Jurnal Ilmu Perbankan dan Keuangan Syariah
Vol. 7 , No. 1 (2025), page 35-54
p-ISSN: 2963-3524 e-ISSN: 2686-6625
Journal homepage: http://jurnaljipsya.org/index.php/jipsya

Cyber crime vs cyber security: implications for customer trust in e-banking at Indonesian Islamic banks

Ubay Harun[1], Muthmainnah[2], Rizki Amalia [3]
[1,] Sharia Economic Law, Faculty of Sharia, State Islamic University Datokarama Palu, Indonesia
[2,3] Sharia Banking, Faculty of Economics and Islamic Business, State Islamic University Datokarama Palu, Indonesia

Corresponding email: ubayharun@uindatokarama.ac.id, mutmainnah831@gmail.com, rizkiamalia@uindatokarama.ac.id

Leave it blank

Received: May 2025	Revised: May 2025	Published: June 2025

ABSTRACT

This study explores the impact of cybercrime and cybersecurity on customer trust in e-banking services at Bank Syariah Indonesia (BSI), Palu Gajah Mada Branch, addressing a research gap related to the limited studies in the Islamic banking sector. The study offers a novel approach by integrating sharia principles into the analysis of digital security. The aim of this research is to identify how cyber threats and cybersecurity measures influence customers' perceptions of e-banking security. Using a quantitative approach with a correlational design, the study involved 100 respondents selected through an accidental sampling method. The results of linear regression analysis indicate that cybercrime significantly reduces customer trust, while cybersecurity has a strong positive influence. The implications of these findings highlight the need for increased investment in digital security to maintain customer trust, ultimately supporting the stability and growth of Islamic banking.

ARTICLE INFO

Keywords:

Cyber Crime, Cyber Security, Consumer Trust, E-Banking, Islamic Banking.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

INTRODUCTION

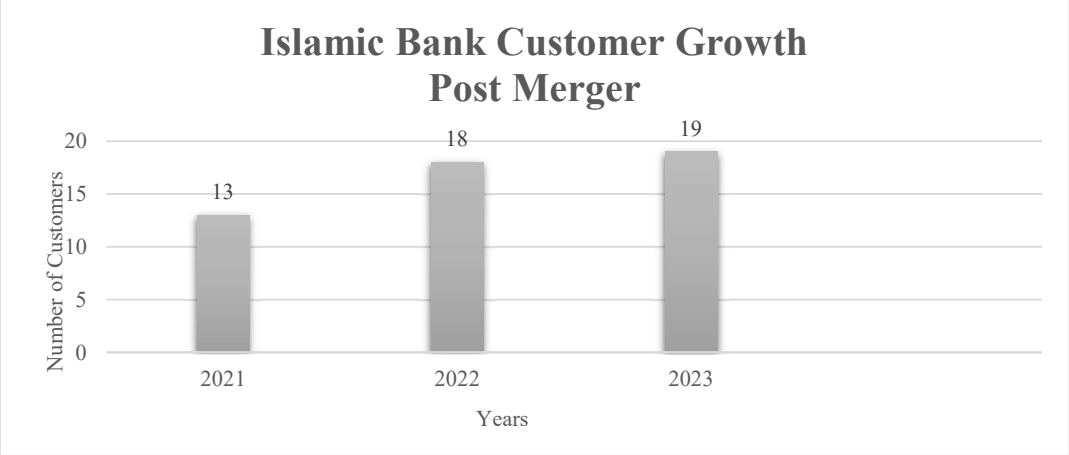
The rapid development of information technology has fundamentally transformed the banking industry landscape, facilitating the provision of more efficient and convenient digital services for customers. E-banking, as one form of digitalization in banking services, has become central to the modernization of financial services. This service offers various benefits, including ease of access, transaction speed, and flexibility for customers in managing their finances. However, alongside these benefits, e-banking also faces major

challenges in the form of increasingly sophisticated cybercrime threats. Cyber threats, such as hacking, malware, and phishing, have become significant issues that threaten the integrity and security of financial transactions on e-banking platforms. Cybercrime can not only compromise security systems but also undermine customer trust in digital banking services. In this context, Bank Syariah Indonesia (BSI), as one of the leading Islamic banks in Indonesia, faces a complex challenge. The bank must balance strict adherence to Sharia law principles with efforts to protect its digital systems from cyber threats (Gani, 2023).

PT Bank Syariah Indonesia Tbk, the result of a merger between three major Islamic banks—PT Bank BRI Syariah, PT Bank BNI Syariah, and PT Bank Mandiri Syariah—on February 1, 2021, is one of the State-Owned Enterprises (BUMN) playing a vital role in the Islamic banking industry in Indonesia. This merger was designed to strengthen the Islamic banking sector in the country, enhance competitiveness with conventional banks, and provide more optimal services to customers. The significant growth in BSI's customer base, from 12–13 million in 2021 to 19.22 million by the end of September 2023, demonstrates its success in attracting new customers (Muna et al., 2023). The increase in digital transaction volume also reflects the widespread adoption of e-banking services, with a year-on-year growth of 41.53% as of December 2020 (Mawarni et al., 2021).

