


# An Evaluation Study of User Authentication in the Malaysian FinTech Industry With uAuth Security Analytics Framework

Soo Fun Tan, Universiti Malaysia Sabah, Malaysia\*

 <https://orcid.org/0000-0001-6318-5274>

Gwo Chin Chung, Multimedia University, Malaysia

## ABSTRACT

The increased cyberattack frequency and ferocity have alerted the fintech industry in detecting existential security threats and risks. Various authentication mechanisms have been deployed to countermeasure cyberattacks; whether these deployed solutions fulfil the security and technical standards has not been significantly investigated. This article proposed an uAuth security analytics framework to evaluate the deployed user authentication mechanisms. Subsequently, the technical evaluation study covered ten major commercial banks in Malaysia, whereas 120 respondents aged 18 to 25 participated in the user awareness study. The result found that mobile banking enforces more robust user authentication mechanisms than internet banking in Malaysia. As 80% of the Malaysia fintech systems only ranked as Level 3 of the uAuth security analytics framework, the authors urge Malaysia fintech industry to enhance their authentication factor, login and transaction verification methods, password policy, as well as readiness for quantum-safe security technologies.

## KEYWORDS

E-Banking, Electronic Banking, FinTech, Internet Banking, Mobile Banking, Password-Based Authentication, Phishing Attack, Privacy, Security Analytics Framework, Security, User Authentication

## 1. INTRODUCTION

The recent advancement of fintech technologies allows users to manage financial activities, such as fund transactions and account balance checking, with digital devices (e.g., computers, tablets, smartphones, etc.) that are connected to the Internet. The convenience and effectiveness of fintech have recently resulted in a high penetration rate in the global banking market, i.e., 73% of participants globally use Internet banking at least once a month, compared to 59% who use mobile banking apps (Srinivas & Wadhwani, 2018). In Malaysia, mobile banking transactions increased dramatically,

DOI: 10.4018/JCIT.318703

\*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

from 13.6 million in 2011 to approximately 936 million in 2020 (Muller, 2021). As fintech promises a transformative service for individuals, enterprises, and governments, the increased frequency and ferocity of cyberattacks have alerted the existential security vulnerabilities, threats, and risks in current fintech technologies. Various electronic authentication mechanisms have been deployed in fintech industries recently; whether these solutions meet the security requirements and technical standards for the fintech industry remains unclear. Several surveys and reviews analysing fintech security threats and risks challenges have been published over the last decade. These existing surveys and analytics on fintech security are chronologically summarised in Table 1.

All studies provided security analysis and review of user authentication in the fintech industry, using either qualitative, quantitative, or mixed methods. These methods include interviews, observations, questionnaires, field tests, and experiments. However, their scope of study is generally limited to Internet Banking. Only Krol et al. (2015), Kiljan et al. (2016), Althobaiti (2016), Sinigaglia et al. (2017), and Anoud and Majdalweieha (2019) covered both Internet and mobile banking. Existing surveys generally have focused on analysing user authentication by comparing and verifying security properties offered by various e-banking systems. Syamsuddin et al. (2009), Park et al. (2014), and Cheng (2014) applied a general analytic hierarchy process (AHP) in analysing the security risk of user authentication methods. Subson and Limwiriyakul (2012) and Sinigaglia (2017) employed a

**Table 1.**  
**Chronological summary of previous security analytics and surveys in the e-banking security**

Year	Reference	I	M	Description
2009	Syamsuddin et al.	✓		A general study of Internet banking security in Indonesia using the analytic hierarchy process (AHP). Focus on the perspectives of management, technology, economy, and culture.
2012	Subson and Limwiriyakul	✓		Comprehensive security analytics of Thai commercial banks that focuses on user and systems information and privacy, authentication technology and security features
2013	Choubey et al.	✓		A review of user identification techniques in European Internet banking
2014	Park et al.		✓	Analyses authentication methods of the smartphone banking system in Korea from the security, convenience and cost perspective, and the studied authentication methods are limited to one-time passwords (OTP), Biometrics, and security cards
	Cheng	✓		A brief security risk analysis of China's e-banking systems by using the AHP approach
	Dmitrienko et al.		✓	Focuses on studying the security of two-factor authentication (2FA) by conducting cross-platform attacks
2015	Krol et al.	✓	✓	Analyses the usability and perceived security of 2FA in UK banks by using the interview method
2016	Kiljan et al.	✓	✓	A comprehensive survey on user authentication and communication mechanisms of internet and mobile banking, involving 80 banks worldwide
	Althobaiti	✓		Assesses usable security of multi-factor authentication (MFA) in United Kingdom banking by using questionnaires and field tests
2017	Bucko		✓	Assess Slovakia's smart banking system from the technological security perspective
	Sinigaglia et al.	✓	✓	A survey of authentication methods in Europe banking
2018	Kiljan et al.	✓	✓	Analyses the authentication methods during the payment transaction
2020	Abualsauod et al.	✓		Focuses on identifying the security assurance gaps of online banking in Saudi Arabia
	Anoud et al.	✓		Analyses the authentication methods of E-banking systems in the United Arab Emirates with different attack vectors
2020	Sinigaglia et al.	✓	✓	Comprehensive security analytics that focuses on MFA mechanisms in supporting banking remote payment transactions
2022	Najam and Butt	✓		A very general discussion on Internet banking

Note. I = Internet banking, M = Mobile banking

comparative approach to assessing user authentication in banking, either using a simple checklist or a descriptive study that involves multi-user evaluation.

On the other hand, multiple studies attempted to use quantitative methods in evaluating user authentication. Compared to Choubey and Choubey (2013) and Sinigaglia et al. (2017), who categorised their assessment rubric into three scaling levels, Anoud et al. (2019) use five scaling levels. Bucko (2017) applied ratio scaling to specify his assessment criteria. These assessment rubrics are fundamentally constructed to assess the heterogeneity of proprietary user authentication mechanisms. As public and private authorities have recently introduced regulations, security policies and requirements and technical guidelines to steer the usage of authentication mechanisms, it has urged a standardisation approach to analysing user authentication security that aligns with the established regulations and policies. The contributions of this article are as follows.

First, this paper proposes a security analytics framework for evaluating user authentication's security level, the uAuth security analytics framework. The uAuth security analytics framework is developed in compliance with technical guidelines of the National Institute of Standard and Technology (NIST) and ISO/IEC 29115 Entity Authentication Assurance Framework and Levels of Authentication Assurance (LoA) project and is grounded further on the Malaysia legal framework-Risk Management in Technology (RMiT) policy that released by the Central Bank of Malaysia in July 2019 (Central Bank of Malaysia., 2020). This study evaluates the deployed user authentication solutions in Malaysia's fintech industry using the proposed uAuth security analytics framework with invited academic and industry security experts. The reported result can serve as an external risk assessment report for the Malaysia fintech industry and contribute to the provision of more secure fintech services.

Based on the findings from the conducted evaluation studies, we step forward to develop a uAuth personal security risk evaluation toolkit for individuals to evaluate the security risk of their practices in the fintech industry. The uAuth toolkit also recommends the best practices and useful tips customised to each individual and their selected banks. Also, a total of 120 respondents aged 18 to 25 years old have been invited to participate in the preliminary surveys, and the result can serve as a reference for the fintech industry in redefining their security policies and management. Lastly, we enumerate open security challenges and future research works.

The rest of this article is organised as follows. Section 2 reviews the background of technical guidelines, security requirements, and user authentication policies. Section 3 presents research problems, and the methodology is elaborated in Section 4. Subsequently, the result of the conducted evaluation study and user personal security risk evaluation are analysed and discussed in Section 4.

## 2. LITERATURE REVIEW

NIST is a United States Department of Commerce unit responsible for promoting and preserving the measurement standards in information technology. An electronic authentication guidelines documentation, NIST SP 800-63, was published in August 2013 to establish technical guidelines for implementing user authentication in E-banking. A digital identity guidelines documentation, NIST SP 800-63-3, has subsequently published in June 2017 to provide technical requirements for implementing digital identity services. While these proposals are explicitly targeted at the United States, they are comprehensively pertinent to any environments that are necessary to authenticate users. On the other hand, ISO/IEC 29115 Entity Authentication Framework (NIST, 2017) promote the standardisation of user authentication security by specifying minimal technical, management and process requirements in assuring the security of identity authentication. The Central Bank of Malaysia released the Risk Management in Technology (RMiT) policy in July 2019 to provide a guideline for financial institutions to withstand the increasing cybercrime and cyberattacks.

## 2.1 National Institute of Standard and Technology

In NIST SP 800-63 Electronic Authentication Guideline document, NIST characterises the technical requirements of authentication security into four *levels of assurance* (LoA) in the regions of identity, proofing, registration, tokens, authentication protocols, and related assertions. In Level 1, any token methods of Levels 2, 3, or 4 are allowed, including a simple PIN. Cryptography methods that block offline analysis by eavesdroppers are not applied in the first level. In Level 2, the single-factor authentication method is required. Memorised-secret tokens, pre-registered tokens, secret look-up tokens, out-of-band tokens, and single-factor one-time password devices are allowed to be used. An example of a memorised personal token is a password or PIN. Pre-registered knowledge token is a response to a security question or image that the user has previously submitted. A secret look-up token is a secret that is stored in a hardware token, such as a number printed on a card. An out-of-band token is a secret received from the verifier via a device such as a mobile phone. A single-factor one-time password device generates a password that can only be used once. Level 3 requires a multi-factor remote network authentication method, which requires at least two authentication mechanisms from two categories of authentication factors (knowledge, possession, and inherence) to work together in a system. At this level, a multi-factor software cryptographic token is required, activating the knowledge factor or inherence factor. Level 4 allowed only the multi-factor hardware cryptographic token. NIST suggested that a Level 3 authentication standard be used to ensure authentication security.

On the other hand, three assurance levels have been proposed for the NIST SP 800-63-3 digital identity guidelines document in 2017. In level 1, the single or multi-factor authenticator is allowed. Memorised-secret token, secret look-up token, out-of-band token, single-factor one-time password device, single-factor cryptographic software, single-factor cryptographic device, multi-factor cryptographic software, and multi-factor cryptographic device are allowed to be used, almost the same as the Level 2 requirements of the electronic authentication guidelines. If the account is in use and exceeds the time limit of 30 days, the account should be logged out automatically. Level 2 requires a multi-factor authenticator or combination of two single-factor authenticators, including the secret look-up token, out-of-band token, single-factor one-time password device, single-factor cryptographic software, single-factor cryptographic device, multi-factor one-time password device, multi-factor cryptographic software, and multi-factor cryptographic device. If the account is in use and exceeds the time limit of 30 minutes, the account should be logged out automatically. Level 3 requires multi-factor authentication but is limited to hardware-based authenticators only. If the account is in use and exceeds the time limit of 15 minutes, the account should be logged out automatically.

