International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 713-722 www.ijaem.net ISSN: 2395-5252

Ensuring Trust and Confidence: Safeguarding Online Banking Transactions with Multi-layered Security in Malaysia

Heng Zhi Yong[1], Mohd Khairudin Bin Kasiran[2]
[1] *Awang Had Salleh Graduate School, School of Computing, Universiti Utara Malaysia, Kedah, Malaysia*
[2] *School of Computing, Universiti Utara Malaysia, Kedah, Malaysia.*

Date of Submission: 20-07-2023 Date of Acceptance: 31-07-2023

ABSTRACT: Online banking has revolutionized convenience in Malaysia, offering seamless access to financial services. Nevertheless, concerns about the security of online transactions have arisen. This study examines security layers implemented by selected Malaysian banks (RHB, BIMB, HLB, PPB, MBB, UOB) for online banking. Experiments were conducted on login credentials, password changes, transaction limits, fund transfers, and mobile prepaid reloads. Observations recorded user experiences, security measures, and vulnerabilities. Findings reveal diverse security measures, including security by application, one-time passwords (OTP), multi-factor authentication (MFA), and multi-layered approaches. These measures effectively enhance transaction security, thwarting unauthorized access and cyber threats. Areas for improvement include regular security updates, user education, collaboration, information sharing, and regulatory compliance. Addressing these areas will bolster online transaction security, fostering customer trust and confidence. In conclusion, securing online transactions is paramount to protect Malaysian bank customers from cyber risks. This study contributes insights into multi-layered online banking security, encouraging enhancements for a reliable and secure banking environment in Malaysia.

KEYWORDS: Online banking, Security layers, Malaysia, Multi-layered security, Trust, Confidence

I. INTRODUCTION

The growth of online banking in Malaysia has provided convenience and accessibility to customers, allowing them to perform financial transactions from the comfort of their homes or on the go. However, this convenience has also raised concerns about the security of online banking transactions. With the increasing prevalence of cyber threats and the potential risks associated with unauthorized access, Malaysian banks must ensuretrust and confidence among their customers by implementing robust security measures.

According to the National Risk Assessment 2020, fraud cases and losses in the nation were higher than they were when the previous evaluation was made in 2017. In 2021 alone, more than 20,000 cybercrimes were enrolled, resulting in damages of RM560 million. Malaysians lost roughly RM2.23 billion as a result of cybercrimes between 2017 and July 2021. As more people use their mobile devices for online transactions, mobile malware-related incidences of online banking fraud are also rising [1]. According to[2], Malaysia's Inspector-General of Police Tan Sri Acryl Sani Abdullah Sani reported 12,092 online fraud cases and losses of RM 415 million from January to July 2022. 33,147 suspects in cyber fraud cases were detained between January 2019 and July 2022, and 22,196 cases resulted in court charges.

This proposal aims to explore the topic of safeguarding online banking transactions with multi-layered security in Malaysia. The study will delve into the existing security measures employed by Malaysian banks and analyze their effectiveness. It will also focus on the concept of multi-layered security approaches, evaluating how these measures can be applied to enhance the security of online banking transactions in Malaysia.

II. LITERATURE REVIEW

i. Existing Security Measures

To protect online banking transactions, Malaysian banks have implemented various security measures. These measures encompass a range of techniques, including user authentication, encryption, secure protocols, transaction monitoring, and anti-fraud mechanisms. By comparing different security measures adopted by Malaysian banks, we can assess their effectiveness in mitigating risks and safeguarding online transactions. Furthermore, vulnerabilities and areas for improvement can be identified to strengthen the security layers.

Table 1. The existing security measures for online transaction in Malaysia

Author	Description
[3]	One-Time Password (OTP)
[4]	Secure by Application
[5]	Token

ii. Multi-layered Security Approaches

A multi-layered security approach involves the implementation of multiple security measures that collectively enhance the protection of online banking transactions. This section will explore the concept of multi-layered security and discuss how it can be applied to online banking transactions in Malaysia. By analyzing different layers of security, such as user authentication, encryption, secure protocols, transaction monitoring, and anti-fraud mechanisms, we can evaluate the effectiveness of these layers in fortifying the security of online banking transactions. According to [6], By offering multiple levels of security, multi-factor authentication (MFA) also known as strong authentication, authenticates users for transactions including making a payment, transferring funds, or logging into the system. In addition to two-factor authentication, which verifies users using a physical token such as a debit card or smart card and a security code, PIN, or password. Multi-factor authentication (MFA) uses a different authentication technique to confirm users. Biometric authentication methods include voice identification, iris recognition, and fingerprint or facial recognition are examples of additional authentication methods.