Figure 1.

Bank Syariah Indonesia Customer Growth After Merger

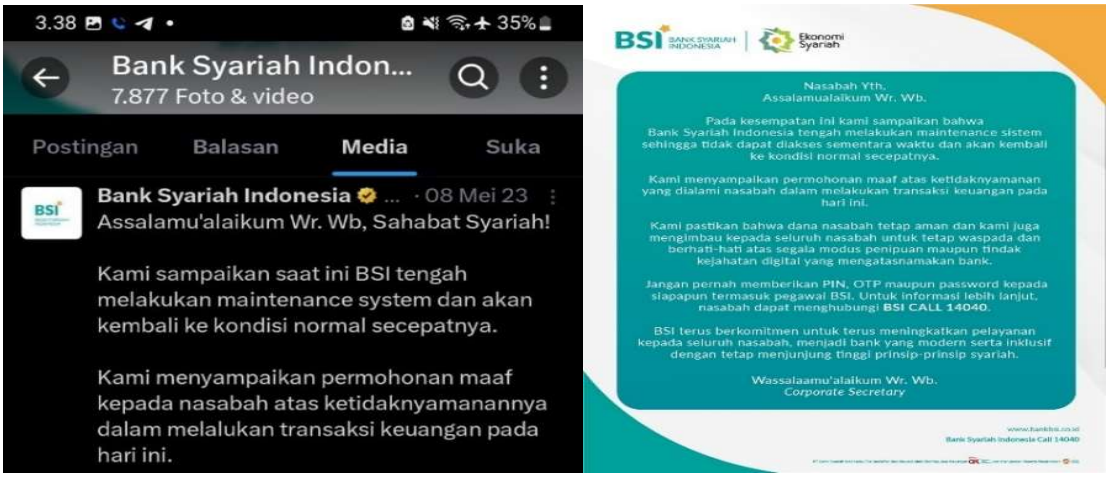


However, along with the rapid growth of Bank Syariah Indonesia (BSI) in offering e-banking services, the bank faces increasingly complex challenges from cyberattacks. The cyberattack incident on May 8, 2023, which caused disruptions to mobile banking, ATMs, and teller services for three days, revealed serious vulnerabilities faced by major banks (Alfi

et al., 2023). This disruption not only affected customer access but also had a significant negative impact on social media, highlighting the urgent need for stronger security systems. It underscores the critical importance of protecting sensitive information to maintain customer trust and uphold the bank's reputation amid increasingly sophisticated cyber threats.

Figure 2.

Official Twitter Screenshoot of Apology Bank Syariah Indonesia



Source: Bank Syariah Indonesia official Twitter

Several studies have shown that factors such as service quality, trust, commitment, brand image, and religiosity play a significant role in shaping customer satisfaction and loyalty in Islamic banks (Juliana et al., 2023; Lubis et al., 2022; Putri & Briliana, 2023). Customer proximity, risk perception, and Sharia compliance also influence customer satisfaction and loyalty (Mulia et al., 2021). In addition, the availability of features, security, and trust greatly affect customer satisfaction in mobile banking services (Khoirunnisa & Trishananto, 2023). However, research on how cybersecurity measures, such as fraud prevention in digital payment systems, impact customer trust in e-banking within Islamic banks remains insufficient.

While many studies have addressed the influence of various factors on customer behavior, there is a lack of exploring the impact of cybersecurity measures specifically on customer trust in e-banking in Islamic banks. Previous research has identified the importance of cybersecurity education and fraud prevention strategies, but no study has explored the overall impact of cybersecurity on customer trust in Indonesian Islamic

banking (Isa et al., 2022; Lestari & Saibil, 2022). Moreover, the interaction between factors such as religiosity and service quality with aspects of cybercrime and cybersecurity in the context of e-banking is less explored (Saputra & Rahmawaty, 2023; Widjajanta et al., 2021). Several international studies highlight the importance of trust in the adoption of e-banking services. Tiwari (2021) emphasizes the role of trust as a mediator between ease of use, infrastructure, and e-banking adoption. Sathar et al. (2022) and Gill et al. (2021) underscore how security and trust contribute to customer satisfaction and demonstrate the need for strong security measures. (Kala Kamdjoug et al., 2022) and Shankar & Jebarajakirthy (2019) reveal the positive impact of security and privacy aspects on customer trust and loyalty.

This study emphasizes that ensuring effective security measures and privacy protection is key to building and maintaining customer trust. The identified research gap highlights the need for studies focused on the interaction between cybercrime, cybersecurity measures, and customer trust in e-banking services within Indonesian Islamic banks. This research aims to provide new insights into how the integration of security factors, religiosity, and customer satisfaction can strengthen trust and loyalty among customers. By highlighting the crucial role of cybersecurity in the context of Islamic banking, this study seeks to offer strategic recommendations to help Islamic banks enhance customer trust in their e-banking platforms and reinforce loyalty through a comprehensive and integrated approach.

