INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 16, Issue 11, (2026) E-ISSN: 2222-6990

# The Impact and Implementation of Advanced Security Technologies in Online Banking

Nik Hadiyan Nik Azman*, Nor Hidayah Binti Nor Hakimi

School of Management, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia

Corresponding Author Email: nikhadiyan@usm.my

Email: hidayahhakimi@student.usm.my

**DOI Link:** http://dx.doi.org/10.6007/IJARBSS/v16-i11/29378

***Published Date:*** 18 November 2026

**Abstract**

The rapid expansion of digital banking has increased cybersecurity risks, necessitating the adoption of advanced security technologies to safeguard online financial transactions. This study investigates the influence of technological, organizational, and environmental factors on the adoption of advanced security technologies in online banking based on the Technology–Organization–Environment (TOE) framework. A quantitative cross-sectional survey was conducted among 60 online banking users, and data were analyzed using SPSS through descriptive statistics, reliability analysis, correlation, and multiple regression techniques. The results indicate that technological and organizational factors significantly influence adoption, with organizational factors representing the strongest predictor. In contrast, environmental factors related to artificial intelligence technology were not found to significantly affect adoption behaviour. The regression model explains 96.4% of the variance in adoption, indicating strong predictive capability. The findings emphasize the importance of organizational readiness and technological effectiveness in enhancing trust and encouraging secure digital banking usage. This study provides empirical evidence supporting cybersecurity adoption strategies and offers practical implications for financial institutions seeking to strengthen online banking security implementation.

**keywords:** Online Banking, Cybersecurity, Technology Adoption, TOE Framework, Digital Banking

## Introduction

In recent years, advanced security technologies have fundamentally transformed online banking by addressing the escalating threats posed by cybercriminals in an increasingly digital financial landscape. Financial organizations are embracing novel technological advancements to enhance the resilience and efficiency of the financial system (Oladapo et al., 2022). With the rapid digitization of financial services, traditional security methods are no longer sufficient to safeguard sensitive customer data and assets. Modern banks now rely on sophisticated measures such as artificial intelligence (AI), blockchain, and biometric authentication to provide robust, multi-layered protection. These technologies enable real-time fraud

detection, risk mitigation, and proactive threat prevention, ensuring that banking transactions remain secure despite the evolving tactics of cyber attackers.

Implementing these advanced security technologies not only enhances the safety of online banking but also reinforces customer trust and regulatory compliance. AI-driven systems analyze behavioral patterns to predict breaches before they occur, while Blockchain technology offers a compelling chance to revolutionize the financial industry by enhancing transaction security, efficiency, and transparency (R. Baldwin, 2020), reducing fraud risks. Biometric authentication contributes by offering secure, convenient user verification and cloud security innovations, including zero-trust architectures and continuous monitoring, which ensure resilience against attacks. Together, these technologies represent a critical shift toward proactive, intelligent, and adaptive cybersecurity frameworks that protect the integrity and reliability of digital banking services in an era of sophisticated cyber threats.

This study aimed to identify the various types of online threats that can lead to fraud in e-banking services and to determine the most effective cybercrime prevention tools for mitigating such threats. The availability of relevant information and effective control mechanisms can significantly contribute to minimizing e-banking fraud. Raising awareness and providing education help individuals and organizations guard against cyber threats (Chaimaa et al., 2021). The results of the study can assist regulatory bodies and banking management teams in identifying areas that require heightened focus and can aid them in devising innovative strategies to help their clients stay secure.

Despite the increasing adoption of advanced security technologies such as Multi-Factor Authentication (MFA) and biometric authentication, Artificial Intelligence (AI), and blockchain-based security in online banking, incidents of fraud, data breaches, and unauthorized access continue to occur. At the same time, stronger security measures may reduce usability and discourage customer adoption. There is limited empirical evidence on how different types and levels of advanced security technologies influence users' perceived security and privacy protection, as well as their willingness to use online banking services. This creates a challenge for banks in determining the most effective security approach that balances protection, privacy, and user convenience. Based on previous studies, online banking adoption has primarily focused on general technology aspects or basic security measures such as passwords and SMS OTPs, without considering more advanced technologies like MFA, biometrics, and AI fraud detection systems, particularly in the TOE model. There are existing research gaps in investigating how these technologies influence risk perceptions and adoption by users, particularly in Malaysia.

