Journal of Harbin Engineering University
ISSN: 1006-7043
Vol 44 No. 11
November 2023

Adoption of Digital Identity in Malaysia Financial Markets: Moderating Role of Fear of Cyberattacks

Pavitira Manogaran[1]*, Teoh Ai Ping[2], Allan Thomas[3]
[1]Faculty of Hospitality, Tourism and Wellness, UniversitiMalaysia Kelantan, Malaysia.
[2]Graduate School of Business, Universiti Sains Malaysia, Malaysia.
[3]Department of Agricultural Extension Education, Kerala Agricultural University, India.

Abstract
Cybersecurity remains a paramount concern in Malaysian financial markets, with the ever-evolving threat landscape necessitating vigilant measures to safeguard sensitive data and infrastructure. Among many technologies, digital identity has been identified as an essential technology to improve cybersecurity issues and thus is increasingly gaining both practitioners' and researchers' attention. The study investigates the adoption of digital identity among tech-savvy financial market participants and its relationship with the fear appeal theory, particularly emphasizing the moderating role of fear of cyberattacks. We have used a questionnaire survey method to collect data from 361 tech-savvy financial market participants. The data analysis shows that the response efficacy, self-efficacy, transparency, and fear of cyberattacks positively influence digital identity adoption. The study further tested the moderating effect of fear of cyberattacks. Our results show that fear of cyberattacks strongly moderates the link between perceived vulnerability and adoption, as well as self-efficacy and adoption. The study provides insights into the application of intelligent systems in the financial sector, offering practical guidance for enhancing digital identity adoption and advocating for measures to bolster cybersecurity practices among financial market participants.

Keywords- Digital Identity, Fear of Cyberattacks, Tech-Savvy, Financial Market Participants, Malaysia

1. Introduction

In the dynamic landscape of Malaysia's digital financial markets, an extraordinary transformation has taken place, one driven by the proliferation of online banking services, mobile applications, and innovative financial technologies (Law, Khair-Afham&Trinugroho, 2023; Chong, Ong & Tan, 2021). This digital revolution has empowered consumers to seamlessly manage their accounts, conduct secure transactions, and access various financial services through digital platforms. Simultaneously, the emergence of digital wallets and electronic payment platforms such as GrabPay, Boost, and Touch 'n Go eWallet has revolutionized cashless transactions, transcending the boundaries of online and offline experiences (Loh, Lee & Leong, 2022).

Malaysia's financial sector has also been the fertile ground for fintech innovations, boasting peer-to-peer lending platforms, robo-advisors, and digital investment services that have bestowed Malaysians with an array of financial management tools (Karim, Naz, Naeem &Vigne, 2022). This transformation has been further facilitated by a well-established regulatory framework that balances innovation with security and consumer protection (Oseni, Adewale & Zain, 2016).

Nonetheless, this digital renaissance has cast a long shadow, as it has brought forth a surge in cyberattacks and scams, especially during the crucible of the COVID-19 pandemic (Wong et al., 2022). Phishing scams have preyed upon the growing dependence on online transactions, while investment scams, ransomware attacks, and insider threats have become formidable adversaries (Al-Musib, Al-Serhani, Humayun &Jhanjhi, 2021; Zahra, Chishti, Baba & Wu, 2022). In response, regulatory bodies like the Securities Commission Malaysia (SC) and Bank Negara Malaysia (BNM) have launched valiant efforts, issuing guidelines and orchestrating public awareness campaigns to educate Malaysians about the lurking specter of cybercrime. However, despite these efforts, the specter remains, and Malaysia's financial markets require further

fortifications (Moghavvemi, Mei, Phoong&Phoong, 2021).

To confront this ever-evolving challenge, this study endeavors to illuminate the potential of digital identity in the fortress against cyber threats. Digital identity, encompassing biometrics like iris scans, facial recognition, fingerprints, retina scans, voice authentication, and signature verification, stands as a formidable sentinel, capable of differentiating individuals in the digital realm (Sim, Asmuni, Hassan & Othman, 2014). It not only offers enhanced security through advanced authentication methods but also acts as a sentinel against identity theft and fraud, streamlining the onboarding process and augmenting user experiences across industries (Mishra, Alzoubi, Anwar & Gill, 2022; Careja&Tapus, 2023; Merlo, Pio, Giusto &Bilancia, 2023).

The value of this innovation becomes particularly pronounced in Malaysia's diverse geographic landscape, ensuring accessibility to financial services nationwide. Financial institutions, too, reap the benefits through cost reductions and streamlined adherence to regulatory standards. Digital identity's proactive monitoring capabilities are a bulwark against fraud, promoting international trade and financial inclusion (Sule, Zennaro& Thomas, 2021). Furthermore, it allows individuals to control their data privacy and enables precise risk assessment, enhancing lending decisions (Sahmim, Gharsellaoui&Bouamama, 2019). As Malaysia's financial sector embraces digital transformation, robust digital identity solutions emerge as the linchpin for a secure, efficient, and sustainable financial ecosystem (Manogaran & Ping, 2022).

The success stories of digital identity implementations in nations such as Singapore, South Korea, and Japan underscore the potential benefits that stem from strong government initiatives, regulatory frameworks, and public-private partnerships. These countries have harnessed digital identity to bolster security, streamline public services, and instill trust in digital transactions (Woods, Bunnell & Kong, 2023; Sullivan, 2014; Voisin et al., 2021). In stark contrast, Estonia's e-residency program and India's Aadhaar system have notched notable achievements in providing secure digital identities that foster business and financial inclusion. This global diversity underscores the pivotal role of digital identity as a catalyst for economic growth and innovation (Sullivan & Burger, 2017; Rao & Nair, 2019; Addo &Senyo, 2021).