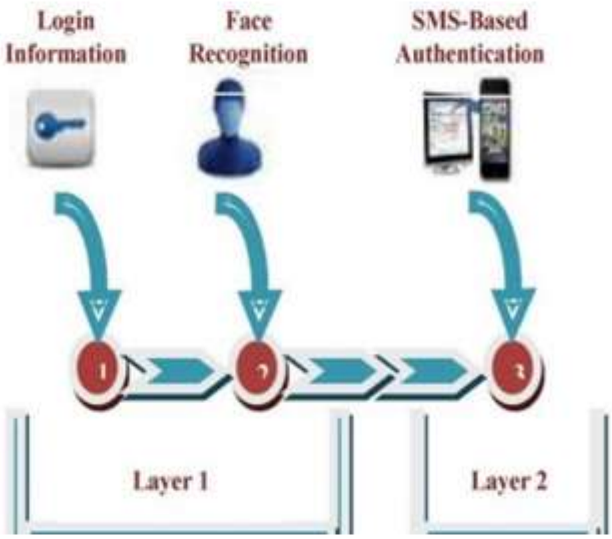


Figure 1: Adapting the facial recognition method for MFA[9]

\

Figure 1 depicts the MFA technique. First, users need to provide their username and password in Step 1. Next, the system will identify users' faces after they have entered those credentials and data in Step 2. In conclusion, after completing Layer 1, users will enter the OTP, Token, or PIN that they received in their token device or mobile phone or Step 3. Layer 1 claims there are two steps, however, Layer 2 claims there is only one step that Layer 1 must complete.

iii. Regulatory Framework

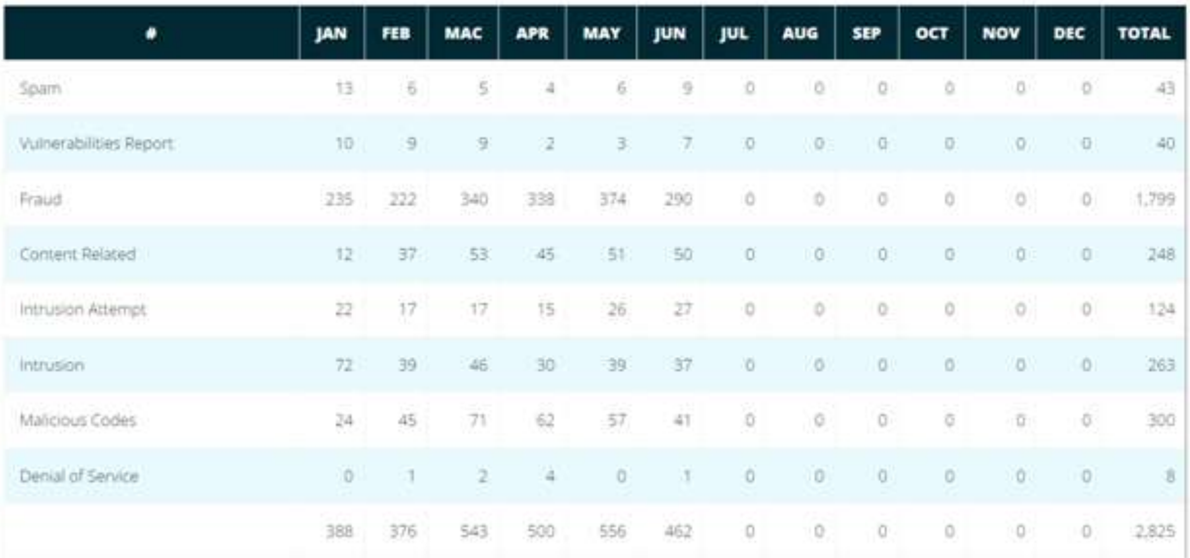
The regulatory framework plays a vital role in ensuring trust and confidence in online banking transactions. This section will compare the regulatory frameworks and guidelines related to online banking security in Malaysia. By evaluating the effectiveness of these regulations, we can assess their ability to minimize risks associated with online transactions and protect customers' interests. Additionally, we will discuss the impact of these regulations on customer trust and confidence in online banking.

