INSPIRE: International Journal of Islamic Economics and Entrepreneurship Studies
Vol. 1, No. 1, June 2026, 23-36
Open Access: https://journal.bacaanmedia.id/index.php/inspire/index
Publshed by Bacaan Media

The Impact of Data Security and Privacy Risks on Muslim Customers Trust in Using BYOND by BSI

Putri Purnama Sari[1], Edy Santoso[2]
[1,2]University of Jember, Indonesia
Email: [1]putripurnamasari2404@gmail.com, [2]edysantoso@unej.ac.id

ARTICLE INFO

Kata Kunci:
Kepercayaan Nasabah; Keamanan Data; Risiko Keamanan; Privasi; BYOND by BSI

Keywords:
Customer Trust; Data Security; Data Security Risk; Privacy; BYOND by BSI

Article history:
Submitted: 19-04-2026
Revision: 20-05-2026
Accepted: 28-05-2026
Published: 11-06-2026

ABSTRAK

Perkembangan layanan perbankan digital telah meningkatkan kebutuhan akan sistem keamanan data dan perlindungan privasi yang mampu menjaga kepercayaan nasabah. Dalam konteks perbankan syariah, kepercayaan menjadi faktor yang sangat penting karena berkaitan dengan prinsip amanah dalam pengelolaan informasi dan transaksi nasabah. Penelitian ini bertujuan menganalisis pengaruh risiko keamanan data dan privasi terhadap kepercayaan nasabah Muslim dalam menggunakan BYOND by BSI di Kabupaten Jember. Penelitian menggunakan pendekatan kuantitatif dengan jenis explanatory research. Data diperoleh melalui penyebaran kuesioner kepada 96 nasabah Muslim pengguna BYOND by BSI yang dipilih menggunakan teknik purposive sampling. Analisis data dilakukan menggunakan Partial Least Square–Structural Equation Modeling (PLS-SEM) dengan bantuan SmartPLS 4. Hasil penelitian menunjukkan bahwa risiko keamanan data dan privasi berpengaruh positif dan signifikan terhadap kepercayaan nasabah Muslim. Risiko keamanan data memiliki pengaruh yang lebih kuat dibandingkan privasi dalam membentuk kepercayaan pengguna. Temuan ini mengindikasikan bahwa kemampuan bank dalam mengelola risiko keamanan, melindungi data pribadi, dan menjaga privasi nasabah berperan penting dalam meningkatkan kepercayaan terhadap layanan perbankan digital syariah. Penelitian ini memberikan implikasi praktis bagi pengembangan sistem keamanan dan tata kelola perlindungan data pada layanan digital perbankan.

ABSTRACT

The rapid development of digital banking services has increased the need for robust data security systems and privacy protection mechanisms capable of maintaining customer trust. Within the context of Islamic banking, trust is a critical factor as it is closely associated with the principle of *amanah* in managing customer information and financial transactions. This study aims to examine the impact of data security risks and privacy on Muslim customers' trust in using BYOND by BSI in Jember Regency. The research employs a quantitative approach using an explanatory research design. Data were collected through questionnaires distributed to 96 Muslim customers of BYOND by BSI selected through purposive sampling. The data were analyzed using Partial Least Square–Structural Equation Modeling (PLS-SEM) with SmartPLS 4. The findings reveal that both data security risks and privacy have a positive and significant effect on customer trust. Data security risk demonstrates a stronger influence than privacy in shaping customer trust. These results indicate that the bank's ability to manage security risks, protect personal information, and safeguard customer privacy plays a vital role in strengthening trust in Islamic digital banking services. The study provides practical implications for enhancing data protection governance and security systems in digital banking platforms.

INTRODUCTION

The rapid advancement of information and communication technologies has fundamentally transformed the global banking industry, including the Islamic banking sector. Digitalization has reshaped the way financial institutions deliver services, enabling customers to conduct transactions more efficiently, conveniently, and independently through digital platforms. As a result, mobile banking applications have become a strategic instrument for enhancing

customer experience and strengthening the competitiveness of banking institutions in an increasingly digital economy (Widyaputri & Gunanto, 2023; Ristya, 2024).

In Indonesia, Islamic banking institutions have actively embraced digital transformation to meet the evolving expectations of customers (Harahap et al., 2023; Astuti, 2024; Ghozali et al., 2025). As the largest Islamic bank in the country, Bank Syariah Indonesia (BSI) continues to expand its digital ecosystem through innovative financial technologies. One of its most significant initiatives is the introduction of BYOND by BSI, a digital banking application designed to provide integrated financial services while improving accessibility, efficiency, and user experience. The application represents BSI's commitment to supporting digital financial inclusion and strengthening its position within the rapidly growing Islamic digital banking market.

Despite the benefits offered by digital banking platforms, the expansion of technology-based financial services has also increased concerns regarding data security and privacy (Santoso et al., 2021; Haris & Manangin, 2024; Alfian et al., 2025). The collection, storage, and processing of customer information expose financial institutions to various cybersecurity threats, including unauthorized access, identity theft, data breaches, phishing attacks, and ransomware incidents. Such threats not only create operational and financial risks but also have the potential to undermine customer confidence in digital banking systems.