## 2.2 Levels of Authentication Assurance

The LoA project investigates a fine-grained authorisation scheme that can represent the level of confidence in the electronic identity of a user presented to the service providers. A four-level of authentication assurance is proposed (Nenadic et al. 2007). Level 1 and level 2 allow four token types: hard token, one-time password token, soft token, and password token. Password token is not allowed in level 3 and the hard token is the only authentication token in Level 4. A minimum requirement of authentication assurance level to ensure security is Level 3. Level 1 consists of minimal confidence in the asserted identity, which will be applied when there is a minimum risk of erroneous authentication. This level does not require a cryptographic method, and there is no specific requirement for the authentication mechanism. Level 2 consists of some confidence in the asserted identity, which will be applied when there is a moderate risk of erroneous authentication. This level accepts single-factor Authentication. Level 3 consists of high confidence in an asserted identity, which will be applied when there is a substantial risk of erroneous authentication. This level accepts multi-factor authentication. The confidential information that is exchanged in the authentication protocols has to be encrypted. Level 4 consists of very high confidence in an asserted identity, which will be applied when there is a high risk of erroneous Authentication. This level accepts multi-factor Authentication as well as Level 3, but there are requirements added, which are identity proofing and storage of secret or private

cryptographic keys in hardware devices. The confidential information exchanged in the authentication protocols has to be encrypted.

### **2.3 ISO/IEC 29115 Entity Authentication Assurance Framework**

Similar to NIST SP 800-63 Electronic Authentication Guideline, ISO/IEC 29115 Entity Authentication Assurance framework proposed four specified LoAs in promoting the worldwide standardisation of implementing user authentication. Level 1 covers minimal confidence in the asserted identity, and a cryptographic method is not required; Level 2 implies some confidence in the asserted identity, and single-factor authentication is required. High confidence in an asserted identity and multi-factor authentication is required in Level 3. Level 4 refers to very high confidence in an asserted identity, and multi-factor authentication is required. Level 4 provides cryptographic protection to all sensitive data, including private keys.

### **2.4 Risk Management in Technology**

The Risk Management in Technology (RMiT) policy was launched in July 2019 by the Central Bank of Malaysia to provide a guideline for financial institutions to withstand the increase in cybercrime. According to the RMiT documentation, the banking system's authentication mechanism shall include at least one of the three factors: knowledge, possession, or inheritance. The Central Bank of Malaysia also encourages financial institutes to implement multi-factor authentication to increase security defence. The documentation also stated that the latest version of Transport Layer Security (TLS) should be employed to ensure that transactions are conducted through secure channels. Additionally, the newest version of the extended validation secure socket layer (SSL) certificate can be applied to build a stronger mutual authentication between the user and the bank server. If a one-time password (OTP) is used as the second factor, whether for login or transaction, it should be dynamic and time bound. All the assessments shall be conducted every three years or whenever there are any changes to ensure the security of the bank system.

## **3. RESEARCH PROBLEMS**

The increasing frequency and ferocity of the cyberattack alerted the existential security vulnerabilities, threats, and risks in cyberspace, especially in the fintech industry. As authentication mechanisms are the front baseline of security defence mechanisms to verify user identity to grant privilege and authorise access to online banking services, assessing existing user authentication mechanisms and countermeasures in the fintech industry has urgent urged. Various user authentication mechanisms have been practised in the banking industry, including password-based, biometrics-based, picture- or gesture-based, and out-of-band authentication (OOBA). The preliminary result revealed that the password-based authentication mechanism had dominated the fintech industries and is still vulnerable to cyber threats and attacks. As every authentication method has its unique solutions and associated vulnerabilities, there is no single best solution for the authentication mechanism in the banking industry. This study aimed to investigate further and evaluate the security of user authentication mechanisms deployed in Malaysia's fintech industry with the proposed uAuth security analytics framework. The study attempts to discuss the following issues:

- Different banking and finance institutes vary in their user authentication mechanisms and standards. Whether these deployed authentication mechanisms meet the global security requirements and technical standard remain unclear. A security analytics framework that complies with the NIST technical guidelines, ISO/IEC 29115 Entity Authentication Assurance Framework, and Malaysia's RMiT policy in evaluating the security level of user authentication mechanism is urgently urged to address this concern.

- An evaluation of the deployed authentication mechanism in Malaysia's fintech industry that can serve as an external risk assessment report for the Malaysia fintech industry and contribute to the provision of more robust fintech services has not been significantly studied.
- Evaluation of user personal security risk and awareness of their practices in the fintech industry has not been significantly investigated, especially in Malaysia.

## 4. RESEARCH METHODOLOGY

### 4.1 Study Instruments

#### 4.1.1 *uAuth Security Analytics Framework*

The developed uAuth security analytics framework is constructed via focus group discussion by referring to the technical guidelines of NIST SP 800-63, NIST SP 800-63-3, and the worldwide standardisation of ISO/IEC 29115. The analytic rubric method is selected to construct the uAuth security analytics framework for evaluating user authentication. The uAuth security analytics framework applies the well-established LoA approach to categorising the assessment levels: Level 1 Adequate, Level 2 Competence, Level 3 Good, and Level 4 Excellent. In the initial stage of establishing the selected security features of the assessment framework, these selected security features of user authentication are classified into five categories, including (1) authentication factor and method; (2) password management and policy; (3) login failure limitations; (4) reauthentication; and (5) the methods of the user authenticates the bank website. Subsequently, these security features are evaluated by using a multi-user evaluation approach. A total of 20 security experts from industry and academia in Malaysia are invited with the cluster sampling method.

With the valuable feedback and constructive inputs from these security experts, the proposed uAuth security analytics framework is further improved and finalised into eight categories: Authentication Factor (C1), Authentication Method for Login (C2), Password Management and Policy (C3), Password Recovery Management and Policy (C4), Transaction Verification (C5), Login Attempt Limitations (C6), Reauthentication (C7), and Types of Encryption Protocol and Certificate Authority (C8), as summarised in Appendix Tables A1–A8.

#### 4.1.2 *uAuth Personal Security Risk Assessment Toolkit*

This research takes a step forward to develop a uAuth personal security risk assessment toolkit for increasing security awareness among the community with an incremental prototyping approach. Ease of use android-based evaluation toolkit is designed based on the findings from conducted technical evaluation study. As Malaysia's fintech industry is practising heterogenous authentication solutions, the security questions are further customised to the selected bank practices and deployed authentication mechanisms to minimise the number of questions that need to be answered by the community. As the assessment framework only involves user site authentication technology, the uAuth evaluation toolkit assessment is limited to the assessment of Authentication Method for Login (C2), Password Management and Policy (C3), Password Recovery Management and Policy (C4), and Transaction Verification (C5).

The implementation of uAuth personal security risk assessment toolkit is demonstrated in Figure 1. The participants are requested to select the banking system they wish to evaluate with the uAuth security analytics framework, as illustrated in Figure 1A. Next, the participants are further requested to select an internet banking or mobile banking application, as demonstrated in Figure 1B. Subsequently, the participant is directed to answer the security questions from Section B, as illustrated in Figure 2A. After completing all security questions, the scoring and results will be calculated and displayed to participants, as demonstrated in Figure 3A. Participants can optionally click on "Check the Suggestions" to navigate to the suggestion page, which aims to increase user awareness and improve their bad practice, as presented in Figure 3B.

Figure 1.  
The implementation of the uAuth personal security risk assessment toolkit

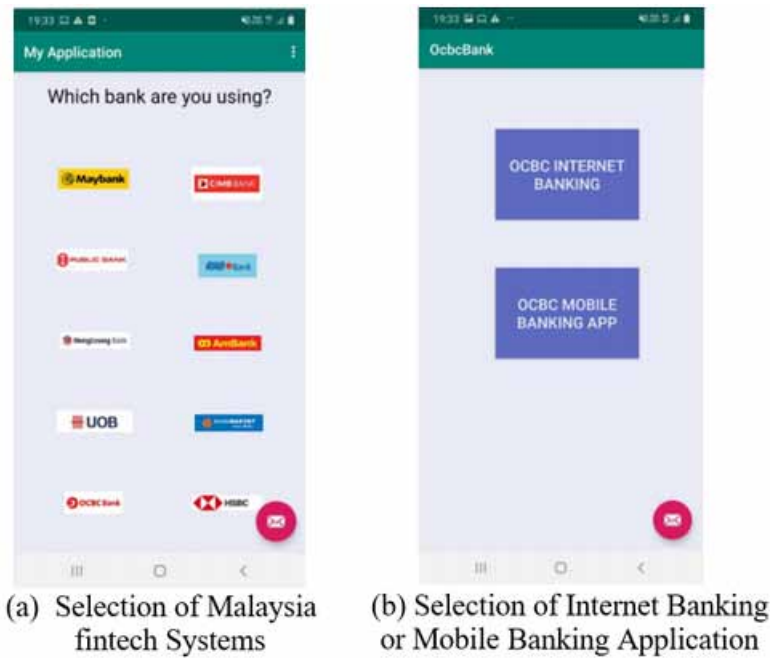
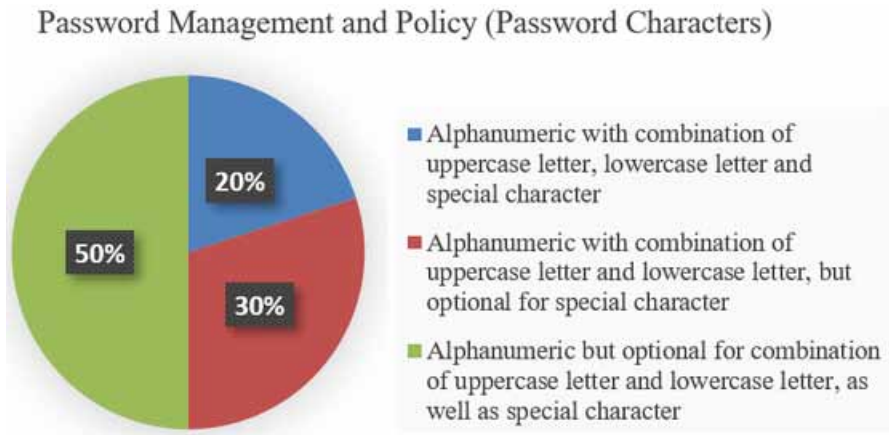


