SOCIETA
Journal of Society and Change

Volume 1, Issue 1, January–June 2026

Building user trust in the digital society: The influence of perceived data security on the DANA digital wallet application

Jenny Karunia Putri Zai[1]*, Darwis Robinson Manalu[2]

[1] [2] Universitas Methodist Indonesia, Medan, Indonesia

*Corresponding Author: jennyzai562@gmail.com

Submission: 20 June 2026 Revision: 1 July 2026 Accepted: 11 July 2026

Abstract

The rapid adoption of digital wallets within society has intensified concerns regarding data security. However, previous studies examining the influence of perceived data security on user trust have primarily focused on statistical relationships without explaining the conceptual mechanism underlying trust formation. This study aims to examine the influence of perceived data security on user trust in the DANA digital wallet application. A quantitative approach employing simple linear regression was conducted using questionnaire data collected from 75 DANA users at Methodist University of Indonesia through a five-point Likert scale. The findings reveal that perceived data security has a positive and statistically significant effect on user trust ($R^2 = 0.738$; $t = 14.343$; $p < 0.001$), indicating that stronger perceptions of data security lead to higher levels of user trust in digital financial services. This study contributes by proposing a conceptual framework that explains the trust formation process while providing practical recommendations for digital wallet providers to strengthen security systems and enhance public trust in digital transactions.

Keywords: Perceived data security; User trust; Digital wallet; DANA; Simple linear regression.

Abstrak

Pesatnya penggunaan dompet digital di masyarakat meningkatkan kebutuhan akan keamanan data, namun penelitian mengenai pengaruh persepsi keamanan data terhadap kepercayaan pengguna masih terbatas pada hubungan statistik dan belum menjelaskan mekanisme konseptual pembentukan kepercayaan. Penelitian ini bertujuan menganalisis pengaruh persepsi keamanan data terhadap kepercayaan pengguna aplikasi DANA. Penelitian ini menggunakan pendekatan kuantitatif dengan analisis regresi linear sederhana terhadap 75 mahasiswa pengguna DANA di Universitas Methodist Indonesia melalui kuesioner berbasis skala Likert. Hasil penelitian menunjukkan bahwa persepsi keamanan data berpengaruh positif dan signifikan terhadap kepercayaan pengguna ($R^2 = 0{,}738$; $t = 14{,}343$; $p < 0{,}001$), yang mengindikasikan bahwa semakin tinggi persepsi keamanan, semakin tinggi pula tingkat kepercayaan pengguna dalam memanfaatkan layanan keuangan digital. Penelitian ini berkontribusi dengan menawarkan kerangka konseptual yang menjelaskan proses pembentukan kepercayaan pengguna serta memberikan rekomendasi bagi penyedia layanan untuk memperkuat keamanan sistem dan meningkatkan kepercayaan masyarakat terhadap transaksi digital.

Kata Kunci: Persepsi keamanan data; Kepercayaan pengguna; Dompet digital; DANA; Regresi linear sederhana.

Introduction

Digital transformation has fundamentally reshaped the financial transaction behavior of Indonesian society (Hasan, 2024). The Indonesian Internet Service Providers Association (APJII) reported that the number of internet users in Indonesia has reached 221.56 million, with an internet penetration rate of 79.5%, indicating that the majority of public activities are now integrated into the digital ecosystem (Susilo et al., 2025). In line with this trend, Bank Indonesia recorded 34.5 billion digital payment transactions throughout 2024, with this figure projected to continue increasing in the following year (Situmorang, 2023). This rapid growth has accelerated the adoption of digital wallet services such as DANA, which provide a fast, convenient, and easily accessible payment platform (Rambe & Bangsawan, 2023). However, alongside this widespread adoption, concerns regarding personal data protection and transaction security have emerged as critical issues for users of digital financial services.

The rapid expansion of digital transactions has not necessarily been accompanied by a corresponding increase in users' sense of security. As more personal information is stored within digital wallet applications, the risks of data breaches, identity theft, account hijacking, phishing attacks, and various forms of cybercrime continue to escalate (Ebadi Ansaroudi et al., 2025). This situation suggests that the security of digital financial services should not be evaluated solely based on the existence of technological safeguards but also on how users perceive the effectiveness of those security measures (Saeed, 2025). Perceived security plays a pivotal role because users' decisions to store balances, conduct financial transactions, and share personal information are strongly influenced by their confidence that the system can consistently protect confidential data and secure financial transactions (Morić et al., 2024). Therefore, perceived data security has become a strategic factor in sustaining the continued use of digital wallet services.