The issue of cybersecurity has become particularly relevant in the Indonesian banking sector following several high-profile incidents involving digital infrastructure vulnerabilities. Public awareness of data breaches and cyberattacks has heightened concerns regarding the ability of financial institutions to safeguard sensitive customer information. In digital environments where transactions occur remotely and personal data are continuously exchanged, customers increasingly evaluate banking services based on their perceptions of security and privacy protection. Consequently, maintaining trust has become one of the most critical challenges facing digital banking providers (Noer et al., 2023).

Customer trust is widely recognized as a fundamental determinant of technology adoption and long-term customer relationships (Asnawi & Setyaningsih, 2021; Babina et al., 2025). Trust reflects the belief that a service provider possesses the competence, integrity, and commitment necessary to protect customer interests. Within digital banking environments, trust becomes even more important because customers must rely on technological systems that they cannot directly observe or control. Therefore, perceptions regarding data security and privacy protection significantly influence customers' willingness to use and continue using digital banking services.

From an Islamic perspective, trust is closely associated with the concept of *amanah*, which emphasizes responsibility, honesty, and accountability in managing entrusted resources. Islamic financial institutions are expected not only to comply with legal and regulatory requirements but also to uphold ethical obligations in protecting customer assets and personal information (Jan et al., 2023; Meero, 2025; Wibowo et al., 2026). The management of customer data therefore extends beyond technical considerations and becomes part of the institution's moral responsibility. Consequently, maintaining data security and privacy can be viewed as an operational manifestation of *amanah* within contemporary Islamic banking practices.

Data security risk refers to the possibility that information systems may experience threats capable of compromising the confidentiality, integrity, or availability of customer data. In the context of digital banking, customers are particularly concerned about unauthorized transactions, financial fraud, identity theft, and misuse of personal information (Harahap et al., 2023; Wang et al., 2024). Previous studies have suggested that perceptions of effective security mechanisms, such as authentication systems, encryption technologies, transaction verification

procedures, and fraud detection tools, can strengthen customer confidence in digital financial services (Nofriansyah et al., 2026). However, empirical findings regarding the relationship between security risk perceptions and customer trust remain inconsistent across different contexts and technological environments.

In addition to security concerns, privacy has emerged as another critical factor influencing customer trust. Privacy refers to an individual's ability to control the collection, use, and dissemination of personal information. As digital banking services increasingly rely on extensive customer data, concerns regarding how information is stored, processed, and shared have become more prominent. Customers are more likely to trust digital platforms that demonstrate transparency, obtain informed consent, and provide clear assurances regarding the protection of personal information. Therefore, privacy protection represents not only a legal requirement but also a strategic component of customer relationship management.

Although the importance of security and privacy has been widely acknowledged, existing studies have produced mixed findings regarding their influence on trust in digital banking services. Some studies report that perceived security and privacy protection positively enhance customer trust, while others suggest that perceived risks may reduce confidence and hinder technology adoption (Jafri et al., 2024; Wang et al., 2024). Furthermore, limited attention has been given to these issues within the context of Islamic digital banking applications, particularly newly introduced platforms such as BYOND by BSI. This situation indicates the existence of a research gap concerning how Muslim customers evaluate security and privacy issues when developing trust toward Islamic digital banking services.

Given the strategic role of trust in ensuring the sustainability of digital banking adoption, examining the influence of data security risk and privacy on customer trust becomes increasingly important (Jan et al., 2023; Nasrun et al., 2025). Understanding these relationships can provide valuable insights for Islamic banking institutions seeking to strengthen customer confidence and improve digital service quality. Moreover, such understanding contributes to the broader discussion of digital trust within Islamic financial ecosystems, where technological innovation must remain aligned with ethical responsibility and the principle of *amanah*.

Based on these considerations, this study investigates the impact of data security risk and privacy on Muslim customers' trust in using BYOND by BSI. Specifically, the study seeks to examine whether perceptions of data security risk and privacy protection significantly influence customer trust and to assess the relative contribution of each factor in shaping trust toward Islamic digital banking services.

METHOD

This study employed a quantitative approach using an explanatory research design to examine the impact of data security risk and privacy on Muslim customers' trust in using BYOND by BSI (Sugiyono, 2023). The study was conducted in Jember Regency, Indonesia, which has experienced increasing adoption of Islamic banking and digital financial services. The target population consisted of Muslim customers who actively use the BYOND by BSI application. A non-probability sampling technique was applied through purposive sampling, whereby respondents were selected based on specific criteria relevant to the research objectives. Using the Lemeshow formula, a total of 96 respondents were determined as the sample for this study.

Primary data were collected through a structured questionnaire developed from established indicators in previous studies (Yusuf, 2006; Iba & Wardhana, 2023). The

questionnaire measured three constructs: data security risk, privacy, and customer trust. Data security risk was assessed through indicators related to payment security, transaction security, authentication, verification, information misuse, and information access. Privacy was measured using indicators associated with legal protection, personal data collection, information-sharing consent, and user comfort in providing personal information. Meanwhile, customer trust was evaluated based on the dimensions of ability, benevolence, and integrity.