In the ever-intensifying shadow of cyber threats, this study provides invaluable insights into the adoption of digital identity among tech-savvy financial market participants. It simultaneously delves into the moderating role of fear in the face of these cyberattacks. By doing so, this research lays down a path for policymakers, regulatory bodies, and financial institutions to navigate the treacherous waters of digital identity adoption, taking into account the ever-present specter of cyberattacks. It seeks to fill critical research gaps in Malaysia's digital transformation, particularly within the financial markets, where the embrace of secure digital identities is increasingly indispensable.

As Malaysia charts its course through the digital frontier, this research endeavors to contribute to both academia and industry practitioners. It offers actionable insights that can inform policy decisions and ultimately work to create a more secure and efficient digital landscape within the nation's financial markets. The objective of this study is clear:

• *To investigate the moderating role of fear of cyberattacks on perceived vulnerability, response efficacy, self-efficacy, and transparency concerning digital identity adoption among tech-savvy financial market participants.*

Through this study, we aim to illuminate the path toward a fortified digital financial landscape empowered by digital identity, where the specter of cyberattacks is met with resilience and preparedness.

2. Research Backgroundand Hypotheses Development

2.1. Background Study on Digital Identity

In today's digitally charged world, the concept of digital identity has surged to the forefront, transforming how we engage with the online realm. At its essence, digital identity encompasses the unique attributes, credentials, and personal information individuals wield to validate their

presence in digital interactions (Smith, 2019). It is the virtual reflection of an individual's identity, granting them secure access to various online services.

A cast of crucial components takes center stage within the intricate architecture of digital identity systems. Identity providers (IdPs) verify and authenticate users' identities. These providers can range from government agencies and financial institutions to private companies offering authentication services. Simultaneously, users yearn for access to digital services, and in this quest, relying parties (RPs) step into the limelight, representing the entities or services users seek to engage with.

The ascendancy of the digital identity concept coincided with the meteoric rise of internet usage. It quickly became indispensable for ensuring secure online transactions, safeguarding personal data, and participating in the digital economy. Armed with their digital identities, individuals could confidently navigate the realms of online banking, e-commerce, and social media while maintaining the sanctity of their personal information (Chen & Zhao, 2012).

As digital identity technologies evolved, a rich tapestry of authentication methods unfolded. These methods span from the traditional username-password combinations to the sophisticated realms of two-factor authentication (2FA), biometrics featuring fingerprint and facial recognition, and the deployment of hardware tokens. These innovations strike a delicate balance between security and user convenience, effectively addressing the challenge of preserving sensitive information in an increasingly interconnected world (Alzahrani et al., 2020).

Nevertheless, significant concerns loom large within this digital identity landscape, casting shadows on the horizon. These concerns are multifaceted, revolving around privacy, security, and data management issues. A central theme in these discussions is the imperative of ensuring that individuals retain control over their digital identities and the usage of their data (De Cristofaro et al., 2012). Furthermore, the relentless surge in cyberattacks and incidents of identity theft has accentuated the exigency for robust digital identity solutions (Finklea et al., 2020).

In light of this backdrop, our study embarks on a journey to explore the adoption of digital identity within the realm of tech-savvy financial market participants in Malaysia. We delve into the intricate layers of digital identity, dissecting its various components and authentication methods. Our objective is to unveil the pivotal role of digital identity in fortifying security and trust within the digital realm. In doing so, we aim to offer valuable insights that resonate deeply within the Information Systems community, shedding light on the transformative power of digital identity in safeguarding our digital existence.

2.2. Theoretical Background& Hypotheses Development

Fear appeal theorystands as a venerable framework, offering invaluable insights into the complex dynamics of individuals' behavior (Truong & Truong, 2022). With its history spanning over half a century, this theory forms the bedrock upon which we explore the intricate psychology underlying encounters with groundbreaking technological innovations. Within the dynamic landscape of digital identity adoption in financial markets, a tapestry of related theories and models, including the drive reduction theory (Hovland, Janis & Kelley, 1953), the parallel response model, parallel process model (Leventhal, Watts & Pagano, 1967), extended parallel process model (Witte, 1992), and protection motivation theory (Rogers, 1975), have become steadfast tools for dissecting the multifaceted realm of fear appeals and their profound implications.

As artfully elucidated by Witte and Allen (2002), fear appeals emerge as persuasive messages meticulously crafted to invoke fear by portraying personally significant threats, all while offering pragmatic solutions for averting these looming perils. At their core, fear appeals serve as potent messages engineered to compel individuals into proactive responses against perceived threats, a concept acutely relevant in digital identity adoption within the financial sector (Williams, 2012).

Delving into the fear appeal framework, we find fear characterized as a subdued agitation accompanied by an adverse emotional response (Witte, 1998). This definition encompasses the

pivotal concepts of perceived threat and perceived efficacy, inextricably linked to the protection motivation theory. In line with Chen (2016), the perceived threat surfaces as an external stimulus beckoning message recipients to acknowledge susceptibility to negative scenarios or adverse outcomes. The facets of perceived danger encompass perceived severity and perceived vulnerability, which are intricately interwoven (Peters et al., 2013).