Literature Review

The Concept of E-Banking and Its Increasing Use

E-banking has become a crucial element in the modern banking system, especially in developing countries, where this technology enhances customer engagement and financial inclusion (Kala Kamdjoug et al., 2022). This transformation, driven by technological advancements and changing consumer preferences, emphasizes convenience, accessibility, and efficiency. However, the adoption and effectiveness of e-banking do not depend solely on the technology itself, but also on several critical factors such as ease of use, service quality, and security. Research shows that complicated procedures and long transaction times can reduce customer interest in e-banking, whereas intuitive interfaces and efficient processes can enhance the intention to use (Anouze & Alamro, 2019; Medyawati, 2011). The success of e-banking in enhancing customer satisfaction and loyalty heavily relies on the implementation of effective design and the management of efficient processes.

However, aspects of trust and cybersecurity play an equally important role. Customer trust in e-banking is often hindered by concerns about the security of personal and financial information (Alsheyyab & Singh, 2013; Bajwa et al., 2023). These concerns indicate that the implementation of comprehensive security measures, such as encryption and multi-factor authentication, is crucial for maintaining customer trust and satisfaction (Daniel et al., 2014; Khalil et al., 2021). Therefore, it can be hypothesized that banks that successfully integrate strong cybersecurity with user-friendly interfaces and efficient processes will be more successful in increasing e-banking adoption and customer loyalty compared to banks that do not prioritize these elements.

Cyber Crime and Customer Trust

The impact of cybercrime on customer trust in e-banking is a complex and multidimensional issue, where aspects of cybersecurity, service quality, and customer awareness interact to shape public perception. The literature review shows that strong cybersecurity measures can significantly enhance customer trust by preventing data breaches that could damage the bank's reputation and customer loyalty (Amer & Al-Omar, 2023). However, although the importance of cybersecurity is recognized, not all banks are able to implement it effectively, which ultimately leads to a decline in customer trust (Abbas & Arif, 2023). In this context, it can be hypothesized that the effectiveness of cybersecurity measures is directly proportional to the level of customer trust, where banks that fail to protect customer data will experience a significant decline in trust and loyalty.

In addition, the quality of e-banking services and customer awareness also play a crucial role in shaping trust. Research shows that high service quality, particularly in terms of reliability, security, and privacy, is correlated with increased customer satisfaction and trust (Hammoud et al., 2018). However, customer awareness of cyber threats is also a crucial factor that influences how they assess the security of the services they use (Bajwa et al., 2023). Therefore, banks are required not only to improve service quality but also to actively enhance customer awareness of cybersecurity measures. Banks that focus on both will be more successful in building and maintaining customer trust compared to those that only focus on the technical aspects of security. This indicates that a holistic approach, combining technical aspects and customer education, is key to addressing the negative impact of cybercrime on customer trust in e-banking.

H1: Cyber crime affects customer trust in using e-banking

Cyber Security and Customer Trust

Cybersecurity has a significant impact on customer trust in e-banking, as it directly influences their perception of the security and reliability of online banking services. Studies show that a robust cybersecurity framework can enhance customer trust by protecting personal and financial information from cyber threats. Specifically, awareness of cybersecurity measures plays a crucial role in shaping trust; customers who actively engage with secure e-banking systems are more likely to have higher levels of trust (Bajwa et al., 2023). Therefore, it can be hypothesized that banks that proactively educate customers about security measures and implement cutting-edge security technologies will experience a significant increase in customer trust compared to banks that do not have a similar strategy.

On the other hand, the quality of e-banking services, including reliability and security features, also plays a critical role in building customer trust. Research indicates that perceptions of the reliability and security of e-banking platforms are directly linked to the level of customer trust, highlighting the importance for banks to prioritize these aspects in order to build a loyal customer base (Gill et al., 2021). In addition, investment in advanced security mechanisms, such as multi-factor authentication and transaction encryption, has been proven to enhance user trust in e-banking services (Almaiah et al., 2023). Conversely, shortcomings in cybersecurity can lead to a significant decline in trust, with privacy and security risks becoming major barriers to service adoption (Peong et al., 2021). Thus, banks that not only improve service quality but also actively mitigate security risks will be more successful in building and maintaining customer trust and loyalty compared to those that neglect these aspects.

H2: Cyber security affects customer trust in using e-banking

Cyber Crime, Cyber Security and Customer Trust

The simultaneous influence of cybercrime and cybersecurity on consumer trust in e-banking is a complex and interrelated phenomenon, requiring a deep understanding of how these two factors affect each other. The rise in cybercrime creates an atmosphere of uncertainty and distrust among consumers regarding the security of their transactions, which can hinder the adoption and continued use of e-banking services. (Lagazio et al. 2014) it underscores that the financial sector is highly vulnerable to cyberattacks, which can result in significant financial losses and decreased customer loyalty. This perceived risk often influences consumers' decisions to avoid e-banking services due to concerns about