User trust constitutes the cornerstone of successful digital financial services because all transactions are conducted without direct physical interaction between users and service providers (Roh et al., 2024). Under these circumstances, users must trust that service providers possess the technical capability, integrity, and commitment required to safeguard their personal information and financial transactions. Trust is not established instantly through the mere presence of security features such as PIN authentication, one-time passwords (OTP), or data encryption; rather, it develops through users' experiences when they perceive that the system provides reliable and effective protection. The stronger users' perceptions of security, the lower the uncertainty they experience during transactions, thereby strengthening their confidence in the service (Park et al., 2019). Consequently, perceived data security functions not only as a technical attribute but also as a psychological mechanism that fosters user trust in the DANA digital wallet application.

Numerous studies have investigated the relationship between data security and user trust in digital payment services. A study by Almaiah et al. (2023) demonstrated that perceived security positively influences user trust by enhancing users' sense of security during digital transactions. Aldboush and Ferdous (2023) found that personal data protection and transparency in information management are essential for maintaining user trust; however, their discussion primarily focused on privacy issues without explaining the underlying process through which trust is established. Li et al. (2019) further reported that system quality and service reliability strengthen the relationship between security and trust, although their study emphasized technical aspects rather than users' security perceptions. Despite these contributions, there remains a need to explain how perceived data security shapes user trust through a more comprehensive conceptual mechanism within the context of the DANA digital wallet application.

Based on these issues, this study aims to examine the influence of perceived data security on user trust in the DANA digital wallet application using a simple linear regression approach. Beyond empirically testing the relationship between the two variables, this study proposes a conceptual framework to explain how security features shape users' perceptions of data security, influence their psychological responses, and ultimately foster trust in digital financial services. The findings are expected to contribute theoretically by enriching the literature on trust formation in digital financial services while offering practical recommendations for digital wallet providers to design security systems that are not only technically robust but also capable of enhancing users' perceived security and sustaining public trust over time.

Method

This study employed a quantitative approach with an explanatory research design to examine the influence of perceived data security on user trust in the DANA digital wallet application (Creswell, 2014). The study was conducted among students at Methodist University of Indonesia who had previously used the DANA application for digital financial transactions. A purposive sampling technique was employed, whereby respondents were selected based on two criteria: having experience using the DANA application and being willing to participate in the study by completing the questionnaire. A total of 75 respondents participated through an online survey administered via Google Forms. The collected data were analyzed using IBM SPSS Statistics to examine the relationship between Perceived Data Security (X) as the independent variable and User Trust (Y) as the dependent variable.

The research instrument was developed by adapting measurement indicators from previous studies. The Perceived Data Security variable was adopted from Pavlou (2003) and comprised four dimensions: *Data Confidentiality*, *Protection Against Unauthorized Access*, *System Reliability*, and *Transaction Data Protection*, which were operationalized into eight questionnaire items. Meanwhile, the User Trust variable was adopted from Mayer et al. (1995) and consisted of three dimensions: *Ability*, *Benevolence*, and *Integrity*, which were operationalized into six questionnaire items. All items were measured using a five-point Likert scale ranging from 1 (*Strongly Disagree*) to 5 (*Strongly Agree*). A summary of the operationalization of the research variables is presented in Table 1.

Table 1. Operationalization of research variables

Variable	Dimension	Number of Items
Perceived Data Security (X)	*Data Confidentiality*	2
	Protection Against Unauthorized Access	2
	System Reliability	2
	Transaction Data Protection	2
User Trust (Y)	*Ability*	2
	Benevolence	2
	Integrity	2

Source: Adapted from Pavlou (2003) and Mayer et al. (1995).

The data were analyzed using Simple Linear Regression to examine the influence of perceived data security on user trust in the DANA digital wallet application. Prior to the regression analysis, the research instrument was evaluated through validity and reliability tests, while the assumptions of the regression model were assessed using normality, heteroscedasticity, and linearity tests. Subsequently, the model's goodness-of-fit was evaluated using analysis of variance (ANOVA), and hypothesis testing was conducted using the t-test at a significance level of 5%. In addition, the coefficient of determination (R^2) was employed to measure the proportion of variance in user trust explained by perceived data security (Astivia & Zumbo, 2019). The regression model used in this study is expressed as:

$$Y = a + bX + e$$

where Y represents User Trust, X denotes Perceived Data Security, a is the regression constant (intercept), b is the regression coefficient, and e represents the error term.