In this framework, perceived efficacy emerges as an individual's unwavering belief in the feasibility of adopting the suggested actions within a message to mitigate the perceived threat (Popova, 2012). Perceived efficacy encompasses the duality of response efficacy and self-efficacy, each integral (Popova, 2012). Within digital identity adoption, the fear appeal theory emerges as remarkably effective when the zenith of perceived efficacy and threat is reached. The fervor of the response to fear appeals hinges primarily on the perceived threat, while the very nature of the response pivots on the perceived efficacy (Witte, 1992).

Witte's pioneering work in 1994 ushered in empirical testing of the Extended Parallel Process Model (EPPM), bearing witness to its widespread acceptance. Within this EPPM framework, the emotional cadence of fear is inextricably tethered to fear control responses, distinguishing itself from danger control responses. Cognitions regarding the recommended response find their home in danger control, diverging from fear control responses. Crucially, when efficacy beliefs stand unwavering, the perceived threat mediates between fear and behavior, forging a path to successful outcomes. As cognitive elements steer us toward fear appeals resulting in triumph, fear control mechanisms come to the fore when the emotional aspect of fear reigns supreme, leading to appeals centered around potential failure or reactive behavior (Witte, 1992).

From a pragmatic standpoint, fear appeals wield formidable persuasive potential, particularly within the EPPM framework. Their efficacy is most pronounced when they summon forth elevated perceptions of threat and fear, harmonized with robust convictions of efficacy regarding a recommended course of action (Popova, 2012). Elevated levels of danger and efficacy stoke the flames of adoption, igniting adaptive behavior across actions and decision-making processes (Witte, 1992). This theory takes on profound relevance in digital identity, given the mounting concerns surrounding cyberattacks and the compelling need for financial market participants to embrace secure digital identity practices (Vrhovec&Mihelič, 2021).

The fear appeal theory and its concomitant models offer a sturdy and illuminating framework for comprehending the intricate psychological underpinnings of digital identity adoption within the ranks of financial market participants. Armed with an understanding of fear, threat, and efficacy, financial institutions and policymakers have the tools to craft persuasive communication strategies that effectively address individuals' concerns. These strategies are the catalysts needed to inspire the secure adoption of digital identity in the financial sector, safeguarding its future amidst the ever-evolving technological landscape.

Perceived vulnerability to threat refers to users' subjectively estimated probability that a security threat will occur. This study defines perceived vulnerability as the extent to which users believe they are likely to experience security threats to their computing devices[54]. Fitness device users care more about perceived vulnerability regarding wearable technology in healthcare [16]. Health information privacy concerns are positively affected by perceived vulnerability [67]. The following hypothesis is posited:

H1. Perceived vulnerability positively influences digital identity adoption among tech-savvy financial market participants.

Recent research has continued to support the importance of response efficacy in predicting new technology acceptance. For example, a study by Rahi et al. (2021) and Zhang et al.[67] found that response efficacy significantly predicted individuals' intention to use mobile health apps. Another study by Wang, Wong, Chen,and Yuen[59] found that response efficacy significantly predicted individuals' intention to use technology-dependent shopping. Additionally, Li, Li, and Fu[32] found that response efficacy significantly predicted individuals' intention to use contact tracing mobile applications during theCoronavirus 2019 (COVID-19) pandemic. These findings suggest that

response efficacy remains crucial in determining individuals' intention to adopt new technology, even in the context of emerging technologies and unexpected events.The following hypothesis is posited:

H2. Response efficacy positively influences digital identity adoption among tech-savvy financial market participants.

Recent research has also highlighted the importance of self-efficacy in predicting new technology acceptance. A study by Wang and Liu (2018) found that self-efficacy significantly predicted individuals' intention to use mobile payment technology. Similarly, a Hu et al. (2019) study found that self-efficacy significantly predicted individuals' intention to use smart home technology. Additionally, a study by Zhang et al.[67] found that self-efficacy significantly predicted individuals' intention to use mobile health apps. These findings suggest that individuals' confidence in their ability to use new technology plays a crucial role in their intention to adopt and use it. The following hypothesis is posited:

H3. Self-efficacy positively influences digital identity adoption among tech-savvy financial market participants.

Transparency is also an essential factor in predicting new technology acceptance. Cheng, Hou, and Mou[13] found that transparency significantly predicted individuals' intention to use ride-sharing services. Similarly, Qin et al. (2020) found that transparency significantly predicted individuals' intention to use autonomous vehicles. Additionally, a study by Chen and Pu (2021) found that transparency significantly predicted individuals' intention to use smart healthcare technology. These findings suggest that individuals are more likely to adopt and use new technology when they clearly understand how it works and what data it collects. The following hypothesis is posited:

H4. Transparency positively influences digital identity adoption among tech-savvy financial market participants.

Fear of cyberattacks is an individual's level of fear when confronted with a cyberattack [58]. It was derived from the EPPM model based on the fear appeal theory [63]. Developed countries are concerned because cyberattacks pose a significant economic risk [40] and raise personal anxiety. After all, it is viewed as a danger to individuals and organizations[8].

Cyberattacks are becoming more sophisticated and complex, and the severity of cyberattacks increases to the point where they cause a financial collapse and destroy companies' reputations ([15]. Cyberattacks are viewed cautiously since hackers steal critical data and information, risking an organization's integrity[56]. A common reaction from someone who is the victim of a cyberattack is apprehension. In contrast, studies also found that the fear of a cyberattack is unavoidable and beneficial because it motivates civilians to take preventative measures and avoid catastrophic events [24].The following hypothesis is posited:

H5. Fear of cyberattacks positively influences digital identity adoption among tech-savvy financial market participants.