The present investigation differs from earlier studies in several important aspects. While Alalwan et al. (2017) examined consumer adoption of mobile banking and Martins et al. (2014) investigated internet banking adoption through the Unified Theory of Acceptance and Use of Technology (UTAUT) and perceived risk, the present study specifically focuses on the adoption of advanced security technologies rather than general digital banking acceptance. Similarly, Oliveira and Martins (2011) reviewed information technology adoption models at the firm level, whereas the present investigation applies the Technology–Organization–Environment (TOE) framework from the perspective of online banking users. Furthermore, while Riasat et al. (2025) investigated customers' adoption of emerging security tools in

mobile banking applications, the present study simultaneously examines technological, organizational, and environmental factors associated with artificial intelligence (AI) technology within an integrated TOE framework. Accordingly, the present investigation complements and extends earlier research by providing preliminary empirical insights into the multidimensional determinants of advanced security technology adoption within the Malaysian online banking context.The paper aims to fill this gap by investigating the effect of technological, organizational, and environmental factors on the adoption of advanced security technologies. Therefore this study aim to examine the impact of technological factors, organizational factors and environmental factors of AI tech on the adoption of advanced security technologies in online banking. The present investigation is expected to contribute to the existing body of knowledge in several ways. First, from a theoretical perspective, this study extends the application of the Technology–Organization–Environment (TOE) framework beyond its conventional organizational-level orientation by examining the adoption of advanced security technologies from the perspective of online banking users. While previous studies have predominantly focused on general digital banking adoption and technology acceptance (Alalwan et al., 2017; Martins et al., 2014), this study provides a more specific examination of advanced security technology adoption. Second, from an empirical perspective, this study advances the existing literature by simultaneously examining the relative importance of technological, organizational, and environmental factors related to AI technology, thereby providing a more comprehensive understanding of the determinants of cybersecurity technology adoption. Third, from a contextual perspective, this study enriches the limited empirical literature on advanced security technology adoption within the Malaysian online banking context, particularly in an emerging digital economy. Finally, from a practical perspective, the findings are expected to provide valuable insights for financial institutions, cybersecurity professionals, and policymakers in developing effective security implementation strategies that balance technological effectiveness, organizational readiness, and customer acceptance. Collectively, these contributions bridge the gap between existing technology adoption literature and the growing need to understand advanced cybersecurity technology adoption in online banking.

## Literature Review

This study is anchored on several theoretical foundations to explain the relationship between Technological factors, organizational factors, environment factors of AI tech. The integration of these theories provides a robust basis for understanding how technological, behavioral, and influence adoption in fintech.

### *Technology-Organization-Environment (TOE) Framework*

The Technology-Organization-Environment (TOE) framework, developed by Tornatzky and Fleischer (1990), is a widely used theoretical model that explains how organizations adopt and implement new technologies. The framework posits that technological adoption is influenced by three interrelated contexts, first, technological context. This includes the characteristics of the technology itself, such as complexity, compatibility with existing systems, perceived benefits, and potential risks. In the case of blockchain-based smart contracts, technological risks can include coding errors, scalability issues, interoperability challenges with legacy banking systems, and a lack of legal enforceability in certain jurisdictions. These technological uncertainties can delay adoption or reduce confidence among managers and end-users (Clohessy et al., 2019). Second, organizational context. This

encompasses internal resources, capabilities, and readiness, including financial capacity, human capital, management support, and IT infrastructure. Organizations with strong technical expertise and well-prepared IT teams are more likely to successfully implement smart contracts and integrate them into existing processes. Conversely, inadequate staff training, limited cybersecurity knowledge, or insufficient infrastructure can impede adoption, even if the technology itself is promising. Third, environmental context. This includes external pressures such as regulatory requirements, competitive dynamics, and market demand. For blockchain adoption, organizations may face legal uncertainties, regulatory compliance challenges, or slow industry-wide acceptance. These external pressures can either accelerate adoption (if the market rewards early adopters) or act as barriers (if regulations are unclear or restrictive).

By applying the TOE framework, this study emphasizes that technological risks are not isolated factors but interact with organizational readiness and environmental pressures to influence adoption decisions. For example, even if a blockchain solution has high technical risk, an organization with strong internal expertise and supportive management may still adopt it successfully. Conversely, external pressures such as regulatory uncertainty may exacerbate perceived risks, discouraging adoption. Prior research has demonstrated that TOE is effective in explaining adoption of emerging financial technologies. Clohessy et al. (2019) found that technological uncertainties, when combined with organizational and environmental factors, significantly influence the uptake of blockchain-based innovations. Similarly, this study uses TOE to justify examining technological risks as an independent variable, as it directly affects the likelihood of adoption of smart contracts in financial and banking systems. This theoretical lens helps managers understand not only the risks of new technology but also how organizational preparedness and external conditions can mitigate or amplify these risks. Empirical research consistently shows that perceived relative advantage positively influences users' intention to adopt digital banking services. A recent Malaysian study focusing on Generation Z's adoption of digital banking reported that relative advantage had a significant positive relationship with behavioral intention, acting alongside trust and perceived value to shape adoption decisions. This suggests that when younger customers see clear benefits in digital banking over traditional means, they are more likely to adopt these services.