Figure 2.  
Sample of security questions customised for the OCBC e-banking system in terms of Password Management and Policy (C3) and Transaction Verification (C5)

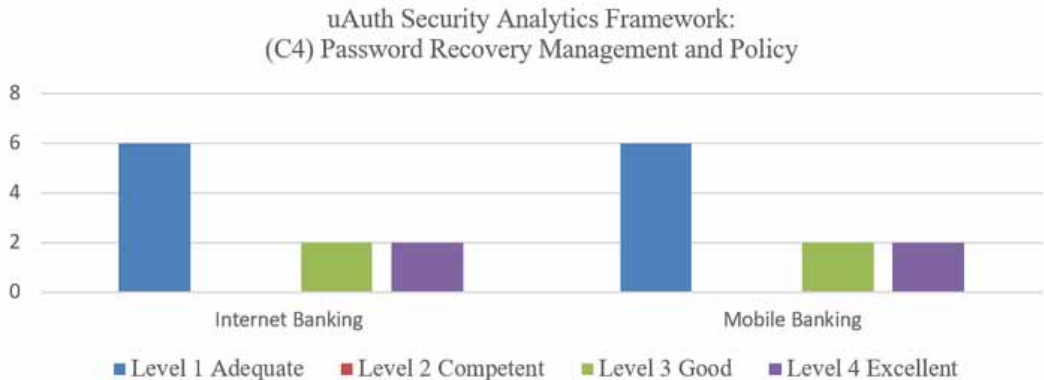


## 4.2 Study Sample and Context

### 4.2.1 Multi-User Technical Evaluation Study

The conducted technical evaluation study focuses on assessing the bank site authentication mechanism from a user perspective. In this technical evaluation study, the implicit multi-user evaluation involving cybersecurity research teams and security experts in Malaysia was employed. A total of six security experts from industry and academia have accepted the invitation to study and evaluate the deployed

Figure 3.  
Sample analytics result of uAuth personal security risk assessment toolkit



user authentication solutions in the Malaysia fintech industry. Considering there are 27 commercial banks in Malaysia, including 90 licensed foreign banks. With purposive sampling, the 10 largest commercial banks, according to their asset values as listed in Standard & Poor’s 2017, were selected in this study. They are Maybank, CIMB Bank, Public Bank, RHB Bank, Hong Leong Bank, Ambank, UOB Bank, Bank Rakyat, OCBC Bank, and HSBC Bank. The evaluation and analysis depend on a dataset gathered by analysing the resources made publicly available by banks, including official documentation, webpages, security announcement and FAQ pages, security guidelines, handbooks, user manuals, and more. Also, the field tests were conducted by registering an individual account with each selected bank to assess the user site authentication technology. During data collection, some conflicts in information from different solutions were detected. In such cases, the significance of official documentation and the latest release was prioritised.

#### 4.2.1 uAuth Personal Security Risk Assessment Evaluation Study

Considering the percentage of Malaysians aged 15 and above increased from 89.6% in 2020 to 96.8% in 2021, meanwhile, the usage of the mobile phone rose to 98.7% in 2021 from 98.2% in 2020 and time feasibility, this evaluation study scoped to invite participants from Malaysia’s campus. A total of 120 participants aged 18 to 25 from Malaysia’s campus have participated in this study, as summarised in Table 2. After the evaluation, the scoring result is displayed to the individual. Subsequently, a customised suggestion will be given based on their practices and selected banks.

Table 2.  
Participants’ gender versus fintech applications cross-tabulation

	Fintech Applications									
Gender	May bank	CIMB	Bank Islam	Public Bank	Hong Leong Bank	Bank Simpanan Nasional (BSN)	Bank Rakyat	Ambank	HSBC Bank	Total
Male	15	21	10	5	1	3	1	0	0	56 (47%)
Female	30	12	9	7	3	0	1	1	1	64 (53%)
Total	45 (38%)	33 (27%)	19 (16%)	12 (10%)	4 (3%)	3 (2%)	2 (2%)	1 (1%)	1 (1%)	120



## 5. RESULTS AND DISCUSSION

### 5.1 Evaluation Study on Malaysia Fintech with Multi-user Evaluation

The result of implementing the uAuth security analytics framework to assess the security level of user authentication for the Malaysia fintech industry is summarised below.

#### 5.1.1 Authentication Factor (C1)

All fintech and financial institutions are deploying the two-factor authentication mechanism and achieving Level 2, *Competent in Internet Banking*, as illustrated in Figure 4. Whereas, the achievement of mobile banking is more encouraging, in which 20% of them are able to reach Level 4, *Excellent*, with the deployment of a hardware token. A total of 40% of banks are ranked as Level 3, *Good*, by deploying the multi-factor authentication mechanisms. Most of them are applying biometric authentication as an optional mechanism, including Maybank (face, fingerprint, or voice recognition), Public Bank (fingerprint recognition), RHB Bank (fingerprint recognition), UOB Bank (face or fingerprint recognition), OCBC Bank (face or fingerprint recognition), and HSBC Bank (face or fingerprint recognition).

#### 5.1.2 Authentication Method for Login (C2)

Among the 10 selected banks in Malaysia, 20% of them are outperformed by other banks in the login authentication method in Figure 5. Only 20% of the selected banks are ranked as Level 4, *Excellent*, for both internet banking and mobile banking. Some 80% of them are limited to reaching Level 2, *Competent*. Various authentication methods have been deployed, and 100% use a password-based authentication mechanism with username and password to verify user credentials in internet banking or mobile banking, as summarised in Figures 6 and 7, respectively. Subsequently, additional authentication methods need to be activated by the user to enjoy more robust security features, including an on-screen keyboard, OTP from SMS, hardware token, software token, and secondary password. Whereas CAPTCHA can be used to prevent password brute-force attacks, 30% of them are focused on using additional security images to tackle increased phishing attacks.

#### 5.1.3 Password Management and Policy (C3)

The achievement in Password Management and Policy need improvement. Most of the selected banks are limited to reaching Level 2, *Competent*, in both Internet and mobile banking, as illustrated in Figure

Figure 4.  
The achievement of Authenticator Factor (C1)

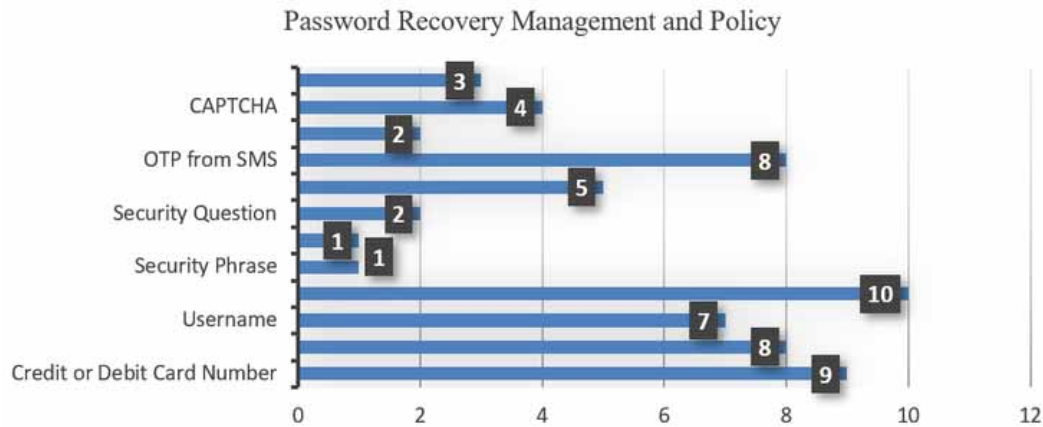


Figure 5.  
The achievement of Authenticator Factor for Login (C2)

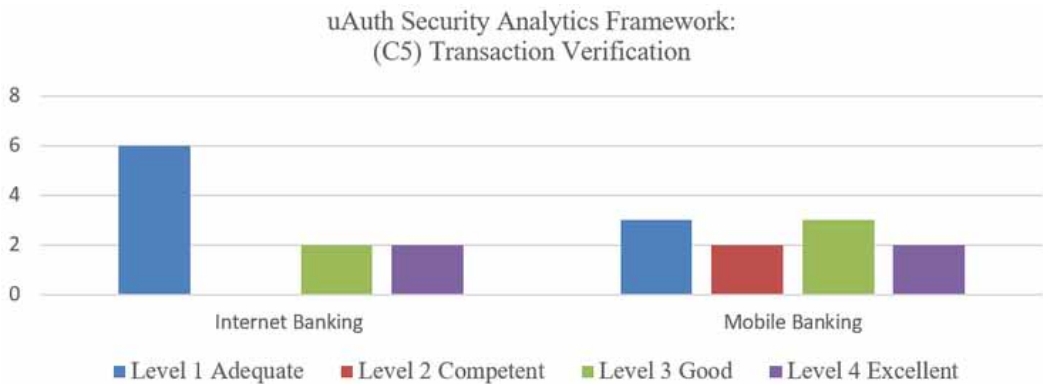


Figure 6.  
Login authentication method of Internet banking application

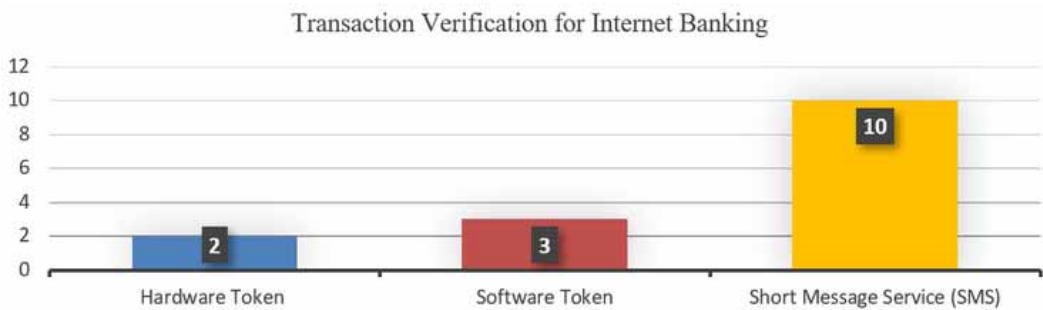


Figure 7.  
Login authentication method of mobile banking application



8. The main reason is that 90% of their password policy only requires a minimum length of eight characters, and an unfavourable 10% of them only require a minimum length of six characters. None of the chosen banks can reach Level 3, *Good*, requiring a minimum password length of 12 characters. The detailed analysis of password length and usage of characters pattern is further summarised in Figures 9–10, respectively. Maybank, Public Bank, and OCBC Bank recommend the password length of 8–12 characters. Hong Leong Bank supports the password length of 8–16 characters. CIMB Bank and Bank Rakyat recommend the password length of 8–20 characters, while the UOB Bank supports

the password length of 8–24 characters. All the banks require an alphanumeric password, 50% require a combination of uppercase and lowercase letters, and 20% need special characters. In contrast, others are optional for combining uppercase and lowercase letters and special characters. All the banks did not check password strength automatically while creating a new password. Also, they did not provide a password hint when the user forgot the password.