Governments worldwide develop action plans to use digital technology with good governance and autonomous control to reduce cyberattacks [2]. Digital identity is among the most successful initiatives worldwide. The fear appeal has been researched in various settings, including COVID-19 prevention [45], travel intention [4], anti-speeding intention [10], and HPV vaccination [9]. Fear plays a minor influence in technological studies, particularly in identification and authenticity [58]. This study addresses its role as a moderator to identify its significance in adoption. The following hypotheses are posited:

H6: Fear of cyberattacks strengthens the influence of perceived vulnerability on digital identity adoption among tech-savvy financial market participants.

H7: Fear of cyberattacks strengthens the influence of response efficacy on digital identity adoption among tech-savvy financial market participants.

H8: Fear of cyberattacks strengthens the influence of self-efficacy on digital identity adoption among tech-savvy financial market participants.

H9: Fear of cyberattacks strengthens the influence of transparency on digital identity adoption among tech-savvy financial market participants.

2.3. Theoretical Framework

Fear appeal theory is the foundational framework for understanding the role of fear, perceived

vulnerability, response efficacy, self-efficacy, transparency and their influence on behavior. This theoryprovides insights into how fear can be harnessed to motivate financial market participants to take action against perceived threats. It helps explain how messages that invoke fear can lead to behavioral responses to mitigate the perceived threat. In this framework, fear of cyberattacks plays a moderating role in influencing these relationships.The theoretical framework is depicted in Figure 1. Four independent variables, perceived vulnerability, response efficacy, self-efficacy, and transparency, influence the dependent variable, digital identity adoption,which is investigated. The moderating role of fear of cyberattacks on these relationships is identified.

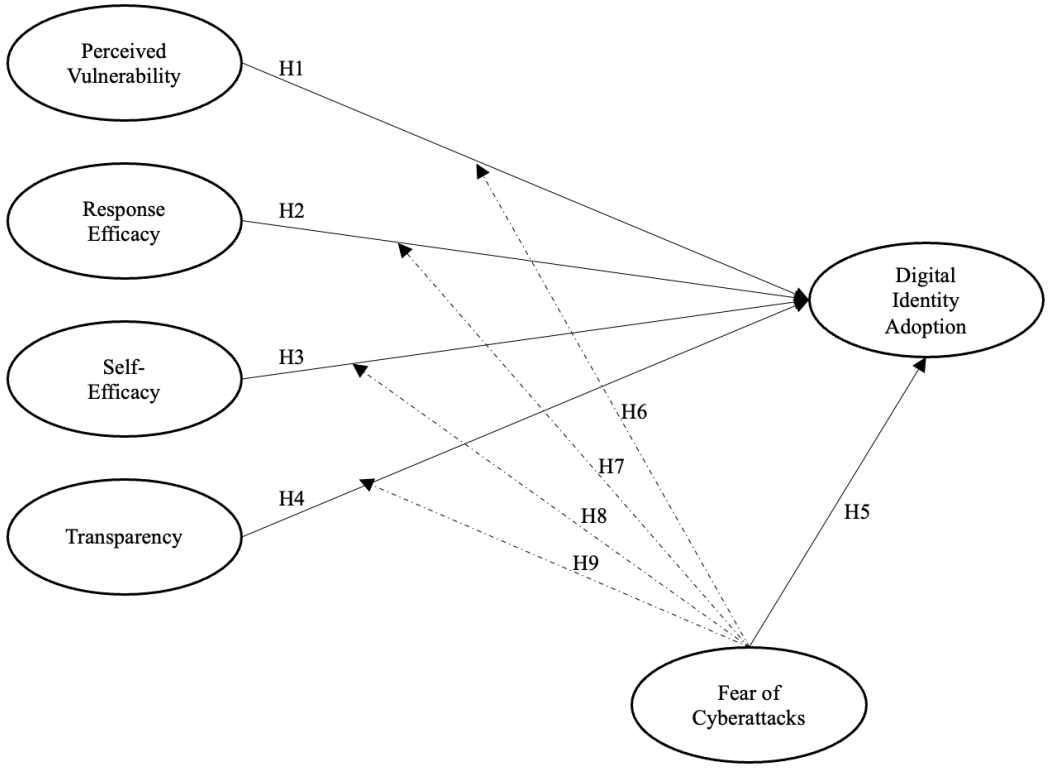

Fig.1. Theoretical Framework.

3. Methodology

The study collects data using a 7-point Likert scale online survey method. Data is analyzed using quantitative statistical tools such as IBM SPSS Statistics 26 and SmartPLS 3.2.9 software. Table 1 shows the variables, their operational definitions, and the sources of the variables adapted. The study focuses on financial market participants attached to Bursa Malaysia, as these participants are involved in the legal and authorized financial markets. The samples are determined using the non-random purposive sampling technique.

Table 1Measurement Variables.

No.	Variable Name	Operational Definition	Items	Source
1	Perceived Vulnerability	Perceived vulnerability is the individual's evaluation of the probability of menacing events.	3	Sun et al. [50]
2	Response Efficacy	Response efficacy is the individual's belief in the advantage obtained from their actions.	3	Sun et al. [50]
3	Self-Efficacy	Self-efficacy is the individual's capability and perception of their abilities to overcome or accomplish a behavior.	3	Sun et al. [50]
4	Transparency	Transparency is the extent to which an individual can clearly understand something used.	3	Venkatesh et al. [57]

No.	Variable Name	Operational Definition	Items	Source
5	Fear of Cyberattacks	Fear of cyberattacks is the level of the individual's emotional fear when facing cyberattacks	3	Vrhovec&Mihelič[58]
6	Digital Identity Adoption	Digital identity adoption is the degree to which a person consents to use the identity.	3	Chong, Ong, & Tan[14]

4. Findings And Discussion

Table 2 shows the details of the participants. The financial market participants are 21 to 40 years old, as these groups mainly participate in the digital platform. The majority of the market participants are men. All the market participants have an educational background. Figure 2 shows the measurement model of this paper.