The collected data were analyzed using Partial Least Square–Structural Equation Modeling (PLS-SEM) with SmartPLS 4 software (Hair et al., 2019; Huang, 2022). The analysis consisted of three stages. First, the measurement model (*outer model*) was evaluated to assess the validity and reliability of the constructs through convergent validity, discriminant validity, composite reliability, Cronbach's alpha, and Average Variance Extracted (AVE). Second, the structural model (*inner model*) was examined to evaluate the relationships among variables through path coefficients and the coefficient of determination (R^2). Finally, hypothesis testing was conducted using the bootstrapping procedure to determine the significance of the effects of data security risk and privacy on Muslim customers' trust in using BYOND by BSI.

RESULT AND DISCUSSION

The empirical findings indicate that data security risk and privacy exert distinct influences on Muslim customers' trust in using BYOND by BSI. These differences are reflected in the statistical testing results, both at the measurement model and structural model levels. Prior to examining the relationships among variables, the measurement model was evaluated to ensure that the constructs met the required standards of validity and reliability. The results of these assessments are presented below.

Result

A. Measurement Model Assessment (*Outer Model*)

The measurement model was evaluated to assess the validity and reliability of the research constructs. The assessment included tests of convergent validity, discriminant validity, and construct reliability. These procedures are essential to ensure that the indicators accurately measure their intended latent constructs and provide consistent results.

1. Convergent Validity

Convergent validity was assessed using factor loadings and Average Variance Extracted (AVE). According to the recommended threshold, indicator loadings should exceed 0.70, while AVE values should be greater than 0.50 to demonstrate adequate convergent validity.

Table 1. Convergent Validity Results (Factor Loadings)

Variable	Indicator	Loading Factor		
		Score	Rule of Thumb	Description
Data Security Risk (X1)	X1.1	0.802	0.700	Valid
	X1.2	0.797	0.700	Valid
	X1.3	0.713	0.700	Valid
	X1.4	0.706	0.700	Valid
	X1.5	0.804	0.700	Valid
	X1.6	0.744	0.700	Valid

Privacy (X2)	X2.1	0.751	0.700	Valid
	X2.2	0.736	0.700	Valid
	X2.3	0.785	0.700	Valid
	X2.4	0.798	0.700	Valid
Trust (Y)	Y1.1	0.806	0.700	Valid
	Y1.2	0.767	0.700	Valid
	Y1.3	0.798	0.700	Valid

Source: Primary data processed by the authors (2026)

The results presented in Table 1 show that all indicators exhibit factor loading values above the recommended threshold of 0.70. The loading values for the Data Security Risk construct range from 0.706 to 0.804, the Privacy construct ranges from 0.736 to 0.798, and the Customer Trust construct ranges from 0.767 to 0.806. These findings indicate that all indicators adequately represent their respective constructs and satisfy the requirements of convergent validity.

Table 2. Average Variance Extracted (AVE) Results

Variable	Average Variance Extracted (AVE)		Description
	Score	Rule of Thumb	
Data Security Risk (X1)	0.581	0.500	Valid
Privacy (X2)	0.590	0.500	Valid
Trust (Y)	0.625	0.500	Valid

Source: Primary data processed by the authors (2026)

The AVE values for Data Security Risk, Privacy, and Customer Trust are 0.581, 0.590, and 0.625, respectively. Since all values exceed the recommended threshold of 0.50, the constructs demonstrate satisfactory convergent validity. This indicates that each construct explains more than half of the variance of its indicators and effectively captures the underlying concept being measured.

2. Discriminant Validity

Discriminant validity was evaluated using the cross-loading criterion. A construct is considered to possess adequate discriminant validity when each indicator exhibits a higher loading on its associated construct than on any other construct.

Table 3. Cross-Loading Results

Item	Data Security Risk (X1)	Privacy (X2)	Trust (Y)
X1.1	0.802	0.388	0.464
X1.2	0.797	0.484	0.643
X1.3	0.713	0.635	0.436
X1.4	0.706	0.692	0.429
X1.5	0.804	0.499	0.581
X1.6	0.744	0.479	0.435
X2.1	0.510	0.751	0.536
X2.2	0.533	0.736	0.383
X2.3	0.544	0.785	0.431
X2.4	0.516	0.798	0.476

Y1.1	0.568	0.482	0.806
Y1.2	0.532	0.440	0.767
Y1.3	0.482	0.511	0.798

Source: Authors' calculation based on primary survey data (2026)

The results reveal that all indicators load more strongly on their respective constructs than on other constructs within the model. Furthermore, the primary loadings of all indicators exceed the recommended threshold of 0.70. These findings confirm that each construct is empirically distinct from the others and that the measurement model satisfies the requirements of discriminant validity.

3. Reliability Assessment

Construct reliability was assessed using Cronbach's Alpha and Composite Reliability. Both measures should exceed 0.70 to indicate acceptable internal consistency.