*Emoirical Review*

Riasat, Shah, and Gonul (2025) found that mobile banking users' *perceptions of usefulness* and the *usefulness of security tools* such as biometric authentication significantly affect their willingness to adopt these technologies, indicating that when users recognise clear benefits (e.g., enhanced protection of sensitive data), the likelihood of adoption increases. In this study, participants considered technologies like biometric authentication and SMS alerts as *useful tools* for safeguarding accounts, which aligns with the concept of relative advantage as a predictor of user behaviour within technology acceptance frameworks. Moreover, perceived trust and ease of use were also linked with greater adoption when users understood how these security tools improved account protection.

Technological factors refer to the characteristics and capabilities of advanced security technologies implemented in online banking systems. These include security features such as Multi-Factor Authentication (MFA), biometric authentication, and AI-based fraud detection,

which are designed to protect users from cyber threats and unauthorized access. According to the Technology–Organization–Environment (TOE) framework, technological attributes such as perceived effectiveness, reliability, compatibility, and ease of use play a crucial role in determining technology adoption (Tornatzky & Fleischer, 1990). Previous studies have found that robust and user-friendly security technologies enhance users' confidence and reduce perceived vulnerability, thereby positively influencing the adoption of online banking services (Kumar et al., 2020)

Organizational factors refer to the internal capabilities and readiness of banks to implement and manage advanced security technologies effectively. These factors include top management support, availability of technological infrastructure, employee expertise, and organizational commitment to cybersecurity. Within the TOE framework, organizational readiness is considered a key determinant of successful technology implementation (Oliveira & Martins, 2011). Empirical evidence suggests that banks with strong managerial support and adequate IT resources are more likely to adopt advanced security technologies, which in turn enhances system reliability and customer trust in online banking platforms (Alalwan et al., 2017).

Environmental factors encompass external pressures that influence banks' adoption of advanced security technologies in online banking. These pressures include regulatory requirements, competitive intensity, and increasing customer expectations for secure digital financial services. Regulatory bodies and financial authorities often impose stringent cybersecurity and data protection standards, compelling banks to strengthen their security infrastructure (Zhu & Kraemer, 2005). Additionally, competitive pressure among financial institutions encourages banks to implement advanced security technologies as a means of differentiation and trust-building, thereby improving customer confidence and adoption of online banking services.

Adoption of advanced security technologies in online banking refers to users' intention to use and continue using online banking services that incorporate enhanced security features. Adoption is influenced by both technical and perceptual factors, including perceived security, trust, and ease of use. Prior research indicates that when users perceive online banking platforms as secure and reliable, their intention to adopt and continue using these services increases significantly (Venkatesh et al., 2012). Therefore, the successful adoption of advanced security technologies plays a crucial role in strengthening customer trust and ensuring the sustainability of online banking services.

**Methodology**

This study adopts a quantitative research approach employing a survey method to examine the factors influencing the adoption of advanced security technologies in online banking. A quantitative design is considered appropriate as it enables empirical testing of theoretically derived hypotheses and facilitates systematic analysis of relationships between technological, organizational, and environmental factors and the adoption of advanced security technologies in digital banking environments. A cross-sectional research design is applied, whereby data are collected from respondents at a single point in time to capture users' perceptions, experiences, and behavioural responses toward online banking security mechanisms. This approach is suitable for investigating user acceptance of emerging security

solutions such as Multi-Factor Authentication (MFA), biometric authentication, and artificial intelligence (AI)-based fraud detection systems, which play an important role in shaping users' perceived risk, trust, and adoption behaviour in online banking services.

The target population of this study consists of individuals who actively use online banking services, as these users possess direct experience with digital banking platforms and are capable of evaluating the effectiveness and usability of advanced security technologies. A non-probability sampling technique is employed due to practical considerations related to accessibility and time constraints. Specifically, purposive sampling is used to ensure that respondents meet predefined eligibility criteria, while convenience sampling facilitates efficient data collection through accessible online channels. Respondents are required to be aged 18 years and above and to have used online banking services for at least six months to ensure sufficient familiarity with banking security features. The sample size is determined based on recommended guidelines for Partial Least Squares Structural Equation Modeling (PLS-SEM), ensuring adequate statistical power and reliable estimation of model relationships.

Primary data are collected using a structured questionnaire developed through Google Forms and distributed via online platforms, including email and social media applications. Screening questions are placed at the beginning of the survey to confirm respondents' eligibility prior to participation. Participation is voluntary, and respondents are informed about the purpose of the study, confidentiality assurance, anonymity protection, and the academic use of collected information to encourage honest and unbiased responses while ensuring compliance with ethical research standards. The questionnaire is divided into five sections covering technological factors, organizational factors, environmental factors related to AI technology, adoption of advanced security technologies in online banking, and demographic information. Measurement items are adapted from established and validated instruments reported in prior literature to ensure theoretical consistency and measurement accuracy. All items are measured using a seven-point Likert scale ranging from 1 (strongly disagree) to 7 (strongly agree), allowing greater response sensitivity and improved variance explanation.