Table 2 Detail of participants.

Category	Description	Frequency	Percent (%)
Gender	Male	220	60.9
	Female	141	39.1
Age	21-25 years old	101	28.0
	26-30 years old	89	24.7
	31-35 years old	79	21.9
	36-40 years old	92	25.5
Education	Diploma or equivalent	121	33.5
	Bachelor's degree	159	44.0
	Master's degree	51	14.1
	Ph.D./Doctorate	19	5.3
	Professional certificates	11	3.0

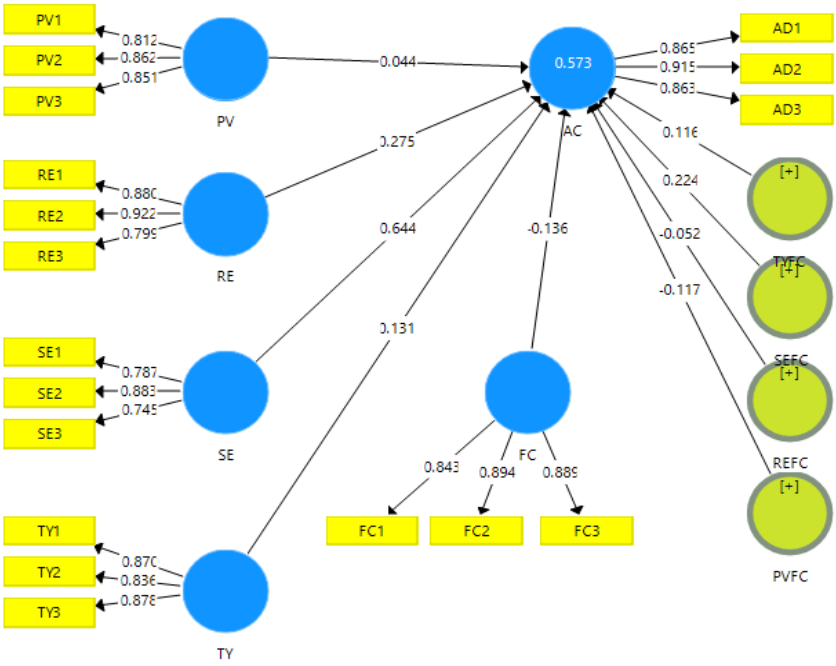

Fig.2. Measurement Model.

Table 3 shows the validity and reliability of the test results. The indicator loadings are higher than 0.708, which is acceptable. All Cronbach'salpha and composite reliabilityvalues are higher than 0.7, and the average variance extracted ishigher than 0.5 [46]. Hence, the indicators and variables are suitable for further analysis.

Table 3 Validity and reliability test results.

Items	Factor Loading	Cronbach's Alpha	Composite Reliability	AVE
Adoption				
AD1	0.865	0.857	0.913	0.777
AD2	0.915			
AD3	0.863			
Perceived Vulnerability				
PV1	0.812	0.802	0.879	0.709
PV2	0.862			
PV3	0.851			
Response Efficacy				
RE1	0.880	0.838	0.902	0.754
RE2	0.922			
RE3	0.799			
Self-Efficacy				
SE1	0.787	0.736	0.848	0.651
SE2	0.883			
SE3	0.745			
Transparency				
TY1	0.870	0.833	0.896	0.743
TY2	0.836			
TY3	0.878			
Fear of Cyberattacks				
FC1	0.843	0.855	0.908	0.767
FC2	0.894			
FC3	0.889			

The discriminant validity is measured using the heterotrait-monotrait (HTMT) ratio. As displayed in Table 4, all the values passed both the $HTMT_{.90}$[19] and $HTMT_{.85}$[28] thresholds, indicating that discriminant validity is accepted in this study.

Table 4 Discriminant validity.

Items	AD	FC	PV	RE	SE	TY
AD						
FC	0.321					
PV	0.297	0.672				
RE	0.552	0.773	0.502			
SE	0.815	0.611	0.452	0.698		

Items	AD	FC	PV	RE	SE	TY
TY	0.419	0.760	0.485	0.682	0.543	

Table 5 shows that four out of five hypotheses supported the structural model of this investigation. Based on the one-tailed test, the t-value was considered significant if the critical value was more than 1.64 [21].

Table5 Direct relationship results.

H	Path	Beta	Standard Deviation	T Statistics	P Values	5.0%	95.0%	Result
H1	PV -> AD	0.044	0.043	1.011	0.156	-0.027	0.116	Non-support
H2	RE -> AD	0.275	0.055	4.980	0.000	0.192	0.374	Support
H3	SE -> AD	0.644	0.044	14.766	0.000	0.572	0.717	Support
H4	TY -> AD	0.131	0.052	2.537	0.006	0.041	0.211	Support
H5	FC -> AD	-0.136	0.074	1.842	0.033	-0.250	-0.010	Support

Perceived vulnerability did not have a significant positive relationship with adoption (t-value=1.011<1.64, β=0.044, p-value=0.156>0.05). H1 is not supported.Response efficacy is found to have a significant positive relationship with adoption (t-value=4.980>1.64, β=0.275, p-value=0.000<0.05). H2 is supported.Self-efficacy is found to have a significant positive relationship with adoption (t-value=14.766>1.64, β=0.644, p-value=0.000<0.05). H3 is supported.Transparency is found to have a significant positive relationship with adoption (t-value=2.537>1.64, β=0.131, p-value=0.006<0.05). H4 is supported. Fear of cyberattacks is found to have a significant positive relationship with adoption (t-value=1.842>1.64, β=-0.136, p-value=0.033<0.05). H5 is supported.

