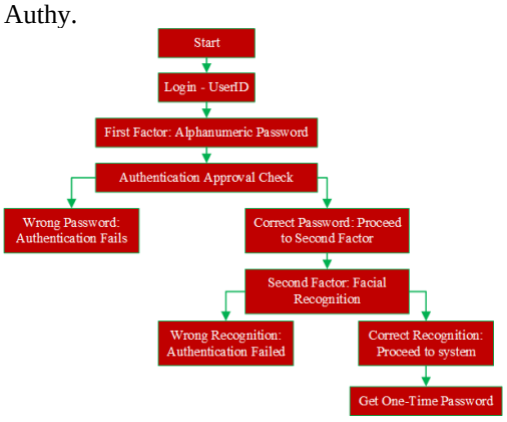

Figure 8.0: Overview of the Proposed System

This proposed system will be using Multi-Factor Authentication which is Three-Factor Authentication. Normally, when bank users sign into their accounts, they are required to enter their passwords. After signing in, they will get the One-Time Password (OTP) to secure their applications or accounts. However, SecureKey will require the user's all biometrics such as facial recognition, fingerprint, or voice recognition before the system proceeds with the One-Time Password (OTP). SecureKey is accessible for Android and iOS mobile devices, as well as Windows, Apple Watch, and even the user's PC. The users also may use SecureKey to secure themself from all devices at the same time. SecureKey enables users to access encrypted backups in the cloud. When a user loses a phone but is still able to access SecureKey accounts from other devices. Since the user has a new phone, all he or she needs to do is install the SecureKey app, authenticate his or her identity, and have access to all of his or her SecureKey tokens. Moreover, SecureKey also has a perfect UI on all platforms, and it is easy to use. The three authentications which are One-Time Password (OTP), Soft Token TOTP, and Push Authentication, are also available in the system.

10. Conclusion

Throughout the course of the investigation, the use of online banking has grown increasingly prevalent in the realm of online transactions. Although there are certain disadvantages to establishing an application, research indicates that developing an application for online transactions benefits all stakeholders, particularly each bank user. The primary goal of this strategy is to add additional new features to the existing system and improve the previously insufficient functionality. It is believed that with successful implementation, cyber fraud in Malaysia would improve and the success rate will be considerably reduced.

References

[1] Amin, H., & Ramayah, T. (2010). *SMS Banking: Explaining the Effects of Attitude, Social Norms and Perceived Security and Privacy*. https://www.researchgate.net/publication/228661739_SMS_Banking_Explaining_the_Effects_of_Attitude_Social_Norms_and_Perceived_Security_and_Privacy

[2] Aravindhan Kurunthachalam, & R R Karthiga. (2013, January). *(PDF) One-time Password: A Survey*. ResearchGate. https://www.researchgate.net/publication/344518837_One-time_Password_A_Survey

[3] Carranza, R., Díaz, E., Sánchez-Camacho, C., & Martín-Consuegra, D. (2021). e-Banking Adoption: An Opportunity for Customer Value Co-creation. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.621248

[4] Charalampos Kynigopoulos. (2019). *Cyber fraud and crime*. https://doi.org/10.13140/RG.2.2.11323.75040

[5] Emin Huseynov, & Jean-Marc Seigneur. (2017). *Google Authenticator - an overview | ScienceDirect Topics*. Www.sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/google-authenticator

[6] Hassan, M. A., Shukur, Z., & Kamrul, M. (2020). An Improved Time-Based One Time Password Authentication Framework for Electronic Payments. *International Journal of Advanced Computer Science and Applications*, *11*(11). https://doi.org/10.14569/ijacsa.2020.0111146

[7] Kaufman, M. (2017, October 29). *Google Authenticator will add a formidable layer of protection to your e-mail account*. Mashable. https://mashable.com/article/how-to-set-up-google-authenticator
Krishna Viraja, V., & Purandare, P. (2021). A Qualitative Research on the Impact and Challenges of Cybercrimes. *Journal of Physics: Conference Series*, *1964*(4), 042004. https://doi.org/10.1088/1742-6596/1964/4/042004

[8] Kumar Goutam, R., & Kumar Verma, D. (2015). Top Five Cyber Frauds. *International Journal of Computer Applications*, *119*(7). https://doi.org/10.5120/21080-3759

[9] Lin, W.-R., Wang, Y.-H., & Hung, Y.-M. (2020). Analyzing the factors influencing adoption intention of internet banking: Applying DEMATEL-ANP-SEM approach. *PLOS ONE*, *15*(2), e0227852. https://doi.org/10.1371/journal.pone.0227852

[10] Lumburovska, L., Dobreva, J., Andonov, S., Hristina Mihajloska Trpcheska, & Dimitrova, V. (2021). A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose? *Security & Future*, *5*(4), 131–136. https://stumejournals.com/journals/confsec/2021/4/131

[11] Muki, H. (2014). Journal of Internet Banking and Commerce Research Trends in the Diffusion of Internet Banking in Developing Countries. *Journal of Internet Banking and Commerce*, *19*(2). https://www.icommercecentral.com/open-access/research-trends-in-the-diffusion-of-internet-banking-in-developing-countries.pdf

[12] Osman, Z., Abdul, A.-A., & Phang, G. (2017). *PERCEIVED SECURITY TOWARDS E-BANKING SERVICES: AN EXAMINATION AMONG MALAYSIAN YOUNG CONSUMERS*. https://jurcon.ums.edu.my/ojums/index.php/JAAAB/article/view/1272/818

[13] Raharja, I. M. S., & Ashari, A. (2021). *Enhancing Security System of Short Message Service for Banking Transaction*. https://pdfs.semanticscholar.org/f3a3/50e05860b20a1f2283d2af7d09ed56d0af01.pdf

[14] Reyes, A. R. L., Festijo, E. D, & Medina, R. P. (2019). *Enhanced Multi-factor Out-of-Band Authentication En Route to Securing SMS-based OTP Ariel*. https://www.researchgate.net/profile/Ariel-Roy-Reyes/publication/331949136_Enhanced_Multi-factor_Out-of-Band_Authentication_En_Route_to_Securing_SMS-based_OTP/links/5c943e3c92851cf0ae8eb018/Enhanced-Multi-factor-Out-of-Band-Authentication-En-Route-to-Securing-SMS-based-OTP.pdf

[15] Samir Pakojwar, & Dr. N. J. Uke. (2014). *Security in Online Banking Services – A Comparative Study*. https://www.researchgate.net/profile/Nilesh-Uke/publication/280864086_Security_in_Online_Banking_Services_-_A_Comparative_Study/links/5dcbbd1a458515143506dc01/Security-in-Online-Banking-Services-A-Comparative-Study.pdf

[16] TWILIO INC. (n.d.). *Twilio Authy | SMS, Voice, Email, Push Authentication features*. Twilio. Retrieved February 8, 2022, from https://www.twilio.com/authy

[17] Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/jfc-10-2017-0095

[18] Wilson Van Voorhis, C. R., & Morgan, B. L. (2007). Understanding Power and Rules of Thumb for Determining Sample Sizes. *Tutorials in Quantitative Methods for Psychology*, *3*(2), 43–50. https://doi.org/10.20982/tqmp.03.2.p043