**Results**

The collected data were analyzed using the Statistical Package for the Social Sciences (SPSS) version 27, which was selected for its reliability and suitability in conducting quantitative statistical analysis. Before hypothesis testing, preliminary data analyses were conducted to ensure the quality and appropriateness of the dataset.

The chapter begins with data screening procedures, including checks for missing values and data consistency, followed by an analysis of the demographic profile of respondents. Next, reliability analysis using Cronbach's Alpha is performed to assess the internal consistency of the measurement scales used for all constructs in the study. Descriptive statistics are then presented to summarize respondents' perceptions of the key variables.

Subsequently, correlation analysis is conducted to examine the relationships between the independent variables (IV), Technological Factors, Organizational Factors, and Environmental Factors of AI technology, and the dependent variable (DV), Adoption of Advanced Security Technologies in Online Banking. Finally, hypothesis testing is carried out to determine the

significance and strength of these relationships in accordance with the proposed research framework.

Table 1 presents the demographic characteristics of the respondents participating in this study. A total of 60 valid responses were obtained and analyzed. In terms of gender distribution, the sample consisted of 32 male respondents (53.3%) and 28 female respondents (46.7%), indicating a relatively balanced gender representation and suggesting that both male and female users actively engage in online banking services. With respect to age distribution, the majority of respondents were within the economically active population. The largest group comprised individuals aged between 20 and 29 years, representing 38.3% of the sample, followed by respondents aged 30 to 39 years (28.3%). Participants below 20 years accounted for 15%, while those aged 40 to 49 years and 50 years and above represented 10% and 8.3%, respectively. This distribution indicates that online banking usage is predominantly concentrated among young and middle-aged adults who are generally more familiar with digital technologies.

In terms of educational attainment, most respondents possessed higher education qualifications. Nearly half of the respondents held a bachelor's degree (46.7%), followed by master's degree holders (16.7%) and doctorate holders (10%). Respondents with diploma-level education and secondary school qualifications each represented 13.3% of the sample. The relatively high educational background of respondents suggests an adequate level of digital literacy, which is important for evaluating advanced online banking security technologies. Regarding income level, the largest proportion of respondents earned between RM4,001 and RM6,000 (36.7%), followed by those earning RM6,001 to RM8,000 (23.3%). Respondents earning below RM2,000 accounted for 21.7%, while smaller proportions were observed in the RM2,001–RM4,000 category (10%) and above RM8,000 income group (8.3%). This distribution reflects participation from diverse income groups, indicating that online banking services are widely utilized across different economic segments.

Analysis of online banking experience shows that most respondents had substantial familiarity with digital banking platforms. Nearly half of the respondents (45%) reported having between one and three years of online banking experience, while 36.7% had more than three years of experience. Only 18.3% reported less than one year of experience, suggesting that the majority of participants possess sufficient exposure to evaluate banking security technologies effectively. Finally, in terms of usage frequency, online banking appears to be integrated into respondents' daily financial activities. A significant proportion of respondents (45%) reported using online banking on a daily basis, followed by 18.3% who used it once a week and 16.7% once a month. Additionally, 15% used online banking several times per week, while only 5% reported rare usage. These findings indicate a high level of engagement with online banking services among respondents, supporting the suitability of the sample for examining the adoption of advanced security technologies.

Table 1
*Demographic Profile*

| Response | Frequency | Percentage (%) |
|---|---|---|
| **Gender** | | |
| Male | 32 | 53.3 |
| Female | 28 | 46.7 |
| **Age Group (Years)** | | |
| Below 20 | 9 | 15 |
| 20-39 | 23 | 38.3 |
| 30-39 | 17 | 28.3 |
| 40-49 | 6 | 10 |
| 50 and above | 5 | 8.3 |
| **Level of Education** | | |
| Secondary School (SPM) | 8 | 13.3 |
| Diploma or Equivalent | 8 | 13.3 |
| Bachelor's Degree | 28 | 46.7 |
| Master's Degree | 10 | 16.7 |
| Doctorate (PHD) | 6 | 10 |
| **Income (RM)** | | |
| Below 2000 | 13 | 21.7 |
| 2001-4000 | 6 | 10 |
| 4001-6000 | 22 | 36.7 |
| 6001-8000 | 14 | 23.3 |
| Above 8000 | 5 | 8.3 |
| **Online Banking Experience** | | |
| Less than 1 year | 11 | 18.3 |
| 1-3 years | 27 | 45 |
| More than 3 years | 22 | 36.7 |
| **Frequency Using Online Banking** | | |
| Daily | 27 | 45 |
| Several times a week | 9 | 15 |
| Once a week | 11 | 18.3 |
| Once a month | 10 | 16.7 |
| Rarely | 3 | 5 |

*N=60 respondents*

To assess the reliability and internal consistency of the measurement instruments used in this study, a reliability analysis was conducted using Cronbach's Alpha. Cronbach's Alpha is a widely accepted statistical measure for evaluating the internal consistency of multi-item scales, indicating how closely related the items are within a construct (Tavakol & Dennick, 2011). Generally, a Cronbach's Alpha value of 0.70 or higher is considered acceptable for reliability (Nunnally & Bernstein, 1994).