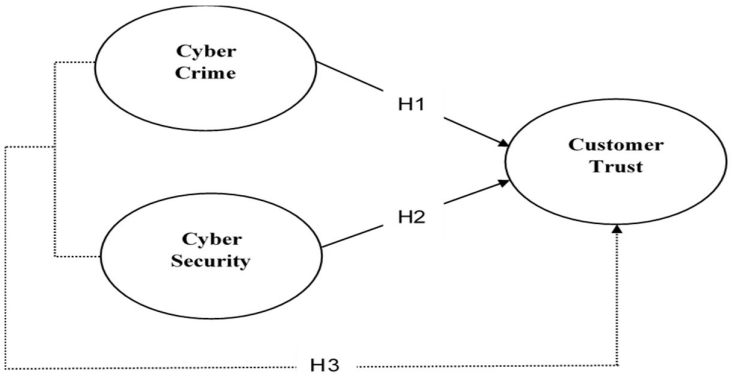
potential fraud or data breaches (Rezk et al., 2017). Therefore, there is an urgent need to implement robust cybersecurity measures to mitigate the negative effects of cybercrime and restore consumer trust.

Conversely, the implementation of effective cybersecurity strategies can play a vital role in reducing the negative impact of cybercrime and strengthening consumer trust. (Amer 2023) it shows that proactive strategies, including employee training and awareness campaigns, can reduce the risk of cybercrime and create a secure banking environment. (Khalil et al.2021) it emphasizes that expenditures on cybersecurity should be viewed as a strategic investment that can enhance financial performance and consumer trust in e-banking. By focusing on security and transparency, banks can improve consumer perceptions of cybersecurity, thereby encouraging broader adoption of e-banking services (Peong et al., 2021).

H3: Cyber Crime and Cyber security simultaneously affect customer trust in using e-banking.

Figure 3.

Research Model



Method

This study uses a quantitative approach with a correlational design to examine the relationship between cybercrime and cybersecurity, as well as their impact on customer trust in the context of digital banking transactions at Bank Syariah Indonesia (BSI) Palu Gajah Mada Branch. The aim of this research is to understand how the interaction between cybercrime threats and the cybersecurity measures implemented by the bank can affect customer perceptions of the security and reliability of e-banking services.

Cybercrime is measured using indicators that reflect customers' knowledge of cybercrime risks and their experiences with cyber incidents, which are adapted from previous research studies (Riek et al. 2016). Meanwhile, cybersecurity is assessed based on the elements of availability, confidentiality, integrity, authentication, and accountability, which are derived from a model developed by (Ernest Chang & Lin 2007). Customer trust is measured by examining the bank's reputation, customer satisfaction, and the integrity of the bank, in accordance with studies conducted by (van Esterik-Plasmeijer & van Raaij 2017). This study was conducted at BSI Palu Gajah Mada Branch, with the population consisting of all customers of that branch. Using Slovin's formula, the sample size was determined to be 100 respondents, selected through the Accidental Sampling method, which is expected to provide a good representation of the population.

The data collected is then analyzed using SPSS software. The analysis includes validity and reliability testing of the measurement instruments, as well as multiple linear regression analysis to evaluate the significance of the influence of cybercrime and cybersecurity on customer trust. Hypothesis testing is conducted to assess whether the observed influence is statistically significant. It is expected that the results of this study will provide valuable insights for bank managers in designing more effective digital security strategies, thereby enhancing customer trust in the e-banking services provided by BSI.

Results and Discussion

Results

Demographic Profile of Respondents

This demographic profile shows that the majority of respondents are aged 15 to 24 years (90%), indicating that the survey was largely completed by individuals who are still in the educational phase or at the beginning of their careers. This dominance of younger age is further emphasized by the fact that 69% of respondents are students, highlighting the survey's focus on the age group currently engaged in higher education. In terms of gender, there is a clear imbalance, with more female respondents (66%) compared to male respondents (34%). This may reflect higher participation from women in this survey or could be related to the context of the survey, which might be more relevant to women.

In terms of education, the majority of respondents have completed their education at the high school level (56%) or hold a bachelor's degree (40%), indicating a relatively high

level of education among the survey participants. Regarding employment, most respondents are students (69%), with a very small number engaged in formal jobs, such as private sector employees (15%) or self-employed individuals (12%). Respondents' income is predominantly in the group earning less than Rp. 1,000,000 (61%), suggesting potential financial dependency on parents or limited resources. The high usage of e-banking, with the majority of respondents using the service 5-7 times (46%) or more than 7 times (30%), indicates widespread adoption of banking technology among them. This profile reflects a combination of a young age group with higher education, low income levels, and significant use of technology.