5.1.4 Password Recovery Management and Policy (C4)

Figure 11 reveals that 60% of the selected banks are ranked as Level 1, *Adequate*, lacking CAPTCHA implementation to prevent password brute-force attacks. It is detected that four banks are implementing CAPTCHA to prevent brute-force attacks. The details of the deployed password recovery methods in Malaysia fintech are summarised in Figure 12. While 90% of these banks require the credit or debit card number to reset the password, subsequently, 89% of them require an additional card PIN to verify legitimate user credentials, 80% of banks require a one-time password (OTP) from a short message service (SMS), 20% of the Bank’s OTP can be accepted through the hardware token, and 70% of them need the account username to reset the password. The verification that relies on security phrases, images, or questions is limited to 30%. Five banks have implemented identity-proofing information. Three banks need the email address to reset the password. All of them require an old password to reset the new password online.

5.1.5 Transaction Verification (C5)

In Internet banking, only 20% of the selected banks fulfil the requirements of Level 4, *Excellent*, whereas 20% are classified into Level 3, *Good*, and the rest are limited to Level 1, *Adequate*, as

Figure 8.  
The achievement of Password Management and Policy (C3)

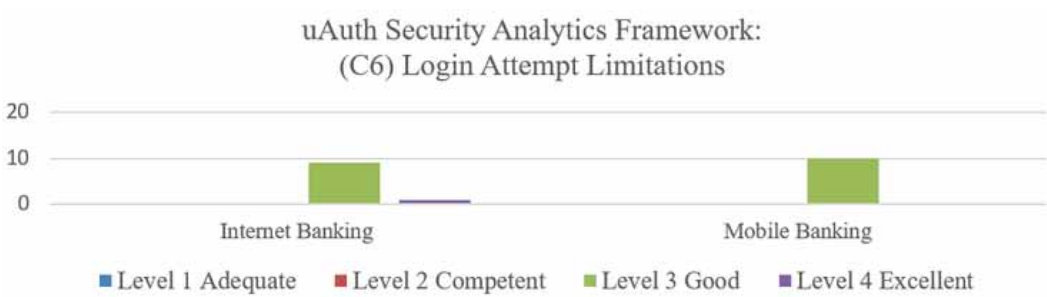


Figure 9.  
Password length requirements

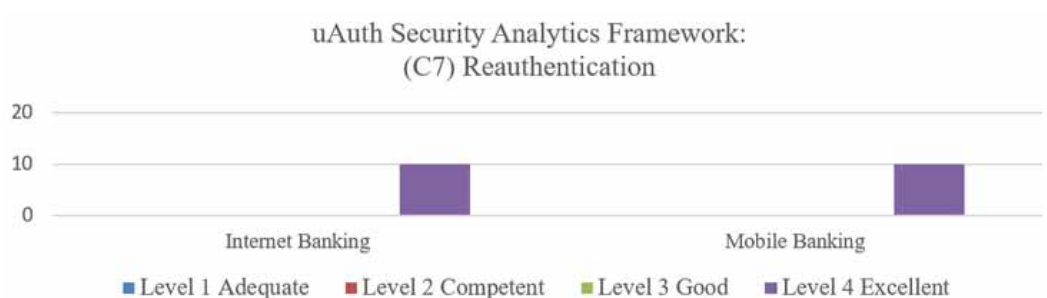


Figure 10.  
Character pattern usage

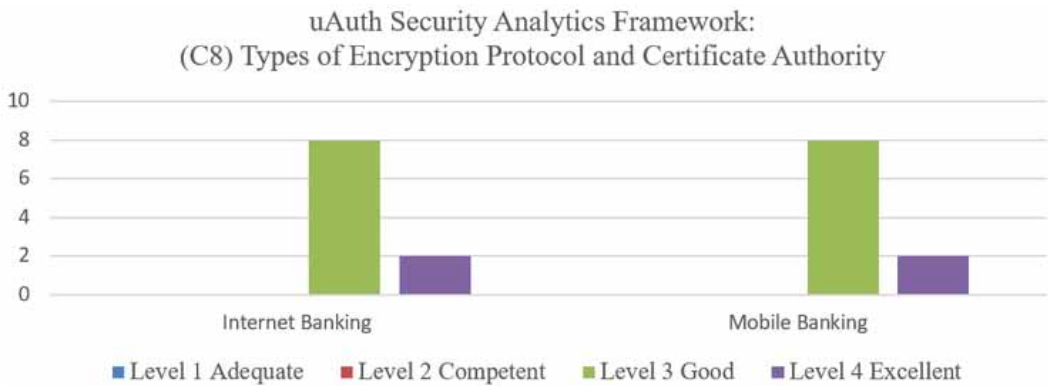
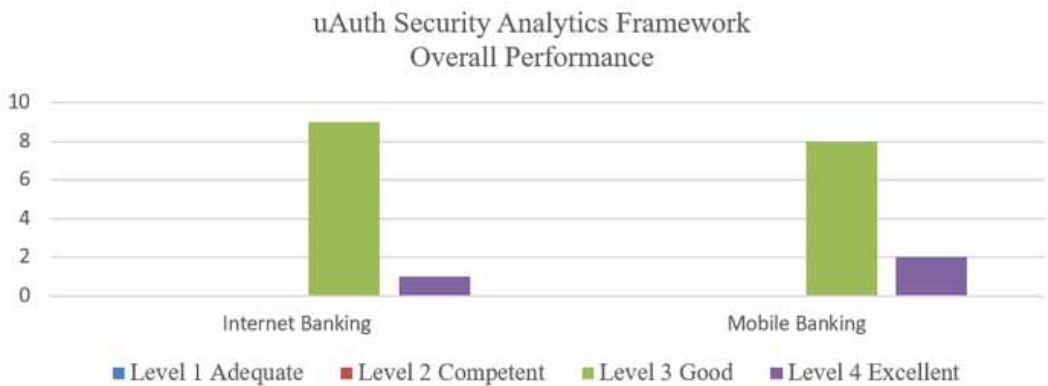


Figure 11.  
The achievement of Password Recovery Management and Policy (C4)



demonstrated in Figure 13. Figure 14 reveals that all banks employ the short message service (SMS) based, one-time password (OTP) to verify the requested transaction. Among 10 selected banks, 20% use the hardware token, while 30% use the software token. Whereas, in mobile banking, 20% of the selected banks can reach Level 4, *Excellent*, and 40% fulfil the requirements of Level 3, *Good*. Figure 15 demonstrated that 80% of them use the SMS-based one-time password (OTP) for transaction verification, 20% rely on a hardware token, 40% use the software token, and 30% of them allow biometric authentication for the transaction, including fingerprint and face recognition.

#### 5.1.6 Login Attempt Limitations (C6)

All selected banks lock off the user account after three attempts, as illustrated in Figure 16: 90% of them are ranked as Level 3, *Good*, and only 10% reach Level 4, *Excellent*, by implementing a CAPTCHA mechanism during the login attempts.

#### 5.1.7 Reauthentication (C7)

As illustrated in Figure 17, the achievement of reauthentication in Malaysia's fintech industry is very impressive. All selected banks are classified as Level 4, *Excellent*, by limiting the user's active session within five minutes in both Internet banking and mobile banking. The account of Hong Leong Bank

Figure 12.  
Password recovery methods

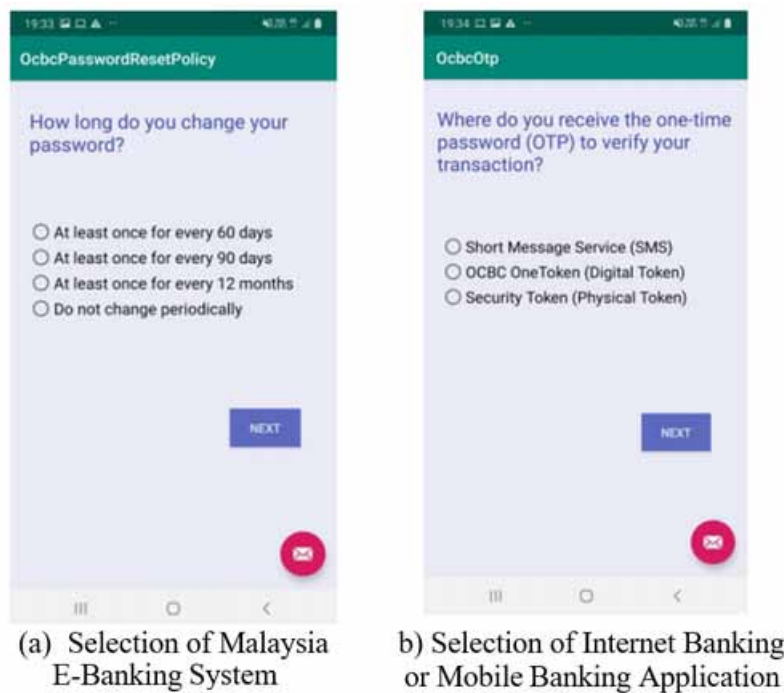
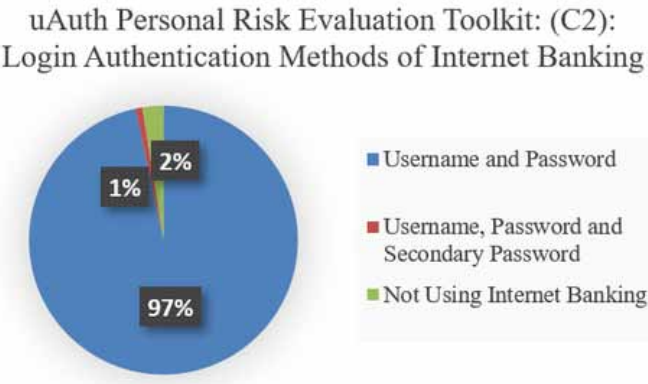


Figure 13.  
The achievement of Transaction Verification (C5)



will be deactivated if it is not used for three months, whereas Public Bank and MayBank enforced six months and twelve months, respectively; 70% of the banks do not have information about the deactivated period.