Table 2
*Reliability Analysis of the Main Variables*

| Variable | Items | Item Deleted | Cronbach's Alpha |
|---|---|---|---|
| Technological Factors | 20 | - | 0.993 |
| Organizational Factors | 15 | - | 0.990 |
| Environmental Factors of AI Tech | 15 | - | 0.977 |
| Adoption of Advanced Security Technologies in Online Banking | 5 | - | 0.976 |

As presented in Table 2, Technological Factors (IV1), consisting of 20 items, recorded a Cronbach's Alpha value of 0.993, indicating excellent internal consistency. Organizational Factors (IV2) with 15 items achieved an Alpha value of 0.990, while Environmental Factors of AI Technology (IV3) also demonstrated strong reliability with an Alpha value of 0.977. The dependent variable, Adoption of Advanced Security Technologies in Online Banking, comprising 5 items, produced a Cronbach's Alpha value of 0.976. No items were deleted for any construct, indicating that all measurement items contributed positively to their respective scales. Overall, the results indicate that all constructs exhibit excellent reliability and are suitable for subsequent statistical analyses. This confirms that the measurement instruments used in this study are both stable and consistent in measuring the intended constructs.

Table 3
*Descriptive Analysis of the Main Variables*

| Variable | Mean | Std. Dev. | Skewness | Kurtosis |
|---|---|---|---|---|
| Technological Factors | 5.7608 | 1.01669 | -1.083 | 1.199 |
| Organizational Factors | 5.6622 | 0.94694 | -0.869 | -0.229 |
| Environmental Factors of AI Tech | 5.7300 | 0.91610 | -0.873 | -0.018 |
| Adoption of Advanced Security Technologies in Online Banking | 5.8500 | 1.00414 | -0.936 | 0.312 |

Table 3 summarizes the descriptive statistics for all variables examined in this study, including the mean, standard deviation, skewness, and kurtosis values. The mean scores for all constructs are relatively high, ranging from 5.66 to 5.85, indicating that respondents generally agreed with the statements related to technological, organizational, and environmental factors, as well as the adoption of advanced security technologies in online banking. Among the variables, the Adoption of Advanced Security Technologies in Online Banking recorded the highest mean value (M = 5.850), suggesting a strong positive perception toward the implementation of advanced security measures. The standard deviation values for all variables are close to 1, indicating a moderate level of variability and consistent responses among respondents. Furthermore, the skewness values for all variables are negative, implying that responses are slightly skewed toward higher agreement levels. The kurtosis values are within the acceptable range of ±2, indicating that the distributions do not deviate significantly

from normality. The results suggest that the data are normally distributed and suitable for further inferential statistical analyses such as correlation and regression testing.

Table 4 presents the results of the Pearson correlation analysis conducted to examine the relationships between the dependent variable, Adoption of Advanced Security Technologies in Online Banking, and the independent variables, Technological Factors, Organizational Factors, and Environmental Factors of AI Technology. The results indicate that all independent variables have a strong positive relationship with the dependent variable and are statistically significant at the 0.01 level (2-tailed).

Table 4
*Correlation of the Main Variables*

| **Construct** | **DV** | **IV1** | **IV2** | **IV3** |
|---|---|---|---|---|
| **DV** | 1 | 0.973** | 0.978** | 0.939** |
| **IV1** | 0.973** | 1 | 0.970** | 0.941** |
| **IV2** | 0.978** | 0.970** | 1 | 0.946** |
| **IV3** | 0.939** | 0.941** | 0.946** | 1 |

**P<0.01 (2-tailed)

Specifically, Organizational Factors show the strongest correlation with the adoption of advanced security technologies (r = 0.978), followed closely by Technological Factors (r = 0.973). Environmental Factors of AI Technology also demonstrate a strong positive correlation with the dependent variable (r = 0.939). Furthermore, high correlations are observed among the independent variables themselves, suggesting that these factors are closely related in influencing the adoption of advanced security technologies in online banking. Overall, the findings indicate that improvements in technological, organizational, and environmental aspects of AI technology are strongly associated with higher levels of adoption of advanced security technologies.