Tabel 1.
Demographic Profile

Demographic Profile	Respondent	Percent (%)
Age		
15-24 years	90	90
25-39 years	9	9
40-54 years	1	1
55 years and above	0	0
Gender		
Male	34	34
Female	66	66
Education Level		
Elementary School	0	0
Junior High School	0	0
Senior High School	56	56
Bachelor (Strata 1)	40	40
Master (Strata 2)	4	4
Doctoral (Strata 3)	0	0
Work		

Demographic Profile	Respondent	Percent (%)
Civil Servant (PNS)	2	2
Private Employee	15	15
Self-employed	12	12
Housewife	0	0
Student	69	69
Laborer/Farmer/Fisherman	2	2
Incomes		
< Rp.1.000.000	61	61
> Rp.1.000.000 – Rp.2.000.000	11	11
> Rp.2.000.000 – Rp.3.000.000	14	14
> Rp.3.000.000	14	14
Frequently Used E-Banking		
Never	0	0
1 - 4 times	24	24
5 - 7 times	46	46
> 7 times	30	30

Validity and Reliability

Based on the factor analysis for the three main variables related to security and trust in the context of digital banking—Cyber Crime, Cyber Security, and Customer Trust—this analysis includes the statement items along with their factor loadings, which indicate the strength of the relationship between each item and its corresponding variable. Additionally, Cronbach's Alpha values are provided to measure the internal consistency of each variable.

From the results in the table, it can be observed that the Cyber Crime variable has factor loadings ranging from 0.766 to 0.858, with a Cronbach's Alpha value of 0.893. This indicates that the items are consistent in measuring the dimension of cyber crime. The

Cyber Security variable exhibits very high factor loadings, with the highest value reaching 0.944 and an excellent Cronbach's Alpha value of 0.969, indicating that this variable is very solid and consistent in assessing cybersecurity aspects. Meanwhile, the Customer Trust variable also shows good factor loadings, although slightly lower than Cyber Security, with a Cronbach's Alpha value of 0.918, suggesting that this variable is also quite consistent in measuring customer trust. Overall, these analysis results indicate that the instruments used in this survey are reliable for measuring key aspects related to security and trust in digital banking.

Tabel 2.

Hasil Uji Validitas dan Reliabilitas

Variabel	Item Pernyataan	Factor Loading	Nilai Crobach's Alpha
Cyber Crime	CC.1	0,858	0,893
	CC.2	0,817	
	CC.3	0,809	
	CC.4	0,837	
	CC.5	0,766	
	CC.6	0,766	
Cyber Security	CS.1	0,942	0,969
	CS.2	0,942	
	CS.3	0,797	
	CS.4	0,939	
	CS.5	0,940	
	CS.6	0,943	
	CS.7	0,942	
	CS.8	0,944	
	CS.9	0,779	
	CS.10	0,679	

Customer Trust	TR.1	0,865	0,918
	TR.2	0,891	
	TR.3	0,879	
	TR.4	0,902	
	TR.5	0,837	
	TR.6	0,632	

Classical Assumptions

The results of the classical assumption tests displayed in the table show that the model used meets the basic statistical assumption criteria, which are crucial for regression analysis. The normality test using the Kolmogorov-Smirnov method yielded a Z value of 0.076 and an Asymp. Sig. of 0.169, both of which are greater than 0.05. This indicates that the data is normally distributed, which is an essential prerequisite for inferential validity in regression models.

Furthermore, the results of the multicollinearity test show that the Variance Inflation Factor (VIF) values for the Cyber Crime and Cyber Security variables are 1.773, which is below the threshold of 5. This indicates no multicollinearity issues, meaning there is no excessive interaction between the independent variables in the model. The heteroscedasticity test also shows significance values greater than 0.05 for both variables (Cyber Crime: 0.149 and Cyber Security: 0.972), which means that the residual variance remains constant across the range of predictors..

Tabel 3.

Hasil Uji Asumsi Klasik

Classical Assumption Test	Criteria	Result	Decision
Normality			
Kolmogorov-Smirnov Z	Z and Sig. > 0,05	0,076	Normally Distributed
Asymp. Sig. (2-tailed)		0,169	

Classical Assumption Test	Criteria	Result	Decision
Multicollinearity			
Cyber Crime	VIF < 5	1,773	No Multicollinearity
Cyber Security		1,773	
Heteroscedasticity			
Cyber Crime	Sig. > 0,05	0,149	No Heteroscedasticity
Cyber Security		0,972	

Hypothesis Test

The results of the hypothesis analysis, which explore the relationship between Cyber Crime, Cyber Security, and consumer trust, involve testing two main hypotheses to determine the extent to which cybercrime and cybersecurity influence the level of consumer trust in the digital context. The coefficients, t-statistics, and significance levels are used to measure the strength and direction of the relationships between these variables.

The interpretation of the table shows that the first hypothesis (H1) indicates a significant negative relationship between cybercrime and consumer trust, with a coefficient of -0.356 and a t-statistic of -4.335. This suggests that as the level of cybercrime increases, consumer trust decreases. On the other hand, the second hypothesis (H2) shows a significant positive relationship between cybersecurity and consumer trust, with a coefficient of 0.295 and a t-statistic of 6.564. This means that improving cybersecurity significantly increases consumer trust. Both of these results are statistically significant, as reflected in the significance value of 0.000, reinforcing the importance of managing cybersecurity to maintain consumer trust in the digital ecosystem.

Tabel 4.

