Journal of Cases on Information Technology
Volume 25 • Issue 1

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

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. Subsorn 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	Subsorn 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