Table 4. Reliability Results

Variable	Cronbach's Alpha	Composite Reliability	Rule of Thumb	Description
Data Security Risk (X1)	0.856	0.892	0.700	Reliable
Privacy (X2)	0.770	0.852	0.700	Reliable
Trust (Y)	0.701	0.834	0.700	Reliable

Source: Authors' calculation based on primary survey data (2026)

The findings show that Data Security Risk achieved a Cronbach's Alpha value of 0.856 and a Composite Reliability value of 0.892. Privacy recorded values of 0.770 and 0.852, respectively, while Customer Trust obtained values of 0.701 and 0.834. All values exceed the recommended threshold of 0.70, indicating that the constructs possess strong internal consistency and reliability.

Overall, the results of the measurement model assessment demonstrate that all constructs satisfy the criteria for convergent validity, discriminant validity, and reliability. Therefore, the indicators employed in this study are considered appropriate for measuring data security risk, privacy, and customer trust, allowing the analysis to proceed to the evaluation of the structural model and hypothesis testing.

B. Measurement Model Assessment (*Outer Model*)

The structural model was evaluated to examine the relationships among the latent variables and to assess the explanatory and predictive power of the proposed research model. The evaluation included the analysis of path coefficients, the coefficient of determination (R^2), and hypothesis testing. These procedures provide insights into the direction, strength, and significance of the relationships between data security risk, privacy, and customer trust.

1. Path Coefficients

Path coefficient analysis was conducted to determine the direction and magnitude of the relationships between the independent variables and the dependent variable. The results are presented in figure 1.

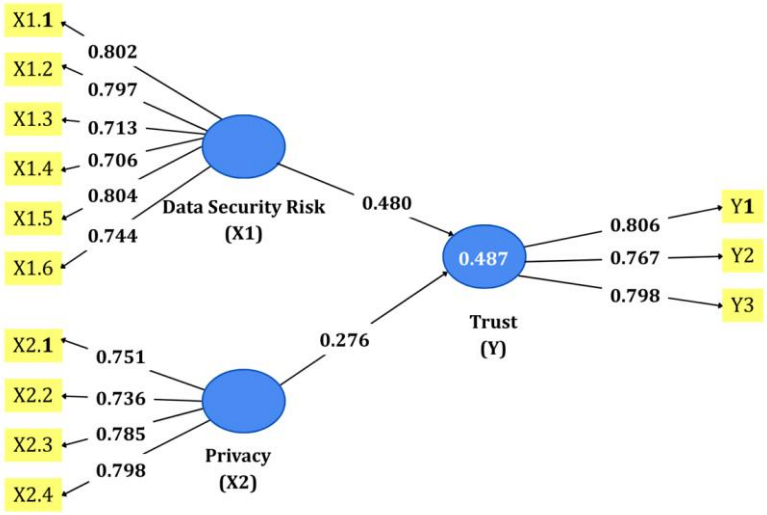

Figure 1. Path Coefficients

Figure 1 illustrates the structural relationships among the latent variables included in the research model. The diagram presents the estimated path coefficients between Data Security Risk, Privacy, and Customer Trust, indicating the direction and strength of the relationships. Both exogenous variables display positive path coefficients toward Customer Trust, suggesting that perceptions of data security and privacy protection are associated with higher levels of trust in using BYOND by BSI. To assess the statistical significance of these relationships, the path coefficient estimates and corresponding *p-values* are presented in Table 5.

Table 5. Direct Effect Significance Test Results

Path	Path Coefficient (β)	p-Value	Decision
Data Security Risk (X1) → Trust (Y)	0.480	0.000	Supported
Privacy (X2) → Trust (Y)	0.276	0.015	Supported

Source: Authors' calculation based on primary survey data (2026)

The results indicate that both independent variables have a positive and statistically significant effect on customer trust. The relationship between Data Security Risk and Customer Trust exhibits a path coefficient of 0.480 with a p-value of 0.000, indicating a significant positive effect at the 5% significance level. This finding suggests that customers' perceptions regarding the effectiveness of data security mechanisms contribute substantially to strengthening their trust in using BYOND by BSI.

Similarly, Privacy demonstrates a positive and significant effect on Customer Trust, with a path coefficient of 0.276 and a p-value of 0.015. The result indicates that customers who perceive stronger privacy protection are more likely to trust the digital banking platform. Comparing the two coefficients, Data Security Risk exhibits a stronger influence on Customer Trust than Privacy, suggesting that security-related considerations play a more prominent role in shaping trust among users of Islamic digital banking services.

2. Coefficient of Determination (R^2)

The coefficient of determination (R^2) was examined to evaluate the explanatory power of the model. The results are presented in Table 6.

Table 6. Coefficient of Determination (R^2)

Variable	R^2	Adjusted R^2	Interpretation
Customer Trust (Y)	0.487	0.476	Moderate

Source: Processed primary data, 2026

The results show that the R^2 value for Customer Trust is 0.487, while the adjusted R^2 value is 0.476. According to commonly accepted PLS-SEM criteria, this value indicates a moderate level of explanatory power. Specifically, Data Security Risk and Privacy jointly explain 48.7% of the variance in Customer Trust. The remaining 51.3% is attributable to other factors not included in the present model, such as perceived usefulness, service quality, user experience, brand reputation, religiosity, and technological readiness.