Results and Discussion

Instrument testing and regression assumption testing

Before conducting the simple linear regression analysis, the quality of the research instrument and the assumptions underlying the regression model were first evaluated. This stage aimed to ensure that the research instrument satisfied the requirements of validity and reliability and that the collected data fulfilled the statistical assumptions necessary to produce reliable regression results (Flatt & Jacobs, 2019). The analyses consisted of validity testing, reliability testing, normality testing, heteroscedasticity testing, and linearity testing. All statistical analyses were performed using IBM SPSS Statistics based on data collected from 75 students who were users of the DANA digital wallet application.

The validity of the research instrument was examined using the Pearson Product-Moment correlation technique to determine the ability of each questionnaire item to measure its intended construct. The analysis was conducted for all items representing the Perceived Data Security (X) and User Trust (Y) variables. With a sample size of 75 respondents and a significance level of 5% ($\alpha = 0.05$), the critical r value was 0.227, calculated based on the degrees of freedom ($df = n - 2 = 73$). A questionnaire item was considered valid if its calculated r value exceeded the critical r value (0.227).

The validity test results revealed that all indicators measuring the Perceived Data Security variable produced calculated r values greater than the critical r value, indicating that all questionnaire items were valid. The correlation coefficients ranged from 0.625 to 0.812, demonstrating that each item adequately measured the construct of perceived data security.

Table 2. Validity test results for the perceived data security variable (X)

Item	**Statement**	**Calculated *r***	**Critical *r***	**Interpretation**
X1	I believe that my personal data are kept confidential by the DANA application.	0.804	0.227	Valid
X2	I believe that my personal information in DANA is not shared with unauthorized parties.	0.770	0.227	Valid
X3	I believe that my DANA account is protected from unauthorized access.	0.625	0.227	Valid
X4	I believe that security features such as PIN and OTP adequately protect my DANA account.	0.632	0.227	Valid
X5	I believe that DANA's security system is reliable when conducting transactions.	0.794	0.227	Valid
X6	I believe that the DANA system operates reliably and rarely experiences disruptions during transactions.	0.698	0.227	Valid
X7	I believe that my transaction data in DANA are protected from misuse.	0.812	0.227	Valid
X8	I feel secure storing my balance in the DANA application.	0.775	0.227	Valid

Source: Processed by the authors using IBM SPSS Statistics.

The validity test was subsequently performed for the User Trust variable. The results showed that all questionnaire items also produced calculated *r* values greater than the critical *r* value (0.227), ranging from 0.794 to 0.840. These findings indicate that all indicators measuring user trust satisfied the validity criteria and were therefore appropriate for use in this study.

Table 3. Validity test results for the user trust variable (Y)

Item	Statement	Calculated *r*	Critical *r*	Interpretation
Y1	I trust that DANA can protect my personal data and account balance from cyber threats.	0.794	0.227	Valid
Y2	I believe that DANA employs adequate security technologies to protect its users.	0.840	0.227	Valid
Y3	I believe that DANA is genuinely committed to protecting users' personal data.	0.801	0.227	Valid
Y4	I believe that DANA uses my personal data solely for legitimate service purposes.	0.815	0.227	Valid
Y5	I believe that DANA is transparent in managing users' personal information.	0.819	0.227	Valid
Y6	I feel comfortable using DANA because I consider it a trustworthy platform.	0.831	0.227	Valid

Source: Processed by the authors using IBM SPSS Statistics.

Based on the validity test results for both research variables, all questionnaire items produced calculated *r* values greater than the critical *r* value, indicating that every item was valid. Therefore, the research instrument satisfied the validity requirements and was suitable for the subsequent stages of reliability testing and simple linear regression analysis.

The reliability of the research instrument was subsequently evaluated using Cronbach's Alpha to assess its internal consistency. An instrument was considered reliable if its Cronbach's Alpha coefficient exceeded 0.60. The analysis yielded Cronbach's Alpha values of 0.879 for the Perceived Data Security variable and 0.898 for the User Trust variable. Both coefficients indicate excellent reliability, demonstrating that all questionnaire items consistently measured their respective constructs.