According to[7], many organizations have adopted various IT governance frameworks, including COBIT (Control OBjectives for Information and Related Technology) and ISO/IEC standards like 27002, to manage IT resources and reduce risks associated with using IT as a result of the US Sarbanes-Oxley Act of 2002 and the steadily rising computer crime, such as virus attacks. Although these frameworks are beneficial and frequently used when organizations wish to execute the suggested best practices, the existence of different standards can be confusing. Furthermore, these frameworks are quite generic and are aimed attop-level management.

iv. Cybersecurity Threats

The landscape of cybersecurity threats is constantly evolving, and online banking transactions in Malaysia are not immune to these risks. This section will analyze the common cybersecurity threats faced by online banking transactions in Malaysia, including phishing attacks, malware, identity theft, and social engineering. By comparing and contrasting these threats, we can highlight the potential risks to online banking security. Furthermore, wewill explore how multi-layered security measures can effectively mitigate these threats, providing a comprehensive defense against cyber-attacks.

According to [8], The National Strategy for Financial Literacy 2019–2023 was put into place by the Malaysian government to improve financial literacy among Malaysians of all ages and stages of life as well as to encourage responsible financial behaviour and positive attitudes toward money management.



#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Spam	13	6	5	4	6	9	0	0	0	0	0	0	43
Vulnerabilities Report	10	9	9	2	3	7	0	0	0	0	0	0	40
Fraud	235	222	340	338	374	290	0	0	0	0	0	0	1,799
Content Related	12	37	53	45	51	50	0	0	0	0	0	0	248
Intrusion Attempt	22	17	17	15	26	27	0	0	0	0	0	0	124
Intrusion	72	39	46	30	39	37	0	0	0	0	0	0	263
Malicious Codes	24	45	71	62	57	41	0	0	0	0	0	0	300
Denial of Service	0	1	2	4	0	1	0	0	0	0	0	0	8
	388	376	543	500	556	462	0	0	0	0	0	0	2,825

Figure 2: Cybercrime Incidents In Malaysia Year 2023 [10]

III. METHODOLOGY

This study adopts an approach to gain access to a specific bank's online banking system and examine the security layers implemented for transactions.

Selection of the Bank

To conduct this study on safeguarding online banking transactions with multi-layered security in Malaysia, a selection of banks was made based on their popularity, customer base, and availability of online banking services. The chosen banks for this observation study include Rashid Hussein Bank (RHB), Bank Islam Malaysia (BIMB), Hong Leong Bank (HLB), Public Bank (PPB), Maybank (MBB), and United Overseas Bank (UOB).

The observation methodology involved conducting experiments with each of the selected banks' online banking functions. The following key functions were examined:

1. Login Credential

This section focused on the login process of each bank's online banking platform. The objective was to assess the effectiveness of the login credentials in preventing unauthorized access. The observations included the strength of password requirements, two-factor authentication implementation, and any additional security measures.

2. Change Password

This section involved the process of changing the account password. This was done to evaluate how easily users could update their passwords and assess the security measures in place to protect against unauthorized password changes.

3. Change the Transaction Limit

This section examined the procedure for changing the transaction limit. This step aimed to determine the level of control users have over their account's transaction limits and whether additional authentication measures are required for such changes.

4. Fund Transfer

This section focused on the fund transfer functionality within each bank's online banking platform. The objective was to observe the security measures implemented during the fund transfer process, including verification steps, recipient validation, and transaction confirmation.

5. Mobile Prepaid Reload

This section involved the process of reloading mobile prepaid credit through the online banking platform. This experiment aimed to evaluate the security measures in place for mobile prepaid transactions, including user authentication and secure payment processing.

Throughout the observation process, detailed notes were taken on the user experience, security measures encountered, and any issues or vulnerabilities identified. The observations were conducted by performing the aforementioned functions on each bank's online banking platform, following a standardized procedure for consistency.

By analyzing the observations from these experiments across multiple banks, we can assess the varying levels of security and identify best practices or areas for improvement in safeguarding online banking transactions. The findings from these observations will contribute to the overall understanding of multi-layered security in online banking and provide insights for enhancing trust and confidence among Malaysian.

IV. FINDING

i. Login Credentials

The login credentials for Banks A, B, C, D, E, and F consist of a unique combination of a username and a password. To initiate the login process, users are required to provide their respective usernames and click on the "LOGIN" or "NEXT" buttons, depending on the specific bank.

For Bank A, upon entering the username and clicking the "LOGIN" button, the user is prompted to enter the "Secure Word" previously set by them. If the entered Secure Word is incorrect, the process will be indicated by the "✕" button, and the user will be redirected to re-enter their username. Conversely, if the Secure Word is correct, the process will be indicated by the "✓" symbol, and the user will proceed to input their password and click the "LOGIN" button to access the bank's dashboard.

For Bank B, after inputting the username and clicking the "Next" button, the webpage displays the "security picture" set by the user. If the displayed "security picture" is incorrect, the user can click the "Back" button to retype the username. However, if the "security picture" is correct, the user must click "Yes, this is my security picture" to proceed and input their password. Afterward, they can click the "Login" button to access the bank's dashboard.