Table 5
*Regression Analysis*

| **The Impact and Implementation of Advanced Security Technologies in Online Banking $R^2$ Change = 0.966** | **Beta** |
|---|---|
| Technological Factors | 0.393 |
| Organizational Factors | 0.550 |
| Environmental Factors of AI Tech | 0.049 |

*Note: N=60; *p<.05, **p<.01,***p<.001*

The linear model of multiple regression analysis has been used to examine the developed hypotheses. The assumption of normality, normality of the error term, constant variance, linearity, multicollinearity, outliers, and autocorrelation have been examined. The ANOVA table shows that the p-value is less than 0.050, which is considered significant. The hypothesis that concludes for this data is from non-multivariate normal populations. To follow the

multivariate normal distribution, the data must be less than 3, but in this research, the result is greater than 3, which concludes that the research hypothesis is non-multivariate normal populations. Normality of the data was assessed using skewness and kurtosis. According to Hair et al. (2010), a skewness between -2 and +2 and kurtosis between -7 and +7 indicate approximate normality.

Table 6
*Normality Table*

| **Variable** | **Skewness** | **Kurtosis** | **Normality** |
|---|---|---|---|
| Technological Factors | -1.083 | 1.199 | Acceptable |
| Organizational Factors | -0.869 | -0.229 | Acceptable |
| Environmental Factors of AI Tech | -0.873 | -0.018 | Acceptable |
| Adoption of Advanced Security Technologies | -0.936 | 0.312 | Acceptable |

All variables are within the acceptable range, indicating that univariate normality is satisfied. Multivariate normality was not formally tested, but the distribution of each variable is approximately normal. The histogram shows a bell-shaped distribution with a mean of 5.85 and a standard deviation of 1.00414, indicating that the residuals are approximately normally distributed. Based on the scatter plot of standardized residuals, the data points are randomly dispersed around the line of best fit across all predicted values. There is no visible systematic pattern, such as a funnel shape or a trend of increasing or decreasing spread. This indicates that the variance of the residuals remains relatively constant throughout the plot. Therefore, the assumption of homoscedasticity (constant variance) is satisfied.

Multicollinearity occurs when independent variables are highly correlated and is commonly assessed using the Variance Inflation Factor (VIF) values, where a VIF greater than 10 indicates a potential problem. Based on the results, IV1 (VIF = 18.661), IV2 (VIF = 20.354), and IV3 (VIF = 10.452) all exceed or are close to this threshold, indicating the presence of multicollinearity among the independent variables. This suggests that the predictors are strongly interrelated, which may affect the stability and reliability of the regression coefficient estimates. The linear model of multiple regression analysis has been used to examine the developed hypotheses. The assumption of normality, normality of the error term, constant variance, linearity, multicollinearity, outliers, and autocorrelation have been examined. The ANOVA table shows that the p-value is less than 0.050, which is considered significant. Table 7 presents the results of the multiple regression analysis examining the relationships between Technological Factors (IV1), Organizational Factors (IV2), and Environmental Factors of AI Technology (IV3) with the Adoption of Advanced Security Technologies in Online Banking. The ANOVA table demonstrates a strong explanatory power, with an $R^2$ value of 0.966 and an adjusted $R^2$ of 0.964, indicating that approximately 96.4% of the variance in the adoption of advanced security technologies is explained by the three independent variables.

Table 7
*Hypothesis Testing*

| Hypothesis | Construct | Unstd. B | Std. Error | Std.B | t-value | p-value | LL | UL | VIF |
|---|---|---|---|---|---|---|---|---|---|
| H1-4 | IV1 | 0.388 | 0.105 | 0.393 | 3.706 | <.001 | 0.178 | 0.598 | 18.661 |
| H5-7 | IV2 | 0.583 | 0.117 | 0.550 | 4.962 | <.001 | 0.348 | 0.818 | 20.354 |
| H8-10 | IV3 | 0.054 | 0.087 | 0.049 | 0.621 | 0.537 | -0.120 | 0.228 | 10.452 |

The results show that Technological Factors (IV1) have a significant positive effect on the adoption of advanced security technologies ($\beta = 0.393$, $t = 3.706$, $p < 0.001$). Therefore, hypotheses H1–H4 are supported, suggesting that technological readiness and related factors play an important role in influencing adoption. Similarly, Organizational Factors (IV2) exhibit a significant positive relationship with the dependent variable ($\beta = 0.550$, $t = 4.962$, $p < 0.001$). This indicates that organizational support, resources, and capabilities significantly influence adoption, thus supporting hypotheses H5–H7. In contrast, Environmental Factors of AI Technology (IV3) do not show a significant effect on the adoption of advanced security technologies ($\beta = 0.049$, $t = 0.621$, $p = 0.537$). As the p-value exceeds the 0.05 significance level and the confidence interval includes zero, hypotheses H8–H10 are not supported. The findings indicate that technological and organizational factors are significant predictors of the adoption of advanced security technologies in online banking, while environmental factors related to AI technology do not have a statistically significant influence in this study.