Table 4. Reliability test results

Variable	Number of items	Cronbach's Alpha	Interpretation
Perceived Data Security (X)	8	0.879	Highly reliable
User Trust (Y)	6	0.898	Highly reliable

Source: Processed by the authors using IBM SPSS Statistics.

After confirming that the research instrument was both valid and reliable, a normality test was conducted to determine whether the regression residuals followed a normal distribution. The analysis employed the Shapiro–Wilk test and was supported by the Normal P–P Plot. The results showed a significance (*p*) value of 0.216, which exceeded the threshold of 0.05. In addition, the data points in the Normal P–P Plot closely followed the diagonal reference line without substantial deviation. These findings indicate that the regression residuals were normally distributed, thereby satisfying one of the fundamental assumptions of linear regression.

Table 5. Normality test results

Variable	**Statistic**	**Sig.**	**Interpretation**
Residual	0.982	0.216	Normally distributed

Source: Processed by the authors using IBM SPSS Statistics.

The next assumption examined was heteroscedasticity using the Glejser test. This analysis aimed to determine whether the residual variance remained constant across observations. The results produced a significance (*p*) value of 0.229, which was greater than 0.05. Therefore, the regression model showed no evidence of heteroscedasticity, indicating that the residual variance was homogeneous and that the model satisfied the classical assumptions of regression.

Table 6. Heteroscedasticity test results (Glejser)

Variable	***t* value**	**Sig.**	**Interpretation**
Perceived Data Security	1.214	0.229	No heteroscedasticity detected

Source: Processed by the authors using IBM SPSS Statistics.

The final assumption evaluated was linearity to determine whether the relationship between Perceived Data Security and User Trust was linear. The results revealed a significance value of 0.000 for the *Linearity* component ($p < 0.05$), whereas the significance value for *Deviation from Linearity* was 0.471 ($p > 0.05$). These findings confirm that the relationship between the two variables is linear, thereby satisfying the assumptions required for subsequent simple linear regression analysis.

Table 7. Linearity test results

Source	**Sum of Squares**	***df***	***F* value**	**Sig.**
Between Groups (Combined)	1389.168	19	11.786	0.000
Linearity	1277.133	1	205.881	0.000
Deviation from Linearity	112.035	18	1.003	0.471
Within Groups	341.179	55	–	–
Total	1730.347	74	–	–

Source: Processed by the authors using IBM SPSS Statistics.

Overall, the results of the instrument testing and regression assumption testing demonstrate that all measurement indicators satisfied the requirements of validity and reliability. Furthermore, the regression model fulfilled the assumptions of normality, homoscedasticity, and linearity. Since all statistical assumptions were satisfied, the dataset was considered appropriate for conducting simple linear regression analysis to examine the influence of perceived data security on user trust in the DANA digital wallet application.

Simple linear regression analysis

After confirming that the research instrument was valid and reliable and that the regression model satisfied the assumptions of normality, heteroscedasticity, and linearity, the next stage involved conducting a simple linear regression analysis. This analysis aimed to examine the magnitude of the influence of Perceived Data Security (X) on User Trust (Y) in the DANA digital wallet application. In addition, the analysis assessed the strength of the relationship between the two variables, evaluated the goodness-of-fit of the regression model, and tested the proposed research hypothesis.

The analysis began with the Model Summary to determine the strength of the relationship between the independent and dependent variables. The results showed an R value of 0.859, indicating a very strong relationship between perceived data security and user trust. Furthermore, the R Square value of 0.738 indicates that 73.8% of the variation in user trust can be explained by perceived data security, while the remaining 26.2% is attributable to other factors beyond the scope of the present model, such as service quality, ease of use, user experience, and the reputation of the service provider.

Table 8. Model summary

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0.859	0.738	0.734	2.492

Source: Processed by the authors using IBM SPSS Statistics.

To evaluate whether the regression model was appropriate for hypothesis testing, an analysis of variance (ANOVA) was performed. The results yielded an F value of 205.711 with a significance (p) value of 0.000, which is lower than the significance threshold of 0.05. These findings indicate that the regression model is statistically significant and appropriate for explaining the influence of perceived data security on user trust in the DANA digital wallet application.