Overall, the structural model demonstrates satisfactory explanatory capability, indicating that both data security risk and privacy are important determinants of Muslim customers' trust in using BYOND by BSI. The findings further suggest that enhancing security mechanisms and strengthening privacy protection policies can play a significant role in increasing customer confidence in Islamic digital banking services.

3. Effect Size Assessment (f^2)

The effect size (f^2) was examined to determine the relative contribution of each exogenous variable to the endogenous construct. According to established PLS-SEM guidelines, f^2 values of 0.02, 0.15, and 0.35 indicate small, medium, and large effects, respectively.

Table 7. Effect Size (f^2) Results

Variable	Trust (Y)	Description
Data Security Risk (X1)	0.240	Medium
Privacy (X2)	0.079	Small

Source: Processed primary data, 2026

The results indicate that Data Security Risk exhibits an f^2 value of 0.240, suggesting a moderate effect on Customer Trust. This finding implies that perceptions of data security play a substantial role in shaping customer trust toward BYOND by BSI. In contrast, Privacy demonstrates an f^2 value of 0.079, indicating a small effect size. Although privacy significantly influences trust, its contribution is relatively weaker compared to data security risk. These findings suggest that customers place greater emphasis on the security of digital transactions and personal information protection when evaluating the trustworthiness of Islamic digital banking services.

4. Predictive Relevance Assessment (Q^2)

The predictive relevance of the model was assessed using the blindfolding procedure. The Q^2 statistic evaluates the model's capability to predict endogenous constructs and determine whether the model possesses sufficient predictive accuracy.

Table 8. Predictive Relevance (Q^2) Results

Construct	Q^2 Predict	RMSE	MAE
Customer Trust (Y)	0.434	0.768	0.573

Source: Processed primary data, 2026

The results reveal a Q^2 value of 0.434 for Customer Trust. Since the value exceeds zero, the model demonstrates adequate predictive relevance. Specifically, the model possesses a predictive capability of approximately 43.4%, indicating that the proposed structural model is capable of predicting customer trust with satisfactory accuracy. These findings confirm that the model is relevant for explaining the relationships among data security risk, privacy, and customer trust within the context of BYOND by BSI.

5. Hypothesis Testing

Hypothesis testing was conducted using the bootstrapping procedure in SmartPLS 4 to assess the significance of the relationships among the variables. The hypotheses were evaluated based on *p-values*, *t-statistics*, and path coefficients. A relationship was considered significant when the *p-value* was below 0.05 and the *t-statistic* exceeded 1.64 at the 5% significance level.

Table 9. Hypothesis Testing Results

Relationship	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T-Statistic	P-Value	Result
X1 → Y	0.480	0.484	0.113	4.263	0.000	Significant
X2 → Y	0.276	0.285	0.127	2.169	0.015	Significant

Source: Processed primary data, 2026

The findings indicate that Data Security Risk has a positive and significant effect on Customer Trust. The relationship is supported by a path coefficient of 0.480, a *t-statistic* of 4.263, and a *p-value* of 0.000. These values satisfy the established significance criteria, indicating that improvements in customers' perceptions of data security are associated with higher levels of trust in using BYOND by BSI. Therefore, the first hypothesis, which proposed a negative effect of data security risk on customer trust, is not supported. Instead, the findings reveal a significant positive relationship between the two variables.

Similarly, Privacy demonstrates a positive and significant effect on Customer Trust, with a path coefficient of 0.276, a *t-statistic* of 2.169, and a *p-value* of 0.015. These results indicate that customers who perceive stronger privacy protection tend to exhibit higher levels of trust toward the digital banking platform. Accordingly, the second hypothesis is supported.

Overall, the hypothesis testing results confirm that both Data Security Risk and Privacy significantly influence Muslim customers' trust in using BYOND by BSI. However, Data Security Risk exerts a stronger effect than Privacy, suggesting that security-related considerations are the primary determinant of trust formation within Islamic digital banking services. This finding highlights the importance of strengthening cybersecurity infrastructure, transaction protection mechanisms, and customer data safeguards to maintain and enhance trust in digital banking platforms.

Discussion

A. The Effect of Data Security Risk on Muslim Customers' Trust in Using BYOND by BSI

The findings reveal that Data Security Risk has a positive and significant effect on Muslim customers' trust in using BYOND by BSI, as evidenced by a *p-value* of 0.000, a *t-statistic* of 4.263, and a path coefficient of 0.480. Interestingly, the direction of the relationship differs from the

initial hypothesis, which predicted a negative association. Consequently, H1 is not supported. This finding suggests that customers do not necessarily perceive data security risk as a factor that diminishes trust. Instead, they interpret the presence of security risk as an indication of the importance of robust security management and risk mitigation mechanisms implemented by the bank. In other words, customer trust is shaped not by the existence of risk itself, but by the institution's capability to manage and control that risk effectively.