**Discussion**

This study was conducted to examine the factors influencing the adoption of advanced security technologies in online banking, with a particular focus on technological, organizational, and environmental aspects of AI technology. The research employed a quantitative approach using a structured questionnaire to collect data from respondents using Google Forms, and multiple regression analysis (using IBM SPSS) was applied to test the proposed hypotheses. The aim of the current research was to examine the factors that influence the adoption of advanced security technologies in online banking. This section discusses the findings in relation to the research questions and hypotheses developed in the study. The discussion focuses on how technological, organizational, and environmental factors of AI technology affect users' adoption decisions. Each subsection addresses one research question based on the results of the multiple regression analysis.

The findings of this study indicate that technological factors have a significant positive relationship with the adoption of advanced security technologies in online banking. The regression results show that technological factors significantly influence adoption, as evidenced by a positive standardized beta coefficient and a p-value of less than 0.05. This suggests that aspects such as perceived usefulness, system reliability, compatibility, and technological readiness play an important role in encouraging users to adopt advanced security solutions in online banking platforms. When online banking security technologies are perceived as effective in protecting sensitive financial information, users develop greater trust and confidence in the system, leading to higher adoption rates. Similarly, Tornatzky and Fleischer's (1990) Technology–Organization–Environment (TOE) framework emphasizes that technological characteristics play a central role in shaping organizational and user adoption decisions.

Furthermore, prior studies in the context of online banking and financial technologies have found that advanced security features such as encryption, biometric authentication, and fraud detection systems positively affect users' intention to adopt digital banking services (Alalwan et al., 2017; Martins et al., 2014). These technologies reduce perceived risk and increase users' confidence in conducting online transactions. Therefore, the findings of this study reinforce existing literature by confirming that technological factors are a key determinant of the adoption of advanced security technologies in online banking. These results are consistent with prior studies, which emphasize that strong technological infrastructure and perceived technological benefits enhance users' confidence and willingness to adopt security technologies. When users perceive advanced security technologies as reliable, easy to use, and effective in protecting financial information, they are more likely to embrace such systems. Therefore, the findings support the view that technological factors are a critical determinant in the successful adoption of advanced security technologies in online banking.

The results of the hypothesis testing indicate that organizational factors have a significant and positive relationship with the adoption of advanced security technologies in online banking. The multiple regression analysis shows that organizational factors significantly influence adoption, as evidenced by a high standardized beta coefficient and a p-value of less than 0.05. Therefore, hypotheses H5–H7 are supported. This finding suggests that internal organizational elements such as top management support, availability of financial and human resources, organizational readiness, and security policies play a crucial role in encouraging the adoption of advanced security technologies within online banking systems. This finding is consistent with the Technology–Organization–Environment (TOE) framework, which emphasizes that organizational characteristics strongly affect technology adoption decisions (Tornatzky & Fleischer, 1990). Strong managerial commitment and sufficient organizational resources enhance the ability of institutions to implement and sustain advanced security technologies effectively. When organizations prioritize security through clear strategies, training, and investment, users are more likely to trust and adopt these technologies. Moreover, prior empirical studies have demonstrated that organizational support and security governance significantly influence the adoption of security-related technologies in the banking and financial services sector (Thong et al., 2011; Oliveira et al., 2014). Effective organizational structures and leadership commitment help reduce implementation barriers and increase users' confidence in online banking platforms. Therefore, the findings of this study reinforce existing literature by confirming that organizational factors are a key determinant in the adoption of advanced security technologies in online banking.

The findings of the hypothesis testing reveal that environmental factors of AI technology do not have a significant relationship with the adoption of advanced security technologies in online banking. The multiple regression analysis shows that the effect of environmental factors is statistically insignificant, as indicated by a p-value greater than 0.05. Therefore, hypotheses H8–H10 are not supported. This suggests that external environmental elements such as regulatory pressure, industry competition, technological trends, and external support related to AI technology do not significantly influence users' adoption decisions in the context of this study. This finding contrasts with the Technology–Organization–Environment (TOE) framework, which posits that environmental factors can play an important role in shaping technology adoption decisions (Tornatzky & Fleischer, 1990). However, the insignificant result

may be explained by the possibility that advanced security technologies in online banking have already become a standard practice, reducing the influence of external pressures on adoption decisions. Users may prioritize internal technological performance and organizational readiness over external environmental conditions when deciding whether to adopt such technologies. Similar findings have been reported in previous studies, where environmental factors were found to have a limited or insignificant impact on technology adoption in mature or highly regulated industries such as banking (Hameed et al., 2012; Low et al., 2011). In such contexts, compliance with regulatory requirements is often mandatory, which minimizes variation in adoption decisions driven by environmental influences. Therefore, the results of this study suggest that while environmental factors of AI technology may be important at an institutional or policy level, they do not directly affect users' adoption of advanced security technologies in online banking.