5.1.8 Types of Encryption Protocol and Certificate Authority (C8)

All of the selected banks deployed TLS 1.2 on their server edges and ranked as Level 3, *Good*, as illustrated in Figure 18. However, only 20% of the selected banks have stepped forward to support the latest TLS 1.3 released in August 2018.

Figure 14.  
Transaction verification methods used

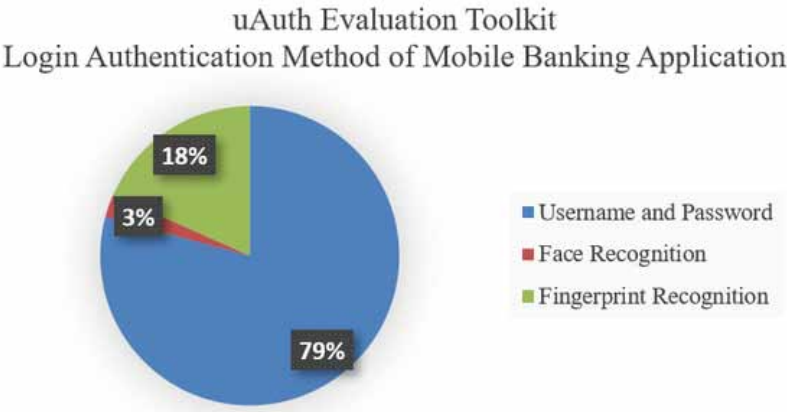


Figure 15.  
Transaction Verification for mobile banking applications

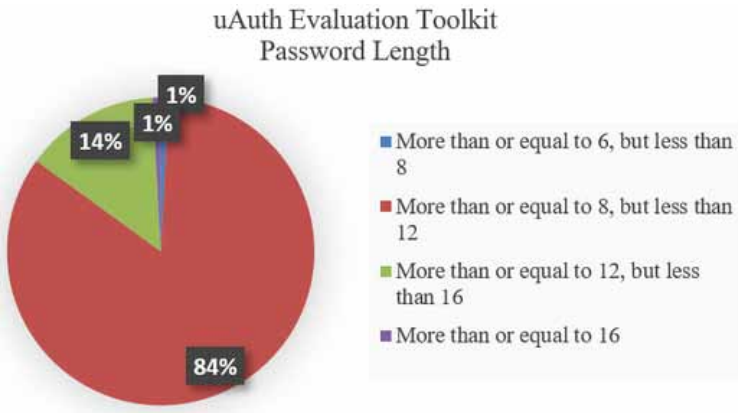


Figure 16.  
Login attempts limitations (C6)

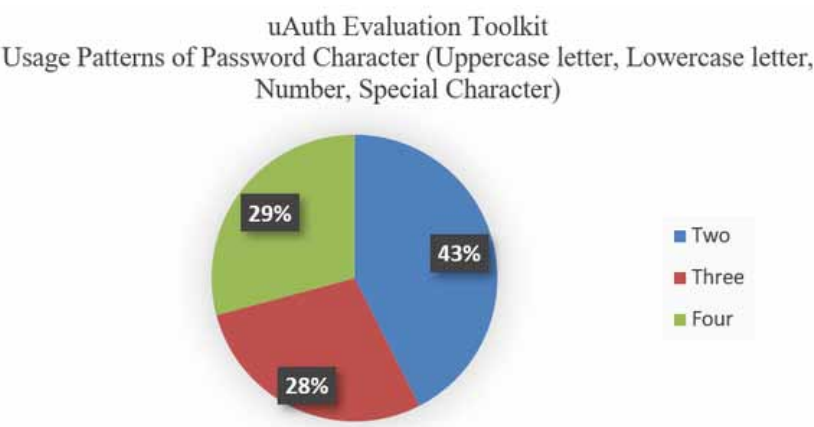


Figure 17.  
Login attempts limitations (C6)

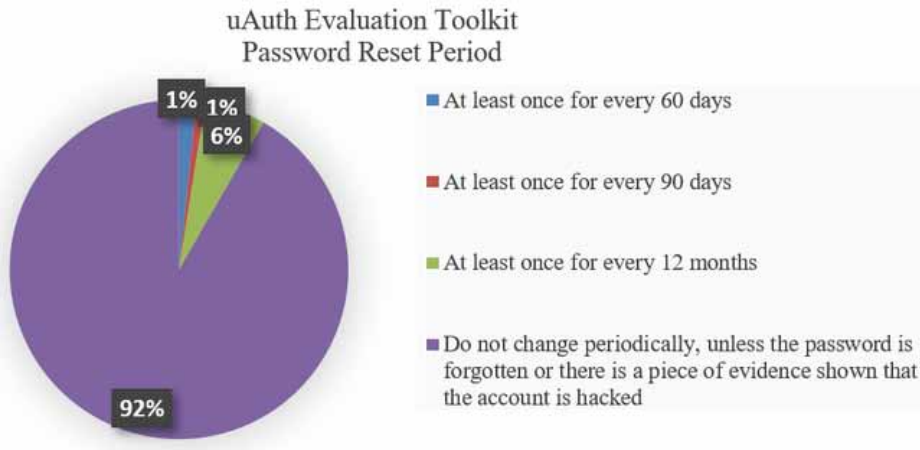
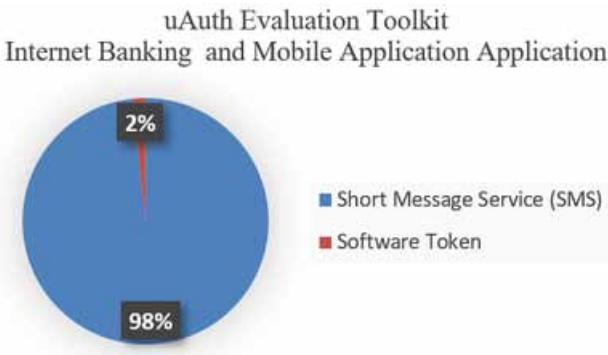


Figure 18.  
The achievement of login attempts limitations (C6)



Generally, most of Malaysia’s fintech institutions and financial banks use the combination of the username and password as the authentication method of the internet banking system and mobile banking application. All selected banks are implementing two-factor authentication, requiring a security image (40%) or security phrase (60%), which fulfil the requirements of NIST, ISO/IEC 29115 Entity Authentication Assurance Framework, and the Central Bank of Malaysia.

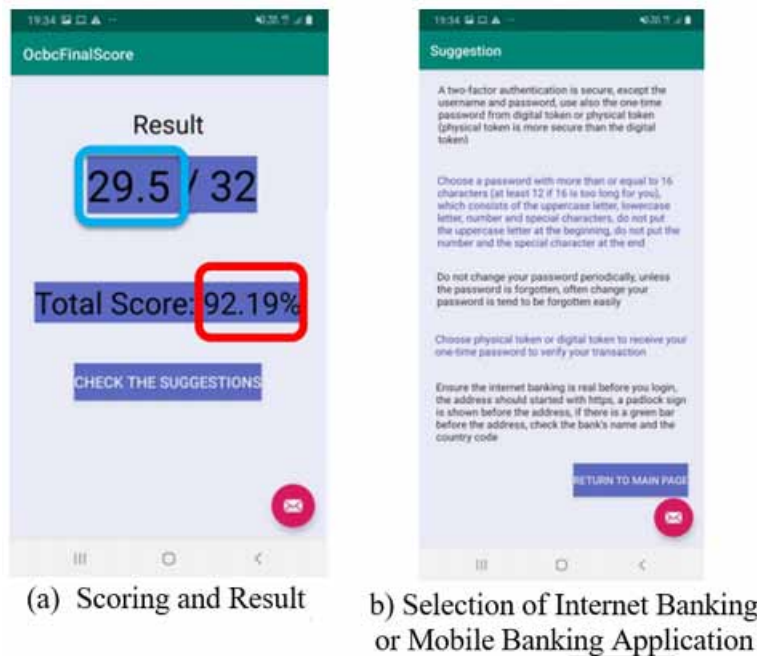
In conclusion, the scoring of mobile banking is slightly higher than Internet banking for all selected banks with the implementation of biometric-based Authentication, as demonstrated in Figure 19. In Internet banking, all selected banks are achieving Level 3, *Good*, and only 10% of the selected banks are classified as Level 4, *Excellent*. Meanwhile, for mobile banking, 20% of the chosen banks can reach Level 4, and the rest of them are ranked as Level 3.

5.2 Evaluation Study on uAuth Personal Security Risk Assessment

The uAuth personal security risk assessment toolkit is developed to collect data from 120 participants to evaluate their security awareness and practices in fintech systems from the aspect of Authentication Method for Login (C2), Password Management and Policy (C3), Password Recovery Management and



Figure 19.  
Overall performance of the deployed user authentication mechanism



Policy (C4), and Transaction Verification (C5). The collected data the detailed results are discussed below.

### 5.2.1 Authentication Method for Login (C2)

For the authentication method of Internet banking during login, most respondents choose to use password-based authentication, which is the combination of the username and password, occupied 97% of the 120 respondents, as illustrated in Figure 20. Only 2% of the respondents are not using Internet banking, and 1% of the respondents use the combination of the username, password, and secondary password as the login authentication method. The results showed that 97% of the respondents prefer to use password-based authentication for authenticating their login in Internet Banking. Only 1% of them apply the secondary password. Subsequently, another 2% of the participants have no experience in using Internet banking.

Likewise, most participants prefer to use password-based authentication for logging into a mobile banking application, occupying 79% in Figure 21. Only 18% of the respondents use the fingerprint authentication method, 3% use the face authentication method, and 21% of the participants use biometric authentication to access their accounts.