This finding reflects the evolving nature of customer perceptions in digital banking environments. As cybersecurity threats become increasingly common in modern financial systems, customers are generally aware that no digital platform can be entirely free from risk. Therefore, trust is more likely to emerge when customers believe that the bank possesses adequate technological capabilities, monitoring systems, and security protocols to protect their information and transactions. In the context of BYOND by BSI, customers appear to associate strong security measures with institutional competence and reliability, thereby strengthening their trust in the platform.

The result is consistent with the study conducted by Larasati and Darpito (2023), which found that perceived security positively influences customer trust in digital financial services. However, it contrasts with the findings of Putri et al. (2021), who reported a negative relationship between security risk and trust. These differing results indicate that the impact of security risk may depend on how customers interpret the bank's response to potential threats. When financial institutions successfully communicate their security capabilities and demonstrate effective risk management practices, perceived security risks may be transformed into indicators of organizational preparedness rather than sources of concern.

From a theoretical perspective, the findings support the Trust Theory proposed by Mayer, Davis, and Schoorman (1995). The dimension of *ability* is reflected in the bank's technical competence to secure customer data and digital transactions. The dimension of *integrity* is demonstrated through the bank's commitment to complying with regulatory requirements and maintaining confidentiality standards. Meanwhile, *benevolence* is manifested through efforts to safeguard customer interests and minimize potential harm arising from cybersecurity threats. Together, these dimensions contribute to strengthening customer trust in BYOND by BSI.

B. The Effect of Privacy on Muslim Customers' Trust in Using BYOND by BSI

The results further indicate that Privacy has a positive and significant effect on Muslim customers' trust in using BYOND by BSI, as reflected by a *p-value* of 0.015, a *t-statistic* of 2.169, and a path coefficient of 0.276. Therefore, H2 is supported. This finding suggests that customers who perceive stronger privacy protection tend to exhibit higher levels of trust toward the digital banking platform. The result reinforces the growing importance of privacy in digital financial ecosystems, where customers are increasingly concerned about how their personal information is collected, stored, and utilized.

The significance of privacy can be understood within the broader context of digital banking, where financial transactions require customers to disclose sensitive personal and financial information. Customers are more likely to trust institutions that provide clear privacy policies, obtain consent for data usage, and demonstrate transparency regarding information management practices. Effective privacy protection reduces uncertainty and perceived vulnerability, thereby fostering confidence in the institution and its digital services.

This finding is consistent with the study of Veronica and Rodhiah (2021), which concluded that privacy positively influences customer trust in electronic banking services. The result further

suggests that privacy protection is not merely a legal obligation but also a strategic factor in developing sustainable customer relationships. In highly competitive digital banking markets, customers increasingly evaluate service providers based on their ability to protect personal information and respect individual privacy rights.

The findings are also supported by the Trust Theory of Mayer, Davis, and Schoorman (1995). The dimension of *ability* is reflected in the bank's technical capability to secure customer information through reliable information systems and privacy protection mechanisms. The dimension of *integrity* is demonstrated through compliance with data protection regulations and transparent information management practices. Furthermore, *benevolence* is reflected in the bank's commitment to prioritizing customer welfare, comfort, and privacy protection as part of its broader responsibility toward stakeholders. Collectively, these dimensions contribute to the formation of trust among Muslim customers using BYOND by BSI.

C. The Simultaneous Effect of Data Security Risk and Privacy on Muslim Customers' Trust in Using BYOND by BSI

The findings demonstrate that Data Security Risk and Privacy jointly influence Muslim customers' trust in using BYOND by BSI. The coefficient of determination (R^2) value of 0.487 indicates that the two independent variables explain 48.7% of the variance in Customer Trust. Furthermore, the structural model results reveal that both variables exert positive and significant effects on trust. Accordingly, H3 is supported. These findings suggest that customer trust is not determined by a single factor but rather emerges from the combined influence of effective security management and privacy protection practices.

The moderate explanatory power of the model highlights the strategic importance of security and privacy in the digital banking sector. While customers recognize the existence of technological risks, their trust is strengthened when financial institutions demonstrate a strong commitment to protecting data and maintaining confidentiality. Consequently, trust is developed through the interaction between technological safeguards and responsible information management practices. This finding emphasizes that digital banking institutions must simultaneously invest in cybersecurity infrastructure and privacy governance frameworks to sustain customer confidence.

The results are consistent with previous studies indicating that security and privacy represent critical determinants of trust in digital financial services. The findings support the argument that trust in digital banking is shaped less by the absence of risk and more by the institution's ability to manage risk effectively, transparently, and responsibly. For Islamic banking institutions, this responsibility carries additional significance because trust is closely related to the principle of *amanah*, which requires institutions to protect assets and information entrusted to them by customers.

The findings can also be interpreted through the lens of Mayer, Davis, and Schoorman's (1995) Trust Theory. The dimension of *ability* is reflected in the bank's competence in implementing reliable security technologies, authentication mechanisms, encryption systems, and fraud detection procedures. *Integrity* is demonstrated through compliance with regulatory requirements, ethical standards, and commitments to safeguarding customer information. Meanwhile, *benevolence* is reflected in the institution's willingness to prioritize customer interests by ensuring privacy protection and minimizing potential security threats. The integration of these dimensions strengthens customer confidence and reinforces the credibility of BYOND by BSI as a digital Islamic banking platform.