Table 9. Analysis of variance (ANOVA) results

Model	**Sum of Squares**	***df***	**Mean Square**	***F* value**	**Sig.**
Regression	1277.133	1	1277.133	205.711	0.000

Residual	453.214	73	6.209	–	–
Total	1730.347	74	–	–	–

Source: Processed by the authors using IBM SPSS Statistics.

A simple linear regression analysis was subsequently conducted to obtain the regression equation describing the relationship between the two research variables. Based on the analysis, the regression equation is expressed as follows:

$$Y = 2.616 + 0.673X$$

The equation indicates that the constant value of 2.616 represents the baseline level of user trust when perceived data security is assumed to remain constant. Meanwhile, the regression coefficient of 0.673 indicates that every one-unit increase in perceived data security is associated with a 0.673-unit increase in user trust. The positive regression coefficient demonstrates that the relationship between the two variables is positive and directly proportional.

Table 10. Simple linear regression results

Model	**B**	**Std. Error**	**Beta**	***t* value**	**Sig.**
Constant	2.616	1.353	–	1.934	0.057
Perceived Data Security	0.673	0.047	0.859	14.343	0.000

Source: Processed by the authors using IBM SPSS Statistics.

Hypothesis testing was performed using the *t*-test to determine the significance of the influence of the independent variable on the dependent variable. With a sample size of 75 respondents, the critical *t* value was 1.666 at the 5% significance level. The results revealed that the calculated *t* value of 14.343 exceeded the critical *t* value, with a significance (p) value of 0.000 ($p < 0.05$). These findings indicate that H_0 is rejected and H_1 is accepted, confirming that perceived data security has a positive and statistically significant influence on user trust in the DANA digital wallet application.

Table 11. Hypothesis testing results (t-test)

Hypothesis	**Calculated *t***	**Critical *t***	**Sig.**	**Decision**
H_0	14.343	1.666	0.000	Rejected
H_1	14.343	1.666	0.000	Accepted

Source: Processed by the authors using IBM SPSS Statistics.

Overall, the regression analysis demonstrates that perceived data security has a very strong and positive influence on user trust in the DANA digital wallet application. The substantial coefficient of determination indicates that data security is a dominant factor in shaping users' trust in digital wallet services. These findings suggest that strengthening security systems, enhancing personal data protection, and improving transparency in information management should remain strategic priorities for digital wallet providers to foster and sustain user trust in the DANA platform.

The influence of perceived data security on user trust in the DANA digital wallet application

The increasing adoption of digital wallets has not always been accompanied by a corresponding increase in user trust. Numerous incidents involving data breaches, account misuse, phishing attacks, and social engineering have demonstrated that even sophisticated security systems cannot necessarily foster trust if users do not perceive those security measures as effective (Salahdine & Kaabouch, 2019). This phenomenon raises a fundamental question regarding how perceived data security evolves into user trust within the context of the DANA digital wallet application. The findings of this study confirm that perceived data security has a positive and statistically significant influence on user trust. Nevertheless, this relationship cannot be adequately understood solely through statistical evidence; instead, it requires a conceptual explanation that illustrates the process through which user trust is developed. Therefore, this study proposes the conceptual framework presented in Figure 1 to explain this underlying mechanism.

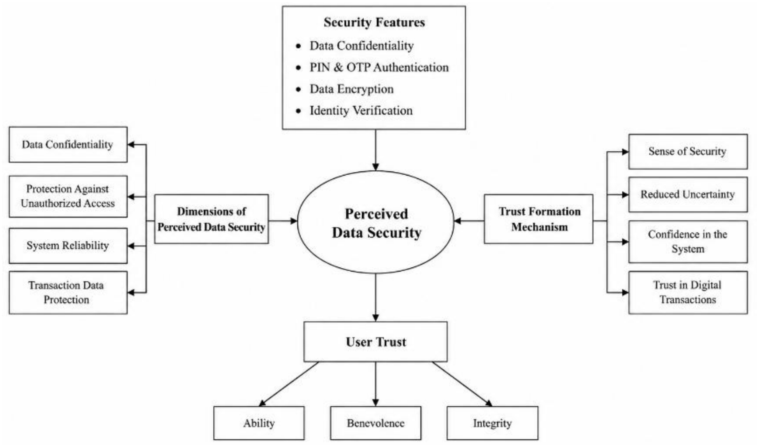

Figure 1. Conceptual framework explaining the influence of perceived data security on user trust in the DANA digital wallet application.