Bank C requests users to input their "USER ID" and click the "LOGIN" button. Upon doing so, the webpage displays the "Private Image" and "Private Word" previously set by the user. If either the "Private Image" or "Private Word" is incorrect, the user should click the "No" button, and the webpage will return to the "USER ID" login page. Conversely, if both the "Private Image" and "Private Word" are correct, the user needs to click the "Yes" button to proceed and input their password. Finally, they can click the "LOGIN" button to access their bank account dashboard.

For Bank D, the user must input their "User ID" and click the "Next" button. The webpage will then display the "Personal Login Phrase" set by the user. If the "Personal Login Phrase" is incorrect, the user should click the "No" button, and the webpage will return to the "User ID" login page. However, if the "Personal Login Phrase" is correct, the user should click the "Yes" button to proceed and input their password. Subsequently, they can click the "Login" button to access their bank account dashboard.

Bank E requires the user to input their "My Username" and click the "LOGIN" button. After clicking the "LOGIN" button, the webpage displays the "Security Phrase" set by the user. If the entered "Security Phrase" is incorrect, the user should click the "NOT ME" button and the webpage will return to the "My Username" login page. Conversely, if the "Security Phrase" is correct, the user should click the "Yes" button to proceed and input their password. Finally, they can click the "LOGIN" button to access their bank account dashboard.

Lastly, Bank F requests the user to input their "USERNAME" and click the "Submit" button. After clicking the "Submit" button, the webpage displays the "Security Word" set by the user. If the "Security Word" is incorrect, the user should click the "No" button, and the webpage will return to the "USERNAME" login page. However, if the "Security Word" is correct, the user should click the "Yes" button to proceed and input their password. Ultimately, they can click the "Login" button to access their bank account dashboard.

ii. Change Password

The password change process allows users to modify their login credentials. Some banks require users to provide their Current or Old Password, New Password, and Confirm New Password to initiate the password change procedure.

Firstly, for Bank A, users are prompted to input the New Password and Confirm New Password. The password must meet specific criteria, including a minimum length of 8 characters, with a combination of alphanumeric and special characters. After clicking the "Submit" button, the user's mobile phone will receive a notification from Bank A, giving them the option to ACCEPT or REJECT the password change. Upon selecting "ACCEPT," the password will be successfully changed. If the user chooses "REJECT," the password will remain the same.

Next, Bank B follows a step-by-step process for password change. Users are required to select their ID Type and input their ID Number, then click the "Next" button. Following this, a TAC (Transaction Authorization Code) is sent to the user's mobile phone, which they must input on the webpage and click the "Next" button. Subsequently, users need to input their Debit Card number and Debit Card PIN before proceeding to input the New Password and Confirm Password. The password must be unique and not reuse any previous passwords, with a length between 8 and 16 characters, and include a combination of uppercase and lowercase alphabets, as well as numbers. Finally, the password change process is completed successfully.

Bank C requests users to input their Current Password, New Password, and Confirm New Password. The password must consist of 8 to 18 characters, containing a combination of uppercase and lowercase alphanumeric characters and special characters. After clicking the "Change" button, the user will see the Change Details and must click the "Next" button to proceed. To confirm the password change, users need to launch the Bank C Application and choose between the "Confirm" or "Reject" buttons. Upon selecting "Confirm," users need to input the verification number displayed in the application, and the password change will be successful. If the user clicks the "Reject" button, the password change will be unsuccessful.

For Bank D, users are required to input their Old Password, New Password, Confirm New Password, and SecureSign Token. The password must be at least 8 characters and include at least one uppercase letter, one lowercase letter, one number, and one special character. To generate the SecureSign Token, users need to use the Token Device. They must start the token device and follow the steps to obtain the SecureSign token code, which they will then input in the SecureSign Token field and click the "Submit" button. After this, the password will be successfully changed.

Furthermore, Bank E requests users to input their Current Password, New Password, and Confirm New Password. The password must be between 8 and 12 characters and include at least one uppercase letter, one lowercase letter, one number, and one special character. It must not contain any spacing or sequences of 3 consecutive characters, such as "123" or "abc." Additionally, the password must not match the user ID or Security Phrase, and it cannot be the same as any of the user's previous 7 passwords. Upon clicking the "SAVE CHANGES" button, users will receive a TAC number on their mobile phones, which they must input to confirm the password change.