From a practical perspective, the findings suggest that efforts to enhance customer trust should focus on strengthening both security and privacy protection mechanisms. Continuous investment in cybersecurity infrastructure, transparent communication regarding data protection policies, and consistent compliance with privacy regulations can contribute significantly to building sustainable trust. For Islamic banking institutions, these initiatives not only improve service quality but also reflect the implementation of *amanah* as a fundamental value underlying ethical and responsible financial services.

CONCLUSION

This study examined the impact of data security risk and privacy on Muslim customers' trust in using BYOND by BSI. The findings demonstrate that both variables have positive and significant effects on customer trust, indicating that trust in digital Islamic banking services is strongly influenced by customers' perceptions of security management and privacy protection. Among the two factors, data security risk exhibits a stronger influence on trust than privacy, suggesting that customers place greater emphasis on the bank's ability to protect transactions and safeguard sensitive information within digital banking environments.

The results further reveal that data security risk and privacy jointly explain 48.7% of the variance in customer trust, highlighting their substantial contribution to trust formation. These findings suggest that customers do not merely evaluate the existence of potential security threats but rather assess how effectively the institution manages, mitigates, and communicates those risks. Similarly, privacy protection strengthens customer confidence by ensuring that personal information is collected, processed, and utilized in a responsible and transparent manner. Consequently, trust emerges from the interaction between technological reliability and institutional accountability.

From a theoretical perspective, this study extends the application of Trust Theory by Mayer, Davis, and Schoorman (1995) within the context of Islamic digital banking. The findings confirm that the dimensions of *ability*, *integrity*, and *benevolence* remain relevant in explaining trust formation in technology-based financial services. Furthermore, the study highlights the relevance of the Islamic principle of *amanah*, whereby the protection of customer data and privacy constitutes not only a technical obligation but also an ethical responsibility that strengthens institutional credibility.

Practically, the findings suggest that Islamic banking institutions should continuously strengthen cybersecurity infrastructure, enhance privacy governance mechanisms, and communicate data protection policies transparently to customers. Investments in advanced authentication systems, data encryption technologies, fraud detection mechanisms, and privacy safeguards are essential for maintaining customer confidence and supporting the long-term adoption of digital banking services. By integrating technological excellence with ethical responsibility, Islamic banks can foster sustainable trust and strengthen their competitiveness in the evolving digital financial ecosystem.

Future research may expand the model by incorporating additional determinants of trust, such as perceived usefulness, service quality, digital literacy, religiosity, customer experience, and brand reputation. Moreover, comparative studies involving different Islamic banking institutions or digital financial platforms may provide broader insights into the factors shaping customer trust in the rapidly evolving landscape of Islamic digital finance.

REFERENCES

Alfian, I., Majid, M. S. A., & Sugianto. (2025). The Role of Sharia Fintech in Enhancing Financial Inclusion in the Digital Era. *Journal of Finance and Islamic Banking*, *8*(1), 79–94. https://doi.org/10.22515/JFIB.V8I1.11798

Asnawi, N., & Setyaningsih, N. D. (2021). Islamic Banking Service Innovation in Customer Co-Creation: Its Impact on Customer Trust, Satisfaction, and Loyalty. *Journal of Southwest Jiaotong University*, *56*(2), 65–82. https://doi.org/10.35741/ISSN.0258-2724.56.2.7

Astuti, A. R. T. (2024). Islamic Work Ethics, Employee Response, and Job Satisfaction: An Exploration of Indonesian Islamic Banking Employees. *Jurnal Minds: Manajemen Ide Dan Inspirasi*, *11*(1), 59–72. https://doi.org/10.24252/MINDS.V11I1.46069

Babina, T., Bahaj, S., Buchak, G., De Marco, F., Foulis, A., Gornall, W., Mazzola, F., & Yu, T. (2025). Customer Data Access and Fintech Entry: Early Evidence from Open Banking. *Journal of Financial Economics*, *169*(2), 103950. https://doi.org/10.1016/j.jfineco.2024.103950

Ghozali, M., Rofiah, K., Zahro', K., & Sahid, M. M. (2025). Reforming Qardh Practices in Islamic Banking: A Critical Analysis Based on Jasser Auda's Maqāṣid al-Sharīah Systems Approach in Indonesia. *Justicia Islamica*, *22*(2), 437–460. https://doi.org/10.21154/JUSTICIA.V22I2.11165

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to Use and How to Report the Results of PLS-SEM. In *European Business Review* (Vol. 31, Number 1). https://doi.org/10.1108/EBR-11-2018-0203

Harahap, D., Afandi, A., & Siregar, T. M. (2023). The Islamic Banking Customers' Intention to Use Digital Banking Services: An Indonesian Study. *Journal of Islamic Monetary Economics and Finance*, *9*(3), 533–558. https://doi.org/10.21098/JIMF.V9I3.1673

Haris, C., & Manangin, S. (2024). The Digital Revolution in Exploring the Impact of Fintech on Islamic Financial Services. *Kunuz: Journal of Islamic Banking and Finance*, *4*(2), 171–187. https://doi.org/10.30984/KUNUZ.V4I2.1267

Huang, A. H. (2022). Olah data SEM dengan LISREL, AMOS atau SMART PLS? *GLOBALSTATS ACADEMIC: Statistic Consultant for Academic Research*.