Hasil Uji Results of Hypothesis Testing through T-test Coefficients

Hypothesis	Relationship	Coefficient	SE	T statistic	Significance
H1	CC -> CT	-0,356	0,082	-4,335	0,000

Hypothesis	Relationship	Coefficient	SE	T statistic	Significance
H2	CS -> CT	0,295	0,045	6,564	0,000

Note: CC: Cyber Crime, CS: Cyber Security, CT: Consumer Trust

Meanwhile, the results of the third hypothesis analysis (H3), which examines the simultaneous relationship between the independent variables, namely Cyber Crime and Cyber Security, and the dependent variable, consumer trust, are as follows. The F Statistic, significance level, and Adjusted R Square value were used to evaluate how well this model explains the variability in consumer trust. The interpretation of the table reveals that the F Statistic result of 88.164 with a significance level of 0.000 indicates that this model is highly significant overall. This means that the combination of cybercrime and cybersecurity variables together contributes significantly to consumer trust. The Adjusted R Square value of 0.638 indicates that 63.8% of the variability in consumer trust can be explained by this model, while the remaining variability is influenced by other factors not included in this analysis. These results highlight the importance of considering both cybercrime and cybersecurity simultaneously in efforts to maintain and enhance consumer trust in the digital era.

Tabel 5.

Results of Hypothesis Testing through the F-Test and Determination (R2) Test

Hypothesis	F Statistic	Significance	Adjusted R Square
H3	88,164	0,000	0,638

Discussion

The results of this study provide deep insights into the dynamics between cybercrime, cybersecurity, and consumer trust in the increasingly complex digital banking environment, particularly in the context of Bank Syariah Indonesia (BSI). The findings from the first hypothesis (H1) indicate that cybercrime has a significant negative impact on consumer trust, with a negative coefficient of -0.356. This suggests that each increase in cybercrime incidents has the potential to substantially lower consumer trust, which could threaten BSI's reputation and reduce public confidence in digital Islamic banking services.

This impact becomes even more relevant in an era where cybercrime is becoming more rampant and complex, as emphasized by (Lagazio et al. 2014) which identifies the financial sector as a primary target for cybercriminals, potentially leading to significant financial losses and a decline in customer loyalty. In this context, BSI needs to address the risks of cybercrime with more advanced and proactive strategies to maintain trust and long-term relationships with customers.

Second hypothesis (H2) emphasizes the importance of cybersecurity in enhancing consumer trust, with a positive coefficient of 0.295 and a statistically significant T-statistic. This suggests that effective cybersecurity measures not only protect customer data but also increase their confidence in BSI's digital Sharia platforms. This aligns with the principle of mashlahahiyat in Sharia risk management, which prioritizes the protection and well-being of customers as the primary benefit of implementing Sharia. BSI's investment in cybersecurity can be viewed as a key strategy that not only protects but also strengthens customer loyalty, ultimately having a positive impact on the bank's overall business performance. (Rezk et al. 2017) this view is supported by showing that strong cybersecurity contributes to reducing customers' fears of cybercrime risks and reinforces their trust in digital banking platforms. When customers feel secure that their data and transactions are protected, their willingness to engage with digital banking services increases, leading to higher satisfaction and loyalty. This not only enhances the user experience but also strengthens the overall reputation of the bank, fostering long-term relationships with customers.

Third hypothesis (H3) emphasizes the importance of a holistic approach in considering both cybercrime and cybersecurity together in influencing consumer trust. With an F Statistic of 88.164 and an Adjusted R Square of 0.638, the results show that these two variables together explain more than 63% of the variability in consumer trust. However, there remains about 36.2% of the variability unexplained, indicating the presence of other factors such as service quality, transparency, and user experience, which also play a significant role. From a Sharia perspective, this suggests the importance of a tahsiniyat approach, which focuses on improving service quality and enhancing the customer experience to achieve higher levels of trust. This view aligns with the broader perspective, (Amer 2023) it emphasizes that, in addition to security, customer education and awareness also play a crucial role in creating a safe and trustworthy banking environment.

The implications of these results for BSI are the need to strengthen risk management integrated with Islamic principles, such as haruriyat (basic needs) which ensures the security and reliability of e-banking services, mashlahahiyat which emphasizes optimal benefits for customers, and tahsiniyat which focuses on improving service quality. BSI must enhance its cybersecurity system with a layered approach, including increased education for customers and employees, transparency in security procedures, and collaboration with regulators to comply with high security standards. Investment in technologies such as artificial intelligence (AI) and machine learning to proactively detect cyber threats is a relevant solution, as suggested by (Khalil et al. 2021), which states that investment in cybersecurity should be seen as a strategic move to improve financial performance and customer trust.

As a solution, BSI should also adopt a sustainable approach to risk management by strengthening customer education on good security practices in digital transactions, improving transparency by clearly and openly communicating security policies, and ensuring that security systems are continuously updated to face evolving threats. In this context, the tahsiniyat approach can be applied by improving and enriching the quality of digital services, thus providing a better user experience and enhancing overall consumer trust. With this approach, BSI can not only manage cybercrime risks more effectively but also strengthen consumer trust in secure and reliable sharia e-banking services, ultimately boosting BSI's competitiveness in the digital banking industry.