Source: Developed by the authors based on Mayer et al. (1995), Pavlou (2003), and the findings of this study.

Figure 1 is not intended to introduce a new conceptual model or an additional statistical model. Rather, it serves as an interpretive framework that provides a more comprehensive explanation of the empirical findings. Although the regression analysis confirms that perceived data security significantly influences user trust, this relationship develops through a sequence of interconnected processes. The proposed framework illustrates that application security features first shape users' perceptions of data security, which subsequently generate psychological responses in the form of a heightened sense of security and reduced uncertainty. These psychological responses ultimately evolve into trust in the digital service. Consequently, Figure 1 functions as a conceptual bridge linking the statistical findings with the theoretical explanation of how user trust is established in digital wallet services.

The first stage of the framework begins with the presence of *security features*, including *data confidentiality*, *PIN and OTP authentication*, *data encryption*, and *identity verification*. These components represent technical safeguards designed to protect user accounts, personal information, and transaction activities. However, the existence of security features alone does not automatically generate trust. Instead, these features first shape users' perceptions regarding the overall security of the application. This finding is consistent with the study by Krishna et al. (2025), which explained that the implementation of digital security mechanisms constitutes the initial foundation for developing users' security perceptions in electronic payment systems. Similarly, Reuter et al. (2022) found that transparency in security features enhances users' confidence in a system's ability to protect personal information. The findings of the present study further reinforce those of Zhang et al. (2019) by demonstrating that the effectiveness of security features depends more on how they are perceived by users than on their mere technical existence.

The second stage of the framework illustrates that *perceived data security* is constructed through four primary dimensions: *data confidentiality*, *protection against unauthorized access*, *system reliability*, and *transaction data protection*. These dimensions indicate that perceived security is a multidimensional construct encompassing not only the protection of personal information but also the system's ability to maintain operational reliability and secure digital transactions. When users perceive that their personal data are protected, unauthorized access is effectively prevented, the system operates reliably, and transactions are conducted securely, their perception of application security increases. These findings are consistent with the study by Atlam and Wills (2020), which argued that perceived security is established through the integration of data protection and system reliability. Likewise, Shin and Cheng (2023) demonstrated that transaction security plays a critical role in strengthening users' confidence in digital financial services. In contrast to the findings of Al-Okaily et al. (2023), which emphasized privacy as the primary determinant, the present study indicates that all four dimensions simultaneously contribute to shaping users' perceptions of security within the DANA digital wallet application.

Figure 1 further demonstrates that perceived data security does not directly produce user trust; rather, this relationship is mediated through psychological mechanisms consisting of a *sense of security*, *reduced uncertainty*, *confidence in the system*, and *trust in digital transactions*. When users perceive that the system effectively protects both their personal information and financial transactions, their uncertainty during digital transactions decreases, leading to a stronger sense of security while using the application. This sense of security subsequently develops into confidence in the system's capability and ultimately results in trust toward the digital service as a whole. These findings are consistent with the study by Al-Adwan et al. (2022), which identified uncertainty reduction as a fundamental mechanism underlying trust formation in digital environments. Similarly, Alraja et al. (2019) reported that a sense of security strengthens the relationship between system security and user trust. Extending the findings of Alifa et al. (2025), the present study demonstrates that, within the context of the DANA application, trust formation is influenced not only by technical security measures but also by users' subjective interpretations of the security they experience while using the application.

The final stage of the framework culminates in the development of *user trust*, represented by three core dimensions: *ability*, *benevolence*, and *integrity*. *Ability* reflects users' confidence in DANA's technical capability to protect personal information and financial transactions. *Benevolence* represents users' perception that the service provider genuinely intends to safeguard their interests, whereas *integrity* reflects the provider's consistency in implementing security principles, transparency, and personal data protection. Together, these dimensions demonstrate that user trust is established not only through technological sophistication but also through users' confidence in the provider's long-term commitment to maintaining trustworthy relationships. These findings are consistent with Ting et al. (2021), who identified *ability*, *benevolence*, and *integrity* as the fundamental pillars of trust formation in digital environments. Likewise, Hassan et al. (2020) emphasized that service provider integrity is essential for sustaining user trust in electronic transactions. In contrast to Owens and Khazanchi (2018), who regarded technical capability as the dominant determinant of trust, the present study demonstrates that these three dimensions operate complementarily in shaping user trust in the DANA digital wallet application.