Beyond corroborating previous research on technology adoption, this study offers additional insights into the relative explanatory relevance of the three dimensions of the TOE framework within the context of advanced online banking security. A particularly noteworthy finding is that organizational factors recorded the largest standardized regression coefficient ($\beta = 0.550$, $p < 0.001$), exceeding that of technological factors ($\beta = 0.393$, $p < 0.001$). This suggests that users' perceptions of organizational capabilities, readiness, and commitment to cybersecurity may be particularly relevant to their acceptance of advanced security technologies. Moreover, the insignificant relationship between environmental factors related to AI technology and adoption ($\beta = 0.049$, $p = 0.537$) provides an additional insight into the context-dependent applicability of the TOE framework. While external environmental conditions may be relevant to institutional technology implementation, their direct explanatory contribution to user-level adoption may be less apparent when technological and organizational factors are considered simultaneously. These findings suggest that the relative relevance of the TOE dimensions may differ depending on the unit of analysis and technological context. Nevertheless, given the limited sample size and substantial multicollinearity among the predictors, these insights should be regarded as preliminary empirical evidence requiring further investigation.

**Conclusion**

In conclusion, this study contributes meaningful insights by integrating multiple SPSS analytical techniques rather than relying solely on regression results. The combined use of demographic analysis, reliability testing, correlation analysis, and graphical diagnostics provides strong empirical support for the study's conclusions. The findings emphasize the importance of internal technological capabilities and organizational readiness in promoting the adoption of advanced security technologies in online banking. Despite its limitations, this research offers a solid foundation for future studies and practical decision-making aimed at enhancing security and trust in digital banking environments.

**Conflicts of Interest**

The authors declare that they have no known financial or personal relationships that could have appeared to influence the work reported in this paper. The research was conducted independently without any commercial or financial bias.

**Source of Funding Statements**

This research received no external funding. The study was conducted independently by the authors, and no financial support was obtained from any public, commercial, or not-for-profit funding agencies.

**Acknowledgments**

The authors would like to express their sincere appreciation to the School of Management and the university for providing academic support and necessary resources to complete this study. Special thanks are extended to colleagues and peers who provided constructive feedback and encouragement throughout the research process

**References**

Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2017). Consumer adoption of mobile banking in Jordan. *Journal of Enterprise Information Management, 30*(3), 416–440.

Al-Mazroua, M., & Al-Ketti, A. (2022). Privacy concerns in fintech adoption: Exploring consumer attitudes towards data protection. *Journal of Information Privacy and Security, 18*(3), 145–160.

Chaimaa, B., Najib, E., & Rachid, H. (2021). E-banking overview: Concepts, challenges and solutions. *Wireless Personal Communications, 117*(2), 1059–1078. https://doi.org/10.1007/s11277-020-07911-0

Clohessy, T., Acton, T., & Morgan, L. (2019). Smart contracts and blockchain: The role of the TOE framework in adoption. *Information Systems Frontiers, 21*(5), 1231–1245. https://doi.org/10.1007/s10796-019-09932-7

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451–474.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2023). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage Publications.

Hameed, M. A., Counsell, S., & Swift, S. (2012). A conceptual model for the process of IT innovation adoption in organizations. *Journal of Engineering and Technology Management, 29*(3), 358–390.

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2017). Advances in social media research: Past, present and future. *Information Systems Frontiers, 20*(3), 531–558. https://doi.org/10.1007/s10796-017-9810-y

Khrais, L. T. (2015). Highlighting the vulnerabilities of online banking system. *Journal of Internet Banking and Commerce, 20*(3), 1–10.

Kitsios, F., & Kamariotou, M. (2022). Digital transformation strategy and organizational performance: A managerial perspective. *Sustainability, 14*(15), 1–18.

Kumar, V., Park, Y., & Subramaniam, A. (2020). Cybersecurity and digital banking adoption. *Technological Forecasting and Social Change, 157*, 120097.

Li, Y., & Huang, J. (2020). The role of trust and perceived risk in fintech adoption. *Electronic Commerce Research and Applications, 40*, 100944.

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems, 111*(7), 1006–1023.

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding Internet banking adoption: An application of UTAUT and perceived risk. *International Journal of Information Management, 34*(1), 1–13.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Oladapo, I. A., Hamoudah, M. M., Alam, M. M., Olaopa, O. R., & Muda, R. (2022). Customers' perceptions of fintech adaptability in the Islamic banking sector: A comparative study of Malaysia and Saudi Arabia. *Journal of Modelling in Management, 17*(4), 1241–1261.

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation, 14*(1), 110–121.

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption. *Information & Management, 51*(5), 497–510.

Riasat, I., Shah, M., & Gonul, M. S. (2025). Strengthening cybersecurity resilience: An investigation of customers' adoption of emerging security tools in mobile banking apps.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

Thong, J. Y. L., Yap, C. S., & Raman, K. S. (2011). Engagement of external expertise in information systems implementation. *Journal of Management Information Systems, 28*(2), 231–262.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending UTAUT. *MIS Quarterly, 36*(1), 157–178.

Zhou, T. (2012). Understanding users' initial trust in mobile banking. *Computers in Human Behavior, 28*(4), 1518–1525.