Lastly, for Bank F, users are required to input their Existing Password, New Password, and Confirm New Password. The password must be between 8 and 24 characters and consist of alphanumeric characters without spaces. After clicking the "Submit" button, the user's mobile phone will receive a notification from the Bank F application, prompting them to enter the secure PIN to complete the password change for login.

iii. Change the Transaction Limit

The change transaction limit process enables users to modify their daily transaction limits as per their requirements.

For Bank A, users are requested to select the daily limits for various transaction categories, such as DuitNow via Bank Account Number, DuitNow via Mobile/ID/Business Registration Number, Interbank GIRO, Other Account, Own Account, and FPX Payment. After choosing the desired limits for each category, users must click the "SAVE" button. Subsequently, a notification is sent to the user's mobile phone via the Bank A application, presenting the options to "APPROVE" or "REJECT" the changes. Selecting "REJECT" will maintain the existing limits, while choosing "APPROVE" will implement the user-defined changes.

For Bank B, users need to change their daily limits for transfers to third-party accounts, Interbank GIRO (IBG), Instant Transfer, and DuitNow to Account/Mobile/Other ID. To proceed with the limit change, users must download the Bank B application and log in to their accounts. Within the application, they can access the Account Settings & Limits section to input the desired daily limits and click the "Next" button to confirm the changes.

Bank C requires users to modify their daily limits for various transactions, such as Own Account Transfer, Third Party Transfer, Bills Payment, Bill Presentment, E-Sadaqah/Wakaf, JomPAY and Payment Gateway, Prepaid Reloads, FPX, and Quick Transfer Limit. Users can individually set the desired limits for each category and click the "Change" button. Upon doing so, the Change Limit Details will be displayed, and users must click the "Next" button. To confirm or reject the limit change, users must access the Bank C Application, enter the verification number displayed, and choose between "Confirm" or "Reject." Selecting "Confirm" will implement the limit changes, while choosing "Reject" will keep the current limits.

For Bank D, users can change their daily limits for Own Fund Transfer, Own Card Payment, Own Loan/Financing Payment, Third Party Fund Transfer, and Other Limit (Bill Payment, JomPAY, Prepaid Top-up, FPX). The limit change requires users to utilize a token device to obtain a SecureSign token code. After inputting the token code and clicking the "Submit" button, the changes to the selected limits will be successfully implemented.

Bank E allows users to change their daily limits for various transaction types, such as 3rd Party Transfer, Interbank Transfer (DuitNow, DuitNow-Transfer, and GIRO), Overseas Transfer, MIGA-i transfer, Bakong Transfer Limit, FPX, ASNB Own Account Transfer, ASNB 3rd Party Transfer, Tabung Haji Own Account Transfer, and Tabung Haji 3rd Party Transfer. Users can input their desired daily limits and click the "SAVE CHANGES" button. Afterward, a TAC number is sent to the user's mobile phone, which they must input to confirm the changes to the daily transfer limits.

Lastly, for Bank F, users can change their daily limits for Bill Payment & JomPAY, Mobile Prepaid Reload, E-Commerce/FPX, Telegraphic Transfer, DuitNow Online Banking or Wallets, and DuitNow QR. Users can select the limits they wish to change and click the "Save" button. After clicking the "Save" button, the webpage will display the transaction limits, and users must click the "Confirm" button. A notification is sent to the user's mobile phone via the Bank F application, prompting them to enter the secure PIN to confirm the changes to the daily limits.

iv. Fund Transfer

This section presents a comparison of fund transfer methods offered by six different banks in Malaysia, namely Bank A, Bank B, Bank C, Bank D, Bank E, and Bank F.

Bank A facilitates DuitNow transfers using various identifiers such as Bank Account Number, Mobile Number, NRIC Number, Army/Police Number, Passport Number, and Business Registration Number. For DuitNow via Bank Account Number, users need to select the transfer from, transfer to, payment type, recipient residential status, and input the recipient account number, the amount in MYR, recipient reference, and optional payment details. After providing the required information, users must click the "NEXT" button for payment review and then submit the transaction. A notification is sent to the user's mobile phone via the Bank A application, allowing them to either "ACCEPT" or "REJECT" the fund transfer. Accepting the transaction results in a successful transfer while rejecting it leaves the fund transfer unchanged.

Bank B enables users to transfer funds to others through methods such as Overseas Transfer, 3rd Party Account, DuitNow to Account/IBG, and DuitNow to Mobile/Other ID. For DuitNow to Account/IBG, users must choose the transfer from, recipient bank/wallet name, account type, transfer timing, and recipient reference. Additionally, they need to input the account number, the amount in MYR, and other payment details. After completing the input, users must click the "Next" button for transaction review and then input the OTP TAC sent via SMS by Bank B before submitting the transaction. Once submitted, users can download a PDF file for reference.