### 5.2.2 Password Length

Most of the participants' chosen length of passwords is 8–11 characters, which occupied 84%, as shown in Figure 22. Only 14% have password lengths of 12–15 characters. Only one participant used passwords 6–8 characters in length. Also, only 1% of them use a password with 16 or more characters.



Figure 20.  
Login authentication method in Internet banking

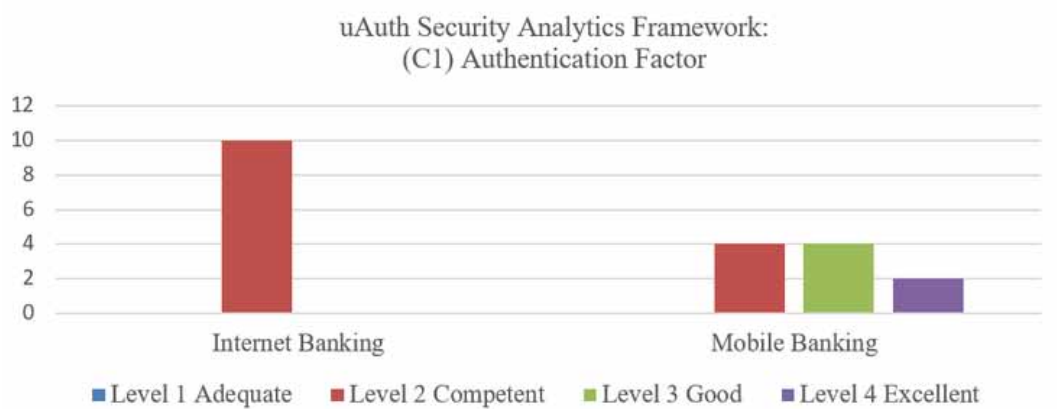
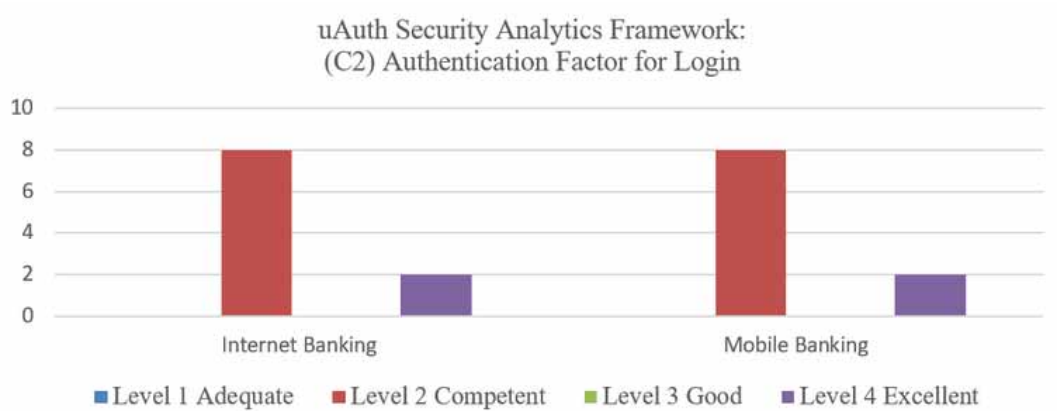


Figure 21.  
Login authentication method in mobile banking applications



### 5.2.3 Usage Pattern of Password Characters

Most participants' passwords consist of a combination of any two character types from the uppercase letter, lowercase letter, numeric, and special character, which occupied 43% in Figure 23. A total of 35 participants defined their passwords with a combination of all character types. At the same time, the rest of the participants have a password consisting of any three of all character types.

### 5.2.4 Password Reset Period

Most participants did not change their password periodically, which occupied 92% as summarised in Figure 24. Only 6% change their password at least once every 12 months. Two participants changed their passwords at least once every two to three months.

### 5.2.5 Transaction Verification

Almost all the participants choose to receive their one-time password (OTP) for transaction verification of internet banking and mobile banking via SMS, which is 98% as shown in Figure 25. Another 2% of the participants receive the OTP via the software token.

Figure 22.  
Password length

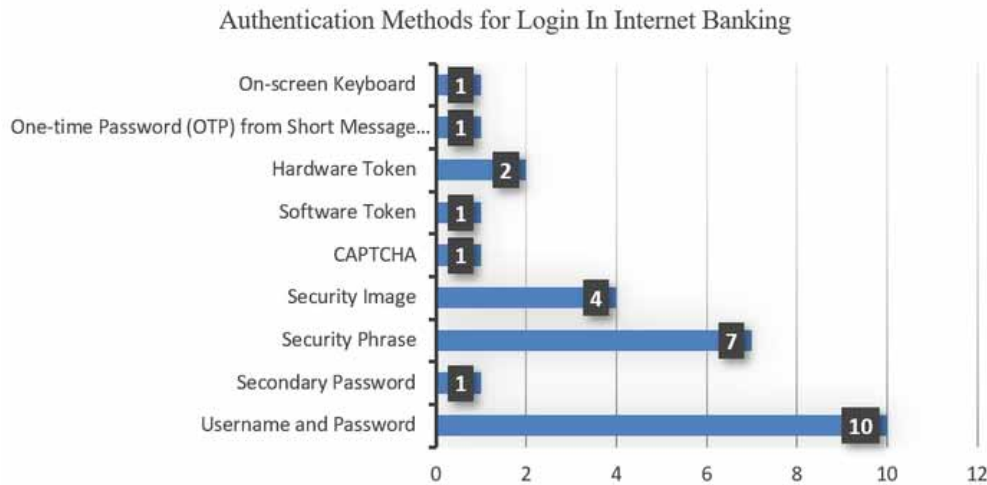


Figure 23.  
Password usage patterns

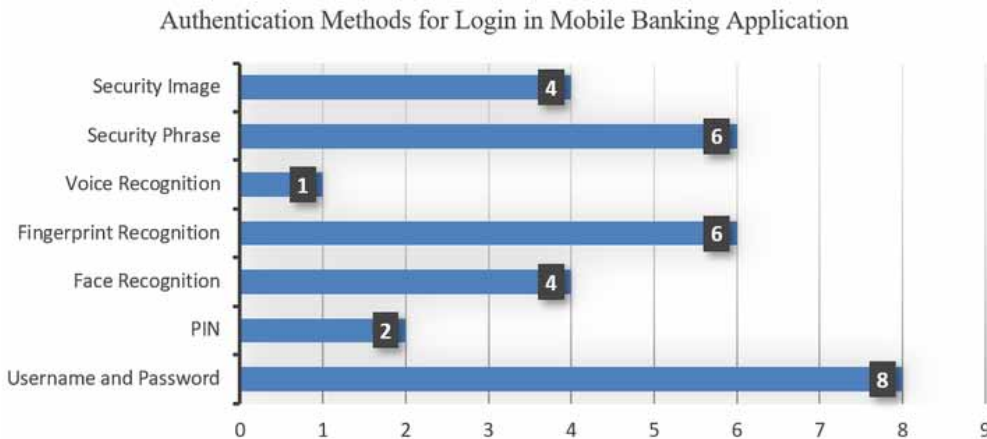


Figure 24.  
Password reset periods

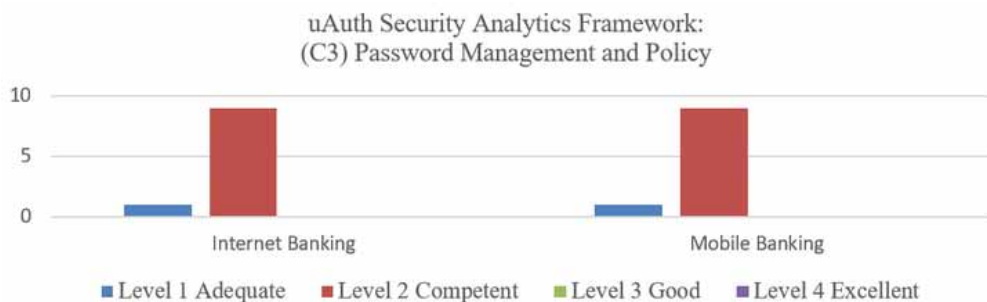
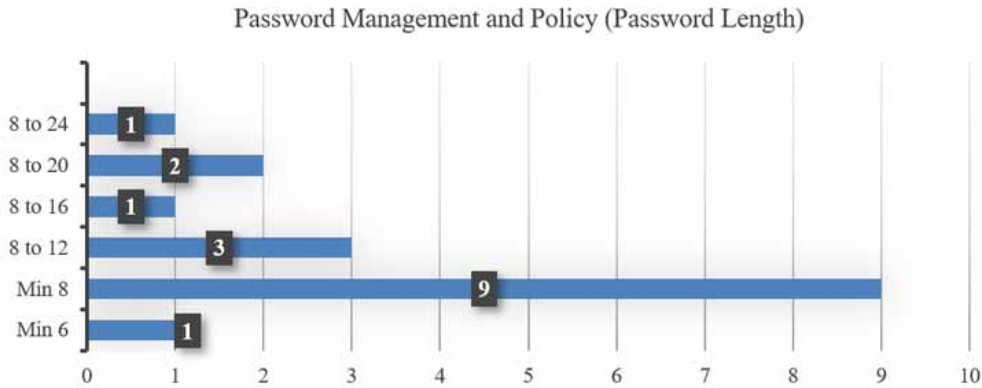


Figure 25.  
Transaction verification in Internet banking applications



In conclusion, this study found that 85% of the participants can score above 65% and achieve Level 3, *Good*, in this evaluation of uAuth personal security risk assessment toolkit. However, most still rely on SMS-based OTP to reset their password and verify their transaction. Also, most participants still prefer to define the password length as less than 12 characters with the combination of any two types of characters.

6. CONCLUSION AND FUTURE DIRECTIONS

This article comprehensively studies deployed user authentication solutions in the Malaysian fintech industry by proposing uAuth security analytics framework to evaluate their security level. While the recent studies are directed at assessing heterogeneity of proprietary user authentication mechanisms, this research stepped forward to propose a uAuth framework that compliance with the latest regulations, security policies and standardisation documentation. These include NIST and ISO/IEC 29115 Entity Authentication Assurance Framework and LoA Assurance project, and Malaysia’s legal framework, RMIT. The proposed uAuth security analytics framework covers the assessment of authentication factors, authentication method for login, password management and policy, password recovery management and policy, transaction verification, login attempt limitations, reauthentication, and types of encryption protocol and certificate authority. Subsequently, the LoA approach is applied to classify the assessment levels: Level 1, *Adequate*, Level 2, *Competent*, Level 3, *Good*, and Level 4, *Excellent*.