Table6 Moderation results.

H	Path	Beta	Standard Deviation	T Statistics	P Values	5.0%	95.0%	Result
H6	FC -> (PV -> AD)	-0.117	0.050	2.371	0.009	-0.196	-0.033	Support
H7	FC -> (RE -> AD)	-0.052	0.074	0.706	0.240	-0.214	0.028	Non-support
H8	FC -> (SE -> AD)	0.224	0.056	3.976	0.000	0.161	0.346	Support
H9	FC -> (TY -> AD)	0.116	0.079	1.463	0.072	0.020	0.278	Non-support

The study's findings support H6, which suggests that the fear of cyberattacks increases the impact of perceived vulnerability on digital identity adoption among tech-savvy financial market participants. The t-value of 2.371 and p-value of 0.009 indicate that H6 is accepted, as it strengthens the influence of the link between perceived vulnerability and adoption. This finding contradicts Vrhovec and Mihelič's[58] argument that fear of cyberattacks does not affect perceived vulnerability and adoption. The study found that high levels of fear of cyberattacks significantly impact perceived vulnerability and adoption, while a decrease in fear weakens the relationship. This contributes to bridging the research gap in digital identity adoption. The study suggests that the more tech-savvy financial market participants fear cyberattacks, the more likely they are to adopt digital identities to protect themselves. Although perceived vulnerability did not directly influence digital identity adoption, the study found that the emotion of fear played a significant role in convincing tech-savvy financial market participants to adopt digital identity.

Based on the study's results, H7 was not supported, indicating that fear of cyberattacks did

not enhance the relationship between response efficacy and digital identity adoption among tech-savvy financial market participants. Although previous studies have explored the fear of cyberattacks as a moderator in various contexts, this study offers new insights into the relationship between response efficacy and adoption. The results indicate that the fear of cyberattacks did not significantly impact the perceived benefits of digital identity, as tech-savvy financial market participants were already willing to accept it due to its benefits. While fear did not play a significant role in influencing the relationship between response efficacy and adoption, this finding is still valuable, as it adds to the growing body of knowledge on the impact of fear appeals on adopting new technologies. Overall, the study underscores the importance of considering various factors, including fear, in promoting the adoption of digital identity among tech-savvy financial market participants.

According to H8, the fear of cyberattacks strengthens the impact of self-efficacy on digital identity adoption among tech-savvy financial market participants. The study's results support H8, as indicated by a t-value of 3.976 and a p-value of 0.000. The findings contribute to the research framework by bridging the gap in the literature on the relationship between self-efficacy and adoption and the moderating role of the fear of cyberattacks.Previous research has explored the fear of cyberattacks as a moderator in various contexts, but the relationship between self-efficacy and adoption has not been thoroughly investigated. High levels of fear of cyberattacks have a more significant impact on the link between self-efficacy and adoption. A decrease in fear of cyberattacks could weaken this relationship.The study highlights that tech-savvy financial market participants possess the necessary abilities to deal with digital identity adoption. However, the fear of cyberattacks substantially influences their decision to accept digital identity. This suggests that despite having the necessary skills and abilities, the fear of cyberattacks plays a significant role in the adoption process, which is crucial to be known amongst policymakers and organizations to consider when promoting digital identity adoption.

H9 proposed that the fear of cyberattacks enhances the influence of transparency on adopting digital identity among tech-savvy financial market participants. However, the findings of this study do not support H9, with a t-value of 1.463 and a p-value of 0.072, indicating that the fear of cyberattacks did not strengthen the relationship between transparency and adoption. While previous research has examined the fear of cyberattacks as a moderator in various contexts, it has not explored the relationship between transparency and adoption. The study found that the fear of cyberattacks did not significantly impact the relationship between transparency and adoption, regardless of whether the participants had a high or low fear. This represents a new finding in the existing body of knowledge. The results suggest that the transparency of the digital identity alone was sufficient for tech-savvy financial market participants to adopt it, and the influence of fear did not play a substantial role in their decision-making process.

5. Implications

Adopting digital identity solutions in financial markets represents a multifaceted challenge, intricately woven with the threads of technology trust and the looming specter of cyberattacks. This research endeavors to illuminate a pivotal aspect of this complex landscape: the moderating influence of fear emanating from cyber threats on the intentions of tech-savvy financial market participants to embrace digital identity solutions. In doing so, it highlights the critical imperative of comprehending and addressing cybersecurity concerns within this context.

Financial institutions and policymakers, at the heart of this transformation, stand to gain invaluable insights from this study. It underscores the pressing necessity to craft digital identity solutions with security as their cornerstone. The findings underscore the need to design robust technical systems and comprehensive regulations and guidelines that facilitate responsible adoption. In a world characterized by evolving threats, this research underscores that a two-pronged approach, combining technical resilience with a regulatory framework that nurtures adoption, is paramount.