Overall, this study demonstrates that the influence of perceived data security on user trust is a gradual process that begins with the implementation of security features, progresses through the development of users' security perceptions, generates psychological responses in the form of a stronger sense of security and reduced uncertainty, and ultimately culminates in trust toward the DANA digital wallet application. The conceptual framework presented in Figure 1 contributes to the literature by explaining that user trust is not merely a consequence of implementing advanced security technologies but also a result of how users interpret the security they experience while interacting with digital financial services. Accordingly, this study not only confirms the positive influence of perceived data security on user trust but also offers an interpretive framework that may serve as a theoretical foundation for future studies investigating trust formation across various digital financial services.

Conclusion

This study demonstrates that perceived data security has a positive and statistically significant influence on user trust in the DANA digital wallet application. The findings indicate that user trust is shaped not merely by the presence of advanced security technologies but, more importantly, by users' perceptions of the effectiveness of data protection and transaction security. Perceived data security develops through users' confidence that their personal information remains confidential, the system is protected against unauthorized access, the platform operates reliably, and digital transactions are adequately secured. These perceptions foster a stronger sense of security, reduce uncertainty during digital transactions, and enhance users' confidence in the service provider's technical capability, integrity, and commitment to safeguarding personal information. Consequently, strengthening user trust depends not only on implementing sophisticated security features but also on the provider's ability to cultivate positive security perceptions through transparent, reliable, and user-centered security practices.

This study contributes theoretically by advancing the understanding of the relationship between perceived data security and user trust through a conceptual framework that explains the trust formation process in digital wallet services. From a practical perspective, the findings provide valuable insights for DANA and other digital wallet providers to strengthen security systems, enhance personal data protection, and improve user education regarding secure digital transactions. Nevertheless, this study is limited by the inclusion of only one independent variable and a sample restricted to university students in North Sumatra, limiting the generalizability of the findings to the broader population of DANA users in Indonesia. Future research is therefore encouraged to include more diverse respondent groups and incorporate additional variables, such as perceived risk, service quality, perceived ease of use, user satisfaction, and user loyalty, in order to develop a more comprehensive model of trust formation in digital financial services.

References

Al-Adwan, A. S., Alrousan, M. K., Yaseen, H., Alkufahy, A. M., & Alsoud, M. (2022). Boosting online purchase intention in high-uncertainty-avoidance societies: A signaling theory approach. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(3), 136. https://doi.org/10.3390/joitmc8030136

Al-Okaily, M., Alqudah, H., Al-Qudah, A. A., Al-Qadi, N. S., Elrehail, H., & Al-Okaily, A. (2023). Does financial awareness increase the acceptance rate for financial inclusion? An empirical examination in the era of digital transformation. *Kybernetes, 52*(11), 4876–4896. https://doi.org/10.1108/K-08-2021-0710

Aldboush, H. H. H., & Ferdous, M. (2023). Building trust in fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. *International Journal of Financial Studies, 11*(3), 90. https://doi.org/10.3390/ijfs11030090

Alifa, N. L., Diana, D., Abdul, F., & Shah, S. M. A. R. (2025). The influence of convenience and security on brand loyalty among DANA Syariah users: The mediating role of brand trust. *Journal of Islamic Economics and Business Ethics, 2*(3), 325–347. https://doi.org/10.24235/jiesbi.v2i3.462

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

Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: The mediation role of risk perception. *IEEE Access, 7*, 111341–111354. https://doi.org/10.1109/ACCESS.2019.2904006

Astivia, O. L. O., & Zumbo, B. D. (2019). Heteroskedasticity in multiple regression analysis: What it is, how to detect it and how to solve it with applications in R and SPSS. *Practical Assessment, Research & Evaluation, 24*(1), n1.

Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. In *Digital twin technologies and smart cities* (pp. 123–149). https://doi.org/10.1007/978-3-030-18732-3_8

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage.