The evaluation study was conducted using a multi-user evaluation approach, together with invited security experts from industry and academia. The top ten largest commercial banks in Malaysia have been selected accordingly to their listed asset values. The analytics result revealed that only 10% and 20% of the selected banks are ranked as Level 4, *Excellent*, in internet banking and mobile banking, respectively. Subsequently, we conducted a evaluation study on user personal risk and awareness that involved 120 respondents by using the developed uAuth personal risk assessment toolkit. The result found that most of the respondents still prefer to use the conventional E-banking system approach, including SMS-based tokens, two-factor authentication (username and password), and the use of numeric and alphabet in defining their password.

Malaysia’s deployed user authentication mechanisms are not a single fintech technology; in turn, it leverages various fintech technologies, such as conventional SMS texting, sensing technologies, biometric technologies, and cross-communication platforms. As most of Malaysia’s fintech systems still rely on traditional security approaches to build up their user authentication mechanisms, we further summarised the remaining open issues and security concerns from future perspectives, as below.

## **6.1 Password-Based Authentication**

All banks rely on two-factor authentication, user ID and password, to authenticate their user, and 90% of them enforce the password policy with a minimum length of eight characters. Recent password cracking studies demonstrated that any hashed eight-characters length password that consists of any combination of 95 characters could be cracked in 5.5 hours with a speed of 350 billion-guess-per-second speed in 2012 (Goodin, 2012) and subsequently reduced to 2.5 hours in 2019 (Hart, 2019). Instead of using the submissive approach, such as forcing a user to select a more robust password or emailing the security announcement to the user, a more proactive approach should be taken. A multimodal biometrics-based authentication, grid-based authentication, or honey encryption can be further considered to address the limitation of password-based authentication.

## **6.2 SMS-Based One-Time Password (OTP)**

The majority of the selected banks rely heavily on SMS-based OTP to reset the login password and verify the requested transaction, which occupied 80%. The SMS-based OTP cannot withstand recent malware attacks, including man-in-the-middle (MITM) and man-in-the-browser (MITB) attacks and SSL stripping attacks. These attacks are capable of intercepting OTP sent to the mobile device.

## **6.3 Limitation of TLS/SSL mechanism**

Most of the fintech technologies in E-banking rely on TLS/SSL mechanisms to protect data transmission and communication with the user. TLS/SSL mechanisms are able to assure the properties of confidentiality, integrity, and authentication; however, they are still vulnerable to application-layer threats. Also, the conducted evaluation study revealed that only 20% of the selected banks are upgrading their TLS version to the latest TLS1.3, published in 2018. Also, the increased frequency and ferocity of phishing attacks, especially during the covid pandemic, have seen 65% of reported cases increase in Malaysia, calling for an effective and practical end-to-end encryption mechanism, including attribute-based encryption to address the bottleneck performance of recent public key infrastructure.

## **6.4 Quantum Safe Cryptographic Algorithm**

The result of the conducted evaluation study revealed that all banks rely on modern cryptographic algorithms such as RSA 2048 bits in generating the key and SHA256 with RSA in the signature algorithm. As RSA guaranteed that the 2048-bit key is adequate until 2030, the banking systems should implement a stronger key of 3072-bit within five years. Also, these modern cryptographic algorithms are constructed based on the number-theoretical approach, such as RSA built from the integer factorisation problem. They cannot withstand quantum attacks in the era of quantum computing.

## **ACKNOWLEDGMENT**

This work was supported by a Fundamental Research Grant Scheme from the Ministry of Higher Education Malaysia [KPT FRGS/1/2020/ICT07/UMS/02/1]. The authors very much appreciate the engagement of security experts from industry and academia. The authors also thank the anonymous reviewers of this manuscript for their careful reviews and constructive comment.

## **FUNDING AGENCY**

This research was supported by the Ministry of Higher Education Malaysia [KPT FRGS/1/2020/ICT07/UMS/02/1].

## REFERENCES

- Abualsauod, E. H., & Othman, A. M. (2020). A study of the effects of online banking quality gaps on customers' perception in Saudi Arabia. *Journal of King Saud University-Engineering Sciences*, 32(8), 536–542. doi:10.1016/j.jksues.2019.09.001
- Althobaiti, M. (2016). *Assessing usable security of multifactor authentication* [Doctoral dissertation]. University of East Anglia.
- Anoud, B.-H., Majdalweieha, M., & AlShamsia, A. (2019). Online authentication methods used in banks and attacks against these methods. *Procedia Computer Science*, 151, 1052–1059. doi:10.1016/j.procs.2019.04.149
- Bucko, J. (2017). Security of smart banking applications in Slovakia. *Journal of Theoretical and Applied Electronic Commerce Research*, 12(1), 42–52. doi:10.4067/S0718-18762017000100004
- Central Bank of Malaysia. (2020). *Risk management in technology (RMiT)*. [https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+\(RMiT\).pdf](https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+(RMiT).pdf)
- Cheng, C. (2014). Implement and research on electronic banking security assessment. *Applied Mechanics and Materials*, 687–691, 4507–4510. doi:10.4028/www.scientific.net/AMM.687-691.4507
- Choubey, J., & Choubey, B. (2013). Secure user authentication in Internet banking: A qualitative survey. *International Journal of Innovation, Management and Technology*, 4(2), 198–203. doi:10.7763/IJIMT.2013.V4.391
- Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A. (2014). Security analysis of mobile two-factor authentication schemes. *Intel Technology Journal*, 18(4), 138–161.
- Goodin, D. (2012). 25-GPU cluster cracks every standard Windows password in < 6 hours. *Ars Technica*. <https://cacm.acm.org/news/158480-25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/fulltext>
- Hart, N. (2019). HashCat can now crack an eight-character Windows NTLM password hash in under 2.5 hours. *Information Security Buzz*. <https://informationsecuritybuzz.com/hashcat-can-now-crack-an-eight-character/>
- ISO/IEC JTC 1/SC27. (2019). *Information technology – security techniques – entity authentication assurance framework*.
- Kiljan, S., Simoens, K., De Cock, D., Van Eekelen, M., & Vranken, H. (2016). A survey of authentication and communications security in online banking. *ACM Computing Surveys*, 49(4), 1–35. doi:10.1145/3002170
- Kiljan, S., Vranken, H., & Eekelen, M. V. (2018). Evaluation of transaction authentication methods for online banking. *Future Generation Computer Systems*, 80, 430–447. doi:10.1016/j.future.2016.05.024
- Krol, K., Philippou, E., Cristofaro, E. D., & Sasse, M. A. (2015). They brought in the horrible key ring thing! Analysing the usability of two-factor authentication in UK online banking. *Proceedings of NDSS Symposium*. doi:10.14722/usec.2015.23001
- Muller, J. (2020). *Volume of mobile banking transactions in Malaysia 2011–2019*. Statista Banks and Financial Services.
- Nenadic, A., Zhang, N., Yao, L., & Morrow, T. (2007). Levels of authentication assurance: An investigation. *Proceedings of the Third International Symposium on Information Assurance and Security*, 155–158. doi:10.1109/ISIAS.2007.4299767
- NIST Special Publication (SP) 800-63-2, *Electronic Authentication Guideline*. (2013). National Institute of Standards and Technology.
- NIST Special Publication (SP) 800-63 *Digital Identity Guidelines*. (2017). National Institute of Standards and Technology.
- Park, K. C., Shin, J. W., & Lee, B. G. (2014). Analysis of authentication methods for smartphone banking service using ANP. *Transactions on Internet and Information Systems (Seoul)*, 8(6), 2087–2103. doi:10.3837/tiis.2014.06.016

Sinigaglia, F., Carbone, R., & Costa, G. (2017). Strong authentication for e-banking: A survey on European regulations and implementations. *Proceedings of the International Joint Conference on e-Business and Telecommunications*, 480–485. doi:10.5220/0006438504800485

Sinigaglia, F., Carbone, R., Costac, G., & Zannone, N. (2020). A survey on multi-factor authentication for online banking in the wild. *Computers & Security*, 95(101745), 101745. doi:10.1016/j.cose.2020.101745

Srinivas, V., & Wadhwani, R. (2018). *The value of online banking channels in a mobile-centric world*. Deloitte Insights.

Subsorn, P., & Limwiriyakul, S. (2012). A comparative analysis of Internet banking security in Thailand: A customer perspective. *Procedia Engineering*, 32, 260–272. doi:10.1016/j.proeng.2012.01.1266

Syamsuddin, I., & Hwang, J. (2009). The application of AHP model to guide decision makers: A case study of e-banking security. In *Proceedings of the 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*. IEEE. doi:10.1109/ICCIT.2009.251

## APPENDIX

**Table A1.**  
**Summary of Authentication Factor (C1)**

Security Level	Score	Descriptors
Level 1	Adequate	<ul style="list-style-type: none"> <li>• Little confidence in the usage of authentication factor in asserted identity's validity</li> <li>• Only limited to knowledge factor</li> <li>• Single-factor authentication</li> </ul>
Level 2	Competent	<ul style="list-style-type: none"> <li>• Some confidence in the usage of authentication factor in asserted identity's validity</li> <li>• Knowledge factor or inherence factor</li> <li>• Require a security image or security phrase</li> <li>• Two-factor authentication</li> </ul>
Level 3	Good	<ul style="list-style-type: none"> <li>• High confidence in the usage of authentication factor in asserted identity's validity</li> <li>• Combination of knowledge factor and ownership factor; or a combination of inherence factor and ownership factor</li> <li>• Multi-factor authentication</li> <li>• Limited to software token</li> </ul>
Level 4	Excellent	<ul style="list-style-type: none"> <li>• Very high confidence in the usage of authentication factor in asserted identity's validity</li> <li>• Combination of knowledge factor and ownership factor; or a combination of inherence factor and ownership factor</li> <li>• Multi-factor authentication</li> <li>• Limited to a hardware token</li> </ul>