However, the significance of this research extends beyond the boardrooms and legislative chambers. It emphasizes the pivotal role of organizations in this ecosystem. The essence of digital identity adoption lies in trust, both with customers and stakeholders. Organizations must invest in cybersecurity measures that go beyond the routine to cultivate this trust. Educationand training initiatives that enhance safe technology use should also be a cornerstone of this trust-building endeavor. This study advocates for a holistic approach, underlining the responsibilities of entities that offer digital identity solutions.

Theoretically, this research introduces a novel dimension to the discourse on digital identity adoption. It elucidates the underexplored impact of fear on this process, particularly the fear of cyberattacks. Delving into the emotional and psychological elements of technology adoption extends the boundaries of our understanding and enriches the existing body of knowledge. It magnifies the significance of considering not just the quantifiable elements of trust but also the intangible, yet potent, aspect of fear in molding individuals' intentions to embrace novel technology.

In the grand tapestry of technology adoption, this research highlights that the interplay between trust and fear is pivotal. These contrasting yet interdependent emotions sway the course of digital identity adoption. This interplay is the core of the findings, shedding light on the intricate psychology behind the decisions of tech-savvy financial market participants.

In sum, this research deepens our comprehension of the multifaceted dynamics of digital identity adoption in the financial sector. It offers guidance to decision-makers and policymakers, echoes the clarion call for cybersecurity fortification, and underscores the profound role of organizations in building trust. In theory, it broadens the horizons of our understanding, transcending the known boundaries and delving into the realm of human emotions. Ultimately, this research carves a path to a more secure, resilient, and enlightened digital ecosystem where trust and fear dance in intricate harmony.

6. Conclusion, Limitations, and Future Directions

In summary, this research unravels the intricate web of factors guiding digital identity adoption among tech-savvy financial market participants in Malaysia, underscoring the pivotal role of perceived severity, response efficacy, self-efficacy, and transparency in propelling adoption. The study also casts light on the moderating influence of fear within this adoption journey, particularly the fear of cyberattacks.

The practical implications of these findings reverberate across various domains, benefiting administrators, regulators, industry practitioners, governments, and society at large. They serve as a beacon for establishing robust cybersecurity measures and promoting secure and responsible technology adoption.

Nonetheless, it is important to acknowledge the study's limitations, including its specific focus on a particular technology domain and population. This narrow scope may temper the generalizability of the findings. Future research avenues should expand to encompass a broader spectrum of industries and diverse populations, offering a comprehensive understanding of how the fear of cyberattacks influences the adoption of new technologies.

As technology continues to evolve, new breeds of cyber threats may emerge, necessitating further exploration of their impacts on adoption behavior and strategies to mitigate them. Ultimately, this study serves as a foundational cornerstone for future research endeavors in digital identity adoption and cybersecurity, carving a path toward establishing a secure and reliable digital ecosystem.

Declaration of Competing Interest

The authors of this paper declare that they have no competing interests.

Authors Biography

Dr. Pavitira Manogaran completed her PhD at the Graduate School of Business, Universiti Sains Malaysia. Her research interests encompass the fascinating realms of business information systems and technology, smart cities and digital identities, reflecting her passionate dedication to advancing the understanding and practical applications in these fields. Building on her Master's in Business

Administration from the same esteemed university, her contributions are poised to leave a lasting impact on the ever-evolving landscape of business and technology integration.
https://orcid.org/0000-0002-3434-9505
pavitira_94@hotmail.com

Ts. Dr. Ai Ping Teoh is currently an Associate Professor and Doctor of Business Administration Program Manager at the Graduate School of Business, Universiti Sains Malaysia. She holds the qualifications of Doctor of Business Administration, Master of Science in Information Technology, and Bachelor of Accountancy (Hons.). She is also a Certified Risk and Compliance Management Professional and Professional Technologist (Cyber Security Technology). Her areas of specialization are Information Systems, Strategic Management, Cybersecurity, E-learning and Governance. Prior to joining USM, Dr. Teoh was a pioneer academic and Deputy Dean in the School of Business and Administration of a private University. Before embarking on a career in education, she had substantial industry experience in Enterprise Resource Planning, Information Systems and Enterprise Risk Management projects.
https://orcid.org/0000-0002-9267-9094

Dr. Allan Thomas currently holds the position of Professor and Head of the Department of Agricultural Extension Education at Kerala Agricultural University. His expertise includes soft skills training, research and extension work, making him a valuable asset for various training programs. His research primarily focuses on biodiversity extension, home gardens, riparian home garden agroecosystems, spatial and temporal design and assessment of rural and urban home gardens, behavioral dynamics, and resource-managed climate adaptation strategies within home garden farming systems. Dr. Thomas has successfully led multiple externally funded projects in these areas. Additionally, he serves as a mentor, guiding both post-graduate and doctoral students.

References

[1] Addo, A., &Senyo, P. K. (2021). Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion. Government Information Quarterly, 38(2), 101568.

[2] Al-Musib, N. S., Al-Serhani, F. M., Humayun, M., &Jhanjhi, N. Z. (2021). Business email compromise (BEC) attacks. Materials Today: Proceedings.

[3] Careja, A. C., &Tapus, N. (2023). Digital Identity Using Blockchain Technology. Procedia Computer Science, 221, 1074-1082.

[4] Chong, L. L., Ong, H. B., & Tan, S. H. (2021). Acceptability of mobile stock trading application: A study of young investors in Malaysia. Technology in Society, 64, 101497.

[5] Karim, S., Naz, F., Naeem, M. A., &Vigne, S. A. (2022). Is FinTech providing practical solutions to Small and Medium Enterprises (SMEs) in ASEAN countries?. Economic Analysis and Policy, 75, 335-344.