Bank C offers fund transfers to various recipients, including DuitNow ID/Account, DuitNow ID Maintenance, Third Party Account, Own Account, Payment (JomPAY), and Interbank GIRO (IBG). For Interbank GIRO (IBG) transfers, users are required to select the from the account, transfer type, transfer mode, recipient type, recipient bank, and recipient ID/IC checking. Additionally, they need to input the transfer amount, recipient account, recipient name, recipient reference, other payment details, and recipient email. Clicking the "Transfer" button displays the transfer and recipient details, followed by launching the Bank C Application for "Confirm" or "Reject" actions. Confirming the transfer involves inputting the verification number from the application, leading to a successful fund transfer, while rejecting it results in an unsuccessful transfer.

Bank D provides options for fund transfers, including DuitNow, Own Account, Other Bank Account, Visa Direct, Western Union, and Foreign Remittance. For DuitNow followed by DuitNow Transfer and To Other Account, users must select and input all the required details before accepting the transaction. To complete the transfer, users need to use a token device to obtain a SecureSign token code, which they must input and click the "Submit" button for a successful fund transfer.

Bank E offers fund transfers through Instant Transfer, Interbank GIRO, and 3rd Party and Own Accounts. Users need to select the transfer from and transfer to, followed by inputting transaction details such as transaction type, transfer mode, effective date, account number, recipient's name, transfer amount, and recipient reference. After clicking the "TRANSFER" button, users can choose between two types of secure verification: Secure Verification and SMS TAC. Selecting SMS TAC, users need to request the TAC number and input it to confirm the fund transfer successfully. A receipt is available for download as a reference.

Bank F provides fund transfer methods such as Quick Payment, IBG/DuitNow (Pay-to-Account-Number), DuitNow ID Registration, One Time Transfer to DuitNow ID, and Switch DuitNow ID to UOB. For IBG/DuitNow (Pay-to-Account-Number), users need to select the payee and click on the "DuitNow & Interbank GIRO" tab. Next, they must select the transfer from, transfer mode, recipient account type, recipient ID type, and recipient reference. Inputting the amount and other payment details, users can then click the "Confirm" button to proceed. A notification is sent to the user's mobile phone via the Bank F application, prompting them to enter the secure pin to complete the fund transfer.

v. Mobile Prepaid Reload

This section presents a comparison of the mobile prepaid reload methods offered by six different banks in Malaysia, namely Bank A, Bank B, Bank C, Bank D, Bank E, and Bank F.

Bank A's mobile prepaid reload process involves clicking on the "TOP UP" option and selecting "Mobile Reload." Users are prompted to choose the source account ("From"), specify the amount in MYR, and input the recipient's name. After clicking the "NEXT" button, the webpage displays the Top Up Review, and users can proceed by clicking the "TOP UP" button. Upon completing the input, users need to click the "NEXT" button for payment review and then submit the transaction by clicking the "SUBMIT" button. A notification is sent to the user's mobile phone via the Bank A application, allowing them to either "APPROVE" or "REJECT" the mobile prepaid reload. Approving the transaction leads to a successful reload while rejecting it cancels the fund transfer.

For Bank B, users are required to select the "Prepaid Reload" option. They must choose the source account ("From"), the prepaid category, the service provider, and the reload amount. After specifying the amount, users need to input the mobile phone number and click the "Next" button to review the mobile prepaid reload details. To proceed, users must input the OTP TAC sent via SMS by Bank B before clicking the "Submit" button. The mobile prepaid reload is completed, and users can download a PDF file for reference.

Bank C's mobile prepaid reload process involves selecting "Prepaid Reload" and specifying the "From Account," "Prepaid Type," "Service Provider," "Prepaid Product," "Method of Reload," and "Amount." Users need to input the mobile number and re-confirm it before clicking the "Purchase" button. The webpage displays the reload details, and users need to launch the Bank C Application to either "Confirm" or "Reject" the transaction. Confirming the reload requires entering the verification number shown in the application, resulting in a successful fund transfer. Rejecting the transaction leads to an unsuccessful reload.

Bank D's mobile prepaid reload process includes selecting "Prepaid Top-up" and choosing the "Prepaid Type." Users then click the "Next" button to input the "Handphone No" and select the "Type of Recharge." After clicking the "Accept" button, users need to use a token device to obtain a SecureSign token code, which they must input and click the "Submit" button to complete the fund transfer.