Ebadi Ansaroudi, Z., Sharif, A., Sciarretta, G., Marino, F. A., & Ranise, S. (2025). Secure and reliable digital wallets: A threat model for secure storage in eIDAS 2.0. *Data and Applications Security and Privacy XXXIX*, 271–289. https://doi.org/10.1007/978-3-031-96590-6_15

Flatt, C., & Jacobs, R. L. (2019). Principle assumptions of regression analysis: Testing, techniques, and statistical reporting of imperfect data sets. *Advances in Developing Human Resources, 21*(4), 484–502. https://doi.org/10.1177/1523422319869915

Hasan, Z. (2024). Impact of digital financial literacy on consumer protection, investor security, and financial transactions in Indonesia. *International Journal of Islamic Economics and Finance Research, 7*(2), 55–77. https://doi.org/10.53840/ijiefer165

Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An efficient secure electronic payment system for e-commerce. *Computers, 9*(3), 66. https://doi.org/10.3390/computers9030066

Krishna, B., Krishnan, S., & Sebastian, M. P. (2025). Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: A critical realist perspective. *Information Technology & People, 38*(2), 714–756. https://doi.org/10.1108/ITP-05-2023-0434

Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., & Chen, D. (2019). Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach. *IEEE Access, 7*, 9368–9383. https://doi.org/10.1109/ACCESS.2018.2890432

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review, 20*(3), 709. https://doi.org/10.2307/258792

Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of personal data in the context of e-commerce. *Journal of Cybersecurity and Privacy, 4*(3), 731–761. https://doi.org/10.3390/jcp4030034

Owens, D., & Khazanchi, D. (2018). Exploring the impact of technology capabilities on trust in virtual teams. *American Journal of Business, 33*(4), 157–178. https://doi.org/10.1108/AJB-04-2017-0008

Park, J., Amendah, E., Lee, Y., & Hyun, H. (2019). M-payment service: Interplay of perceived risk, benefit, and trust in service adoption. *Human Factors and Ergonomics in Manufacturing & Service Industries, 29*(1), 31–43. https://doi.org/10.1002/hfm.20750

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Rambe, H., & Bangsawan, S. (2023). The influence of use benefits, convenience, discounts, security and risk on the intention to use Indonesian digital wallets (DANA) in Bandar Lampung. *International Journal of Regional Innovation, 3*(2). https://doi.org/10.52000/ijori.v3i2.78

Reuter, C., Iacono, L. L., & Benlian, A. (2022). A quarter century of usable security and privacy research: Transparency, tailorability, and the road ahead. *Behaviour & Information Technology, 41*(10), 2035–2048. https://doi.org/10.1080/0144929X.2022.2080908

Roh, T., Yang, Y. S., Xiao, S., & Park, B. I. (2024). What makes consumers trust and adopt fintech? An empirical investigation in China. *Electronic Commerce Research, 24*(1), 3–35. https://doi.org/10.1007/s10660-021-09527-3

Saeed, S. (2025). Digital transformation in governmental public service provision and usable security perception in Saudi Arabia. *Information, 16*(3), 247. https://doi.org/10.3390/info16030247

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89. https://doi.org/10.3390/fi11040089

Shin, N., & Cheng, T. C. E. (2023). Gaining user confidence in banking industry's quest for digital transformation: A product-service system management perspective. *Industrial Management & Data Systems, 123*(8), 2216–2240. https://doi.org/10.1108/IMDS-06-2022-0358

Situmorang, S. H. (2023). Mobile payment: Trends in the digital shopping behaviour of the millennial generation. In *Digital transformation for business and society* (pp. 196–217). Routledge.

Susilo, M. E., Prayudi, P., & Florestiyanto, M. Y. (2025). Oversharing behavior in Gen Z on social media. *SHS Web of Conferences, 212*, 04022. https://doi.org/10.1051/shsconf/202521204022

Ting, H. L. J., Kang, X., Li, T., Wang, H., & Chu, C.-K. (2021). On the trust and trust modeling for the future fully-connected digital world: A comprehensive study. *IEEE Access, 9*, 106743–106783. https://doi.org/10.1109/ACCESS.2021.3100767

Zhang, J., Luximon, Y., & Song, Y. (2019). The role of consumers' perceived security, perceived control, interface design features, and conscientiousness in continuous use of mobile payment services. *Sustainability, 11*(23), 6843. https://doi.org/10.3390/su11236843