[6] Law, S. H., Khair-Afham, M. M., &Trinugroho, I. (2023). Financial inclusion and economic uncertainty in developing countries: The role of digitalization. Economic Analysis and Policy, 79, 786-806.

[7] Loh, X. M., Lee, V. H., & Leong, L. Y. (2022). Mobile-lizing continuance intention with the mobile expectation-confirmation model: An SEM-ANN-NCA approach. Expert Systems with Applications, 205, 117659.

[8] Manogaran, P., & Ping, T. A. (2022). Determinants of National Digital Identity Verification Platform Acceptance Among Young Investors in Malaysia. Journal of Governance and Integrity, 5(3), 308-316.

[9] Merlo, V., Pio, G., Giusto, F., &Bilancia, M. (2023). On the exploitation of the blockchain technology in the healthcare sector: A systematic review. Expert Systems with Applications, 213, 118897.

[10] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120, 102820.

[11] Moghavvemi, S., Mei, T. X., Phoong, S. W., &Phoong, S. Y. (2021). Drivers and barriers of mobile payment adoption: Malaysian merchants' perspective. Journal of Retailing and Consumer Services, 59, 102364.

[12] Oseni, U. A., Adewale, A., & Zain, N. R. B. M. (2016). Customers' perceptions on the dispute resolution clauses in Islamic finance contracts in Malaysia. Review of Financial Economics, 31, 89-98.

[13] Rao, U., & Nair, V. (2019). Aadhaar: governing with biometrics. South Asia: Journal of South Asian Studies, 42(3), 469-481.

[14] Sahmim, S., Gharsellaoui, H., &Bouamama, S. (2019). Edge computing: smart identity wallet-based architecture and user centric. Procedia Computer Science, 159, 1246-1257.

[15] Sim, H. M., Asmuni, H., Hassan, R., & Othman, R. M. (2014). Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. Expert systems with applications, 41(11), 5390-5404.

[16] Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. Technology in Society, 67, 101734.

[17] Sullivan, C. (2014). Protecting digital identity in the cloud: Regulating cross border data disclosure. Computer Law & Security Review, 30(2), 137-152.

[18] Sullivan, C., & Burger, E. (2017). E-residency and blockchain. computer law & security review, 33(4), 470-481.

[19] Voisin, C., Linden, M., Dyke, S. O., Bowers, S. R., Alper, P., Barkley, M. P., ... &Nyrönen, T. H. (2021). GA4GH Passport standard for digital identity and access permissions. Cell Genomics, 1(2).

[20] Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., &Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management, 66, 102520.

[21] Woods, O., Bunnell, T., & Kong, L. (2023). The state-led platformisation of financial services: Frictionless ecosystems and an expansive logic of “smartness” in Singapore. Geoforum, 146, 103849.

[22] Zahra, S. R., Chishti, M. A., Baba, A. I., & Wu, F. (2022). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining-based intelligence system. Egyptian Informatics Journal, 23(2), 197-214.

[23] Truong, D., & Truong, M. D. (2022). How do customers change their purchasing behaviors during the COVID-19 pandemic?. Journal of Retailing and Consumer Services, 67, 102963.

[24] Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). Communication and Persuasion: Psychological Studies of Obvious Change. New Haven, CT: Yale University Press

[25] Leventhal, H., Watts, J. C., & Pagano, F. (1967). Effects of fear and instructions of how to cope with danger. Journal of Personality and Social Psychology, 6(3), 313-321. https://psycnet.apa.org/doi/10.1037/h0021222.

[26] Witte, K., & Allen, M. (2002). A meta-analysis of fear appeals: Implications for effective public health campaigns. Health Education &Behavior, 27(5), 591-615. https://doi.org/10.1177/109019810002700506.

[27] Witte, K., & Morrison, K. (2000). Examining the influence of trait anxiety/repression sensitization of individuals' reactions to fear appeals. Western Journal of Communication, 64(1), 1-28. https://doi.org/10.1080/10570310009374661.

[28] Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change.Journal of Psychology, 91(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803.

[29] Witte. (1992). Putting the fear back into fear appeals: The extended parallel process model. Communication Monographs, 59(4), 329-349. https://www.uky.edu/~ngrant/CJT780/readings/Day%209/Witte1992.pdf.

[30] Witte. (1994). Fear control and danger control: A test of the extended parallel processmodel (EPPM). Communication

Monographs, 61(2), 113-134.https://eric.ed.gov/?id=EJ487675.

[31] Williams, K. C. (2012). Fear appeal theory. Research in Business and EconomicsJournal, 5(1), 1-21. https://www.aabri.com/manuscripts/11907.pdf.

[32] Chen, M. F. (2016). Impact of fear appeals on pro-environmental behavior and crucial determinants. International Journal of Advertising, 35(1), 74-92. https://doi.org/10.1080/02650487.2015.1101908.

[33] Peters, G. J., Ruiter, R. A., &Kok, G. (2013). Threatening communication: A critical reanalysis and a revised meta-analytic test of fear appeal theory. Health Psychology Review, 7(1), 8-31. https://doi.org/10.1080%2F17437199.2012.703527.

[34] Popova, L. (2012). The extended parallel process model: Illuminating the gaps in research. Health Education &Behavior, 39(4), 455-473. https://doi.org/10.1177/1090198111418108.

[35] Vrhovec, S., &Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. Computers & Security, 106, 102309. https://doi.org/10.1016/j.cose.2021.102309.