Iba, Z., & Wardhana, A. (2023). *Operasionalisasi Variabel dalam Penelitian Kuantitatif*. Eureka Media Aksara. https://www.researchgate.net/publication/382028555_OPERASIONALISASI_VARIABEL_DALAM_PENELITIAN_KUANTITATIF

Jafri, J. A., Amin, S. I. M., Rahman, A. A., & Nor, S. M. (2024). A Systematic Literature Review of the Role of Trust and Security on Fintech Adoption in Banking. *Heliyon*, *10*(1), e22980. https://doi.org/10.1016/j.heliyon.2023.e22980

Jan, A., Rahman, H. U., Zahid, M., Salameh, A. A., Khan, P. A., Al-Faryan, M. A. S., Che Aziz, R. B., & Ali, H. E. (2023). Islamic Corporate Sustainability Practices Index Aligned with SDGs Towards Better Financial Performance: Evidence from the Malaysian and Indonesian Islamic Banking Industry. *Journal of Cleaner Production*, *405*, 136860. https://doi.org/10.1016/J.JCLEPRO.2023.136860

Meero, A. (2025). Islamic vs. Conventional Banking in the Age of FinTech and AI: Evolving Business Models, Efficiency, and Stability (2020–2024). *International Journal of Financial Studies 2025, Vol. 13, 13*(3). https://doi.org/10.3390/ijfs13030148

Nasrun, M. K., Susilo, H., & Afrianty, T. W. (2025). Accelerating Digital Transformation Through Digital Leadership: Strategies for Innovation, Sustainability, and Organisational Performance Enhancement. *BISMA: Bisnis Dan Manajemen*, *17*, 264–291. https://doi.org/10.26740/BISMA.V17N2.P264-291

Noer, D., Rahmanto, A., Irsyad, S. M., Nurwiyanti, F., Haq, A., Sultan, K., Mu', A. H., & Sani, A. A. (2023). Islamic Banks: Study of Financial Literacy, Digital Marketing, Accessibility, Age, and Education. *Journal of Islamic Economics and Finance Studies*, *4*(1), 66–82. https://doi.org/10.47700/JIEFES.V4I1.5805

Nofriansyah, N., Vhalery, R., Wibowo, W., & Supardi, E. (2026). Islamic Digital Financial Literacy in Navigating Wealth Ethics and Sustainability in the 21st Century. *Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/979-8-3373-1842-4.Ch006*, 145–174. https://doi.org/10.4018/979-8-3373-1842-4.CH006

Ristya, C. V. O. (2024). *Kepuasan Nasabah terhadap Penggunaan Mobile Banking BPD DIY Syariah pada Pembayaran Melalui Qris UMKM Kampung Ramadhan Jogokariyan (KRJ) 2024*. UII. https://dspace.uii.ac.id/handle/123456789/52367

Santoso, W., Sitorus, P. M., Batunanggar, S., Krisanti, F. T., Anggadwita, G., & Alamsyah, A. (2021). Talent Mapping: A Strategic Approach Toward Digitalization Initiatives in the Banking and Financial Technology (Fintech) Industry in Indonesia. *Journal of Science and Technology Policy Management*, *12*(3), 399–420. https://doi.org/10.1108/JSTPM-04-2020-0075

Sugiyono, S. (2023). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. In *Alfabeta*. https://elibrary-dev.nusamandiri.ac.id/readbook/240077/metode-penelitian-kuantitatif-kualitatif-dan-r-d.html

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector. *Computers & Security*, *147*, 104051. https://doi.org/10.1016/j.cose.2024.104051

Wibowo, W., Nofriansyah, N., Nasrudin, N., & Aminuddin, A. (2026). *Integrating Islamic Financial Literacy, Social Entrepreneurship, and Social Finance: Innovative Pathways to Inclusive and Sustainable Development*. 115–144. https://doi.org/10.4018/979-8-3373-1842-4.CH005

Widyaputri, F. F., & Gunanto, E. Y. A. (2023). Shariah Mobile Banking Adoption Trends: Analysis Mob Mentality, Reputation, Perceived Risk, and Islamic Financial Literacy. *Jurnal Ekonomi Syariah Teori Dan Terapan*, *10*(5). https://doi.org/10.20473/vol10iss20235pp482-495

Yusuf, M. (2006). Metode Penelitian Kuantitatif, Kualitatif, dan Penelitian Gabungan. *Kencana*, *1999*(December), 1–6. https://books.google.co.id/books/about/Metode_Penelitian_Kuantitatif_Kualitatif.html?id=RnA-DwAAQBAJ&redir_esc=y