Conclusion

This study successfully reveals that cybercrime and cybersecurity have a significant impact on consumer trust in using e-banking services, particularly in the context of Bank Syariah Indonesia (BSI). The findings show that an increase in cybercrime incidents can significantly reduce customer trust, while the implementation of effective cybersecurity measures can enhance consumer confidence in the digital platform. This study also indicates that these two factors, when considered together, explain much of the variability in consumer trust, although other factors still need to be further explored. In the context of sharia risk management, these results emphasize the importance of a holistic approach that includes aspects of haruriyat, mashlahahiyat, and tahsiniyat to ensure that BSI not only protects customers from cybercrime risks but also strengthens their trust and loyalty through high-quality and transparent services.

Although this study provides important insights, there are several limitations that need to be acknowledged. First, this study is limited to the analysis of two main variables: cybercrime and cybersecurity, without considering other factors that may also significantly impact consumer trust, such as service quality, government regulations, and overall user experience. Second, this study uses data from a single sector of the Islamic banking industry in Indonesia, so the findings may not fully apply to other sectors or countries. For future research, it is recommended to broaden the scope of the study by including additional variables and conducting analyses across different industries and geographic regions to obtain a more comprehensive picture. Furthermore, a longitudinal study that tracks changes in consumer trust over time could provide deeper insights into the long-term impact of cybercrime and cybersecurity on consumer trust in the ever-evolving digital era

References

Abbas, T., & Arif, K. (2023). End-Users' Perception of Cybercrimes Towards E-Banking Adoption and Retention. *Journal of Independent Studies and Research - Computing*, *21*(1). https://doi.org/10.31645/jisrc.23.21.1.10

Abdul Sathar, M. B., Rajagopalan, M., Naina, S. M., & Parayitam, S. (2022). A moderated-mediation model of perceived enjoyment, security and trust on customer satisfaction: evidence from banking industry in India. *J. Asia Bus. Stud.* https://doi.org/10.1108/jabs-03-2022-0089

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 5.

Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. *Sustainability*, *15*(13), 9908. https://doi.org/10.3390/su15139908

Alsheyyab, M. M. A., & Singh, D. (2013). Effect of trust on E-banking user's satisfaction: A review. *Research Journal of Applied Sciences Engineering and Technology*, *5*(4), 1397–1406. https://doi.org/10.19026/rjaset.5.4879

Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications : IJACSA*, *14*(8). https://doi.org/10.14569/ijacsa.2023.0140841

Anouze, A. L. M., & Alamro, A. S. (2019). Factors affecting intention to use e-banking in Jordan. *International Journal of Bank Marketing*, *38*(1), 86–112. https://doi.org/10.1108/ijbm-10-2018-0271

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. *Information and Computer Security*, *31*(5), 635–654. https://doi.org/10.1108/ics-11-2022-0179

Daniel, W. K., William, K. F., Ling, M., Lai, S. M., & Tevanotai, A. (2014). *Awareness in E-Banking Security and Usage*. https://doi.org/10.1109/infoseee.2014.6947856

Ernest Chang, S., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*(3), 438–458. https://doi.org/10.1108/02635570710734316

Gani, T. A. (2023). *Kedaulatan data digital untuk integritas bangsa*. Syiah Kuala University Press.

Gill, A. A., Ansari, R. H., Akram, K., & Tufail, M. W. (2021). Application of cognitive motivational relational theory to examine the influence of E-banking quality factors on customer loyalty. *Journal of Accounting and Finance in Emerging Economies*, *7*(1), 241–249. https://doi.org/10.26710/jafee.v7i1.1608

Hammoud, J., Bizri, R. M., & El Baba, I. (2018). The impact of E-banking service quality on customer satisfaction: Evidence from the Lebanese banking sector. *SAGE Open*, *8*(3), 215824401879063. https://doi.org/10.1177/2158244018790633

Isa, M., Fadlilah, H., Hamid, A., & Lestari, E. (2022). The effect of trust and risk on Interest Using mobile banking. *Journal of Islamic Financial Technology*, *1*(1). https://doi.org/10.24952/jiftech.v1i1.5022

Juliana, J., Nurhaliza, F., Hermawan, R., & Marlina, R. (2023). Bank Syariah Indonesia Customer Loyalty After Merger: Analysis of Trust, Service Quality, and Religiosity. In *Jurnal Ekonomi Syariah Teori dan Terapan* (Vol. 10, Issue 1). https://doi.org/10.20473/vol10iss20231pp96-108

Kala Kamdjoug, J. R., Ndassi Teutio, A. O., Tchakounte Tchouanga, U., & Gueyie, J.-P. (2022). Use of E-banking and customer E-engagement in developing countries: Case of NFC bank Cameroon. *Theor. Econ. Lett.*, *12*(05), 1378–1406. https://doi.org/10.4236/tel.2022.125076