For Bank E, users are requested to reload their mobile prepaid by selecting "Reload From," "Reload To," and "Reload Amount." They need to input the recipient's mobile number and click the "RELOAD" button. Upon doing so, the webpage displays the details of the mobile prepaid reload. Users must choose between two types of secure verification: Secure Verification and SMS TAC. Opting for SMS TAC, users need to request the TAC number and input it to confirm the fund transfer successfully. A receipt is available for download as a reference.

Bank F's mobile prepaid reload process involves adding a new payee to facilitate the reload. Users need to select the "BILLING ORGANIZATION" and input the "BILLER DESCRIPTION" before clicking the "Proceed" button. Afterward, users must input the "BILLER ALIAS" and "MOBILE NUMBER" before pressing the "Submit" button. A notification is sent to the user's mobile phone via the Bank F application, prompting them to enter the secure PIN to reload the mobile prepaid.

V. DISCUSSION

In this section, we will discuss the existing security measures implemented by the selected Malaysian banks (Bank A, Bank B, Bank C, Bank D, Bank E, and Bank F) and compare their effectiveness in safeguarding online banking transactions.

i. Existing Security Measures

Table 1 provides an overview of the existing security measures for online transactions in Malaysia based on the literature review.

Bank A emphasizes security by application. This approach ensures that users must have the bank's official application installed on their devices to access online banking services. By utilizing secure applications, Bank A enhances the security of online transactions, as it reduces the risk of accessing sensitive information through unauthorized third-party applications or fraudulent websites.

Bank B implements One-Time Password (OTP) as a security measure. OTP is a widely adopted method that provides an additional layer of security by generating a unique password for each transaction. This helps protect against unauthorized access, as the password is valid only for a single login session or transaction. OTP adds an extra level of security to the login process and reduces the risk of password-based attacks.

Bank C emphasizes security by application. This approach ensures that users must have the bank's official application installed on their devices to access online banking services. By utilizing secure applications, Bank C enhances the security of online transactions, as it reduces the risk of accessing sensitive information through unauthorized third-party applications or fraudulent websites.

Bank D utilizes multi-factor authentication (MFA) through the implementation of SecureSign Token devices. MFA combines multiple authentication factors to verify user identity, making it more difficult for unauthorized individuals to gain access. By incorporating a token device as one of the authentication factors, Bank D strengthens the security of online banking transactions.

Bank E employs a multi-layered security approach that includes username and password authentication, security phrases, and One-Time Password (OTP). The combination of these security measures enhances the overall security of online banking transactions. The Bank E approach provides multiple layers of protection, requiring users to pass multiple verification steps before completing transactions.

Bank F implements a multi-layered security approach that includes username and password authentication, security words, and secure PINs generated by the bank's application. By combining these security measures, Bank F enhances the security of online banking transactions, ensuring that users undergo multiple authentication steps for added protection.

ii. Effectiveness of Security Measures

Bank A's emphasis on security by application is effective in enhancing the security of online transactions. By requiring users to have the bank's official application installed on their devices, Bank A reduces the risk of unauthorized access through third-party applications or fraudulent websites. This approach helps protect sensitive information and provides a higher level of security.

Bank B's implementation of a One-Time Password (OTP) is an effective security measure. OTPs generate unique passwords for each transaction, making it difficult for unauthorized individuals to gain access. By using OTPs, Bank B adds an extra layer of security to the login process and reduces the vulnerability to password-based attacks.

Bank C's emphasis on security by application, similar to Bank A, is an effective measure. Requiring users to access online banking services through the official application minimizes the risk of unauthorized access through unauthorized third-party applications or fraudulent websites. This approach enhances the security of online transactions and helps protect against potential threats.

Bank D's utilization of multi-factor authentication (MFA) through SecureSign Token devices is an effective security measure. MFA, by combining multiple authentication factors, strengthens the security of online banking transactions. Incorporating a token device as one of the authentication factors adds an extra layer of protection, making it more challenging for unauthorized individuals to gain access.

Bank E's multi-layered security approach, including username and password authentication, security phrases, and One-Time Password (OTP), is effective in enhancing the overall security of online transactions. By implementing multiple verification steps, Bank E adds layers of protection, making it more difficult for unauthorized individuals to compromise the security of online banking activities.

Bank F's multi-layered security approach, incorporating username and password authentication, security words, and secure PINs generated by the bank's application, is also effective. By combining these security measures, Bank F enhances the security of online banking transactions, ensuring that users undergo multiple authentication steps for added protection.