**Table A2.**  
**Summary of Authentication Method for Login (C2)**

Security Level	Score	Descriptors
Level 1	Adequate	<ul style="list-style-type: none"> <li>• Something the user knows, such as a password or PIN</li> </ul>
Level 2	Competent	<ul style="list-style-type: none"> <li>• Something the user is, such as fingerprint, iris, voice, or face; or something the user knows, such as a password or PIN</li> <li>• With the combination of a security image or security phrase</li> </ul>
Level 3	Good	<ul style="list-style-type: none"> <li>• Software token</li> <li>• Activated by knowledge factor (password/PIN) or inherent factor (fingerprint/iris/voice/face) to generate a one-time password (OTP)</li> </ul>
Level 4	Excellent	<ul style="list-style-type: none"> <li>• Hardware token</li> <li>• Activated by knowledge factor (password/PIN) or inherent factor (fingerprint/iris/voice/face) to generate an OTP</li> </ul>

**Table A3.**  
**Summary of Password Management and Policy (C3)**

Security Level	Score	Descriptors
Level 1	Adequate	<ul style="list-style-type: none"> <li>• The password length is 6–7 characters</li> <li>• The password consists of at least two types of characters from uppercase alphabets, lowercase alphabets, numbers, and special characters</li> <li>• Example: ha2rry, pOTTEr</li> </ul>
Level 2	Competent	<ul style="list-style-type: none"> <li>• The password length is 8–11 characters</li> <li>• The password consists of at least three types of characters from uppercase alphabets, lowercase alphabets, numeric, and special characters; the three types of characters are mixed up in no order.</li> <li>• Example: pO2T3ter, pO@Tt#er</li> </ul>
Level 3	Good	<ul style="list-style-type: none"> <li>• The password length is 12–15 characters</li> <li>• The password consists of uppercase alphabets, lowercase alphabets, numeric, and special characters, the different types of characters are mixed up in no order</li> <li>• The uppercase alphabets are not at the beginning of the password</li> <li>• The numeric and special characters are not at the end of the password</li> <li>• Example: h@RR#yP0Tter</li> </ul>
Level 4	Excellent	<ul style="list-style-type: none"> <li>• The password length is 16 or more characters</li> <li>• The password consists of the uppercase alphabets, lowercase alphabets, numbers, and special characters; the different types of characters are mixed up in no order.</li> <li>• The uppercase alphabets are not at the beginning of the password</li> <li>• The numeric and special characters are not at the end of the password</li> <li>• Example: l@ve#aRRy4P0Tter</li> </ul>



**Table A4.**  
**Summary of Password Recovery Management and Policy (C4)**

Security Level	Score	Descriptors
Level 1	Adequate	<ul style="list-style-type: none"> <li>• The password is changed at least once every 60 days</li> <li>• The credit or debit card number, username, and PIN are required to reset the password if the password is forgotten</li> <li>• The credit or debit card number, username, PIN and old password are required to reset the password if the password is not forgotten</li> <li>• A password hint is showed when the user forgot the password</li> <li>• A password-strength meter to examine the password strength is not provided</li> </ul>
Level 2	Competent	<ul style="list-style-type: none"> <li>• The password is changed at least once every 90 days</li> <li>• The credit or debit card number, username, PIN, and OTP are required to reset the password if the password is forgotten</li> <li>• The credit or debit card number, username, PIN, OTP from SMS, and old password are required to reset the password if the password is not forgotten</li> <li>• CAPTCHA is implemented</li> <li>• There is no password hint showing when the user forgot the password</li> <li>• A password-strength meter to examine the password strength is provided</li> </ul>
Level 3	Good	<ul style="list-style-type: none"> <li>• The password is changed at least once every 12 months</li> <li>• The credit or debit card number, username, PIN, and OTP are required to reset the password if the password is forgotten</li> <li>• The credit or debit card number, username, PIN, OTP from software token, and old password are required to reset the password if the password is not forgotten</li> <li>• CAPTCHA is implemented</li> <li>• At least one security question or identity proofing information associated with the party whose identity is being authenticated is asked when resetting the password</li> <li>• There is no password hint showing when the user forgot the password</li> <li>• A password-strength meter to examine the password strength is provided</li> </ul>
Level 4	Excellent	<ul style="list-style-type: none"> <li>• The password is not changed periodically unless there is a piece of evidence shown that the account was hacked, or the password is forgotten</li> <li>• The credit or debit card number, username, PIN, and OTP are required to reset the password if the password is forgotten</li> <li>• The credit or debit card number, username, PIN, OTP, and old password are required to reset the password if the password is not forgotten</li> <li>• CAPTCHA is implemented</li> <li>• At least one security question is asked when resetting the password</li> <li>• At least one identity proofing information that associated with the party whose identity is being authenticated is required when resetting the password, it could be the identity card number, phone number, or postcode</li> <li>• There is no password hint showing when the user forgot the password</li> <li>• A password-strength meter to examine the password strength is provided</li> </ul>

**Table A5.**  
**Summarization of Transaction Verification (C5)**

Security Level	Score	Descriptors
Level 1	Adequate	<ul style="list-style-type: none"> <li>• An OTP is sent to the mobile phone, which is registered to the party whose identity is being authenticated via SMS</li> </ul>
Level 2	Competent	<ul style="list-style-type: none"> <li>• An OTP is sent to the mobile phone, which is registered to the party whose identity is being authenticated via SMS</li> <li>• The requesting party demonstrates its inherent biometric characteristics, or it knows some unique data associated with the party whose identity is being authenticated, such as the fingerprint, iris, voice, face, password, or PIN</li> </ul>
Level 3	Good	<ul style="list-style-type: none"> <li>• The requesting party demonstrates that it has some unique item associated with the party whose identity is being authenticated, which is a software token</li> <li>• Activated by a knowledge factor (password or PIN) or an inherent factor (fingerprint, iris, voice, or face) to generate an OTP</li> </ul>
Level 4	Excellent	<ul style="list-style-type: none"> <li>• The requesting party demonstrates that it has some unique item associated with the party whose identity is being authenticated, which is a hardware token</li> <li>• Activated by a knowledge factor (password or PIN) or an inherent factor (fingerprint, iris, voice, or face) to generate an OTP</li> </ul>

**Table A6.**  
**Summarization of Login Attempt Limitations (C6)**

Security Level	Score	Descriptors
Level 1	Adequate	<ul style="list-style-type: none"> <li>• The bank provides at least 10 times of login attempts</li> </ul>
Level 2	Competent	<ul style="list-style-type: none"> <li>• The bank provides at most five times of login attempts. If the login fails in five attempts, the account will be locked and require the administrator to unlock</li> </ul>
Level 3	Good	<ul style="list-style-type: none"> <li>• The bank provides at most three times of login attempts. If the login fails in three attempts, the account will be locked and require the administrator to unlock</li> </ul>
Level 4	Excellent	<ul style="list-style-type: none"> <li>• The bank provides at most three times of login attempts. If the login fails in three attempts, the account will be locked and require the administrator to unlock</li> <li>• CAPTCHA is implemented before the login attempts</li> </ul>

**Table A7.**  
**Summarization of Reauthentication (C7)**

Security Level	Score	Descriptors
Level 1	Adequate	<ul style="list-style-type: none"> <li>• Reauthentication should be repeated once per 12 hours during an extended usage session</li> <li>• Reauthentication is carried out if the account idles for longer than 30 minutes</li> </ul>
Level 2	Competent	<ul style="list-style-type: none"> <li>• Reauthentication should be repeated once per 12 hours during an extended usage session</li> <li>• Reauthentication is carried out if the account idles for less than or equal to 30 minutes</li> </ul>
Level 3	Good	<ul style="list-style-type: none"> <li>• Reauthentication should be repeated once per 12 hours during an extended usage session</li> <li>• Reauthentication is carried out if the account idles for less than or equal to 15 minutes</li> </ul>
Level 4	Excellent	<ul style="list-style-type: none"> <li>• Reauthentication should be repeated once per 12 hours during an extended usage session</li> <li>• Reauthentication is carried out if the account idle for less than or equal to five minutes</li> </ul>

**Table A8.**  
**Summary of Types of Encryption Protocol and Certificate Authority (C8)**

Security Level	Score	Descriptors
Level 1	Adequate	<ul style="list-style-type: none"> <li>• Transport Layer Security (TLS) 1.2 with the domain validated (DV) certificate is employed</li> <li>• The address starts with “https”</li> <li>• A green padlock sign is shown before the address</li> <li>• The organisation’s name is not shown in the certificate</li> </ul>
Level 2	Competent	<ul style="list-style-type: none"> <li>• Transport Layer Security (TLS) 1.2 with the organisation validated (OV) certificate is employed</li> <li>• The address starts with “https”</li> <li>• A green padlock sign is shown before the address</li> <li>• The organisation’s name is shown in the certificate</li> </ul>
Level 3	Good	<ul style="list-style-type: none"> <li>• Transport Layer Security (TLS) 1.2 with the extended validated (EV) certificate is employed</li> <li>• The address starts with “https”</li> <li>• A green address bar is shown before the address, which consists of the green padlock, the organisation’s name, and the country code</li> <li>• The organisation’s name is shown in the certificate</li> </ul>
Level 4	Excellent	<ul style="list-style-type: none"> <li>• Transport Layer Security (TLS) 1.3 with the extended validation (EV) certificate is employed</li> <li>• The address starts with “https”</li> <li>• A green address bar is shown before the address, which consists of the green padlock, the organisation’s name, and the country code</li> <li>• The organisation’s name is shown in the certificate</li> </ul>

*Tan Soo Fun is a senior lecturer at the Universiti Malaysia Sabah School of Computing and Informatics. She completed her PhD in 2017 at Universiti Sains Malaysia. She received her Bachelor of Information Technology degree in e-commerce and Master of Science in Computer Science from Universiti Malaysia Sabah in 2006 and 2009, respectively. Her research interest includes cryptography and information and network security. She has over 30 publications, including book chapters, journals, technical reports, and proceedings and has received seven research grants in related fields. She is a certified IPv6 Network Engineer, certified IPv6 Security Engineer, Huawei Certified ICT Professional (HCIP), and IBM Certified Academic Associate.*

*Gwo Chin Chung earned the Bachelor of Electronics Engineering (Hons.) degree in telecommunications at Multimedia University, Malaysia, in 2005 and a Master of Engineering Science degree from the same university in 2009. Chung is currently a lecturer on the Faculty of Engineering of Multimedia University in Malaysia, conducting research in wireless communication, especially in digital signal processing, interference suppression, IoT, and machine learning.*