Khalil, K., Manzoor, S. R., Tahir, M., Khan, N., & Jamal, K. (2021). Impact of cyber security cost on the financial performance of e-banking: Mediating influence of product innovation performance. *Humanities & Social Sciences Reviews*, *9*(2), 691–703. https://doi.org/10.18510/hssr.2021.9266

Khoirunnisa, M., & Trishananto, Y. (2023). Trust in mediating the relationship between security and feature availability on customer statisfaction using mobile banking. *IQTISHADUNA*, *14*(1), 11–22. https://doi.org/10.20414/iqtishaduna.v14i1.6208

Lagazio, M., Sherif, N., & Cushman, M. (2014). A Multi-Level Approach to Understanding the Impact of Cyber Crime on the Financial Sector. *Computers & Security*, *45*, 58–74. https://doi.org/10.1016/j.cose.2014.05.006

Lestari, H. B., & Saibil, D. I. (2022). Implication of relationship marketing on loyalty with brand image as A moderation variable. *Al-Amwal J. Ekon. Dan Perbank. Syari Ah*, *14*(2), 183. https://doi.org/10.24235/amwal.v14i2.11183

Lubis, A., Effendi, I., & Rosalina, D. (2022). Pengaruh Kepercayaan dan Komitmen Terhadap Loyalitas Nasabah Bank Syariah Indonesia di Kota Medan. In *Ekonomi, Keuangan, Investasi dan Syariah (EKUITAS)* (Vol. 3, Issue 4). https://doi.org/10.47065/ekuitas.v3i4.1600

Mawarni, R., Iqbal Fasa', M., & Suharto. (2021). Penerapan Digital Banking Bank Syariah Sebagai Upaya Customer Retantion Pada Masa Covid-19. *Al Iqtishod: Jurnal Pemikiran Dan Penelitian Ekonomi Islam*, *9*(2), 39–54.

Medyawati, H. (2011). The influence of computer self efficacy, computer experience and interface design to acceptance of electronic banking: Empirical study of bank customers in bekasi city. *International Journal of E-Education e-Business e-Management and e-Learning*. https://doi.org/10.7763/ijeeee.2011.v1.50

Mulia, D., Usman, H., & Parwanto, N. B. (2021). The role of customer intimacy in increasing Islamic bank customer loyalty in using e-banking and m-banking. *J. Islam. Mark.*, *12*(6), 1097–1123. https://doi.org/10.1108/jima-09-2019-0190

Muna, N. A., Ramadhan, F. I., & Citradewi, A. (2023). Analisis Perkembangan Profitabilitas Bank Syariah di Indonesia Pasca Merger Menjadi Bank Syariah Indonesia. *EL MUDHORIB: Jurnal Kajian Ekonomi Dan Perbankan Syariah*, *4*(1), 12–25.

Peong, K. K., Peong, K. P., & Tan, K. Y. (2021). Behavioural Intention of Commercial Banks' Customers Towards Financial Technology Services. *Gatr Journal of Finance and Banking Review*, *5*(4), 10–27. https://doi.org/10.35609/jfbr.2021.5.4(2)

Putri, T. M., & Briliana, V. (2023). Pengaruh Trust, Commitment, Brand Image, Service Quality, dan Customer Value terhadap Customer Satisfaction: Studi Kasus pada Nasabah BSI di Jakarta. *Mb*, *15*(2), 279–296. https://doi.org/10.34208/mb.v15i2.2195

Rezk, A., Barakat, S., & Saleh, H. (2017). The Impact of Cyber Crime on E-Commerce. *International Journal of Intelligent Computing and Information Sciences*, *17*(3), 85–96. https://doi.org/10.21608/ijicis.2017.30055

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273. https://doi.org/10.1109/TDSC.2015.2410795

Saputra, M. A., & Rahmawaty, A. (2023). The role of Islamic Service Quality on Intention to Use Indonesian Islamic Bank: Trust as an Intervening Variable. *MALIA: Journal of Islamic Banking and Finance*, *7*(1), 13. https://doi.org/10.21043/malia.v7i1.20547

Shankar, A., & Jebarajakirthy, C. (2019). The influence of e-banking service quality on customer loyalty. *Int. J. Bank Mark.*, *37*(5), 1119–1142. https://doi.org/10.1108/ijbm-03-2018-0063

Tiwari, P. (2021). Electronic banking adoption in Ethiopia: an empirical investigation. *SN Bus. Econ.*, *1*(9). https://doi.org/10.1007/s43546-021-00114-0

van Esterik-Plasmeijer, P. W. J., & van Raaij, W. F. (2017). Banking system trust, bank trust, and bank loyalty. *International Journal of Bank Marketing*, *35*(1), 97–111. https://doi.org/10.1108/IJBM-12-2015-0195

Widjajanta, B., Anon, L., & Tanuatmodjo, H. (2021). Islamic ethical behavior to bear out customer trust: Perspective Islamic bank in Indonesia. *Theijbm*, *9*(11). https://doi.org/10.24940/theijbm/2021/v9/i11/bm2111-026