In conclusion, the implemented security measures of the banks, such as security by application, OTP, multi-factor authentication, and multi-layered approaches, contribute to the effectiveness of online transaction security. These measures help mitigate the risks associated with unauthorized access, password-based attacks, and fraudulent activities, providing customers with a higher level of protection for their online banking transactions.

iii. Areas for Improvement

The selected banks have implemented security measures to protect online banking transactions, there are areas where further improvements can be made:

1. Continuous Security Updates

Banks should regularly update their security measures to stay ahead of evolving cyber threats. Regular assessments and updates help identify vulnerabilities and ensure that security measures remain effective against emerging risks.

2. User Education

Banks should invest in user education and awareness programs to educate customers about the importance of online security and safe banking practices. By promoting good security habits among customers, banks can reduce the risk of falling victim to cyber-attacks.

3. Collaboration and Information Sharing

Banks should collaborate with industry peers and regulatory bodies to share information on emerging cyber threats and best practices. This collaboration can help banks stay informed about the latest security trends and enhance their overall security posture.

VI. CONCLUSION

The growth of online banking in Malaysia has provided convenience and accessibility to customers, but it has also raised concerns about the security of online transactions. The selected Malaysian banks have implemented various security measures to protect online banking transactions, such as OTP, secure applications, tokens, MFA, and multi-layered security approaches.

The effectiveness of these security measures varies, with multi-factor authentication and multi-layered security approaches providing stronger protection. However, there are areas for improvement, including continuous security updates, user education, enhanced authentication methods, collaboration and information sharing, robust incident response, and regulatory compliance.

By addressing these areas, Malaysian banks can enhance the security of online banking transactions and foster trust and confidence among their customers. Strengthening security measures is crucial to mitigate risks associated with cyber threats and safeguard the financial interests of Malaysian bank customers.

VII. ACKNOWLEDGEMENT

The authors would like to thank all Schoolof Computing members who were involved in thisstudy. This study was conducted for Online Business, Financial Technology & Cybersecurity ResearchProject. This work was supported by UniversitiUtara Malaysia.

REFERENCES

[1] Reach Publishing Sdn Bhd., “Malaysia Loses

RM2.23 Billion To Cybercrime," BUSINESSTODAY MALAYSIA, 26 July 2022. [Online]. Available: https://www.businesstoday.com.my/2022/07/26/malaysia-loses-rm2-23-billion-to-cybercrime/. [Accessed 5 June 2023].

[2] K. NAIR, "The rise of online financial fraud in Malaysia," The Star, 01 October 2022. [Online]. Available: https://www.thestar.com.my/business/business-news/2022/10/01/the-rise-of-online-financial-fraud-in-malaysia. [Accessed 05 June 2023].

[3] F. Khan, S. Ateeq, M. Ali and N. Butt, "Impact of COVID-19 on the drivers of cash-based online transactions and consumer behavior: evidence from a Muslim market," Journal of Islamic Marketing, vol. 14, no. 3, pp. 714-734, 2023.

[4] S. Chauhan, A. Akhtar and A. Gupta, "Customer experience in digital banking: A review and future research directions," International Journal of Quality and Service Sciences, vol. 14, no. 2, pp. 311-348, 2022.

[5] T. S. Fun and C. G. Chin, "An Evaluation Study of User Authentication in the Malaysian FinTech Industry With uAuth Security Analytics Framework," Journal of Cases on Information Technology (JCIT), vol. 25, no. 1, pp. 1-27, 2023.

[6] W. A. Hammood, R. Abdullah, O. A. Hammood, S. M. Asmara, M. A. Al-Sharafi and A. M. Hasan, "A review of user authentication model for online banking system based on mobile IMEI number," in IOP Conference Series: Materials Science and Engineering, 2020, February.

[7] L. Nena, P. Y. H. P. and Y. Y. Yen, "An online banking security framework and a cross-cultural comparison," Journal of Global Information Technology Management 13, vol. 13, no. 3, pp. 39-62, 2010.

[8] S. A. Basar, N. N. M. Zain, F. Tamsir, A. R. Abdul Rahman, N. A. Ibrahim and H. Poniran, "HOW DIGITAL FINANCIAL LITERACY AFFECTS i-FINTECH ADOPTION AMONG BUMIPUTERA SMEs IN SELANGOR, MALAYSIA," International Journal of Accounting, vol. 7, no. 43, pp. 587-601, 2022.

[9] M. M. Mohammed and M. Elsadig, "A multi-layer of multi factors authentication model for online banking services," in 2013 International Conference on Computing, Electrical and Electronic Engineering (ICCEEE), 2013, August.

[10] Malaysia Computer Emergency Response Team (MyCERT), "Incident Statistics," Malaysia Computer Emergency Response Team (MyCERT), 2023. [Online]. Available: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=70340adb-9f9b-48f3-bf07-11db911e4f00. [Accessed 21 July 2023].