Digitomics
Journal Of Digital Economics And Innovations

e-ISSN. xxxx-xxxx
Vol. 01, No.1, June 2026
Pages 43-58

Check for updates

Digital Trust and Personal Data Protection in Indonesia's Digital Economy

M. Husin Rahayaan[1*], Gadafi Rahayaan[2]

[1]Department of Sharia Business Management, UIN A. M. Sangadji Ambon
Jl. Tarmidzi Taher, Batu Metah, 97224, Ambon, Indonesia
[2]Department of Islamic Economics, UIN A. M. Sangadji Ambon
Jl. Tarmidzi Taher, Batu Metah, 97224, Ambon, Indonesia

Email correponding author: *husinrahayaan@gmail.com

Article Info

Article history:
Received: April 12, 2026
Revised: May 19, 2026
Accepted: June 20, 2026

Keywords:
Digital trust
Cyber security privacy,
E-commerce,
Personal data,
Protection digital.

ABSTRACT

This article discusses digital trust and personal data protection as the foundation of Indonesia's digital economy sustainability. The research uses a structured literature study and secondary data analysis from APJII, BPS, Bank Indonesia, e-Conomy SEA, BSSN, Komdigi, as well as national regulations related to the Personal Data Protection Law. The results of the study show that the expansion of the internet, marketplaces, QRIS, and digital financial services increases economic opportunities, but also increases the risk of data leaks, phishing, ransomware, and misuse of data processing permissions. This article proposes a six-dimensional Digital Trust Index framework, namely data security, platform transparency, consumer protection, digital literacy, regulatory accountability, and service convenience. The novelty of the article lies in the integration of aspects of the digital economy, cyber risk, and personal data governance into an evaluation framework that is easily adaptable for empirical studies, public policy, and digital platform strategies.

: https://doi.org/10.30598/digitomicsv1i1pp43-58

1. INTRODUCTION

Indonesia's digital economy is growing very fast because of the convergence of three main forces: increasingly widespread internet connectivity, digital platforms that are increasingly attached to consumption activities, and digital payment systems that make transactions fast, cheap, and recorded. APJII reported that the number of Indonesian internet users in 2024 will reach around 221.56 million people with a penetration rate of 79.5 percent. At the same time, the e-Conomy SEA 2025 report projects Indonesia's digital economy to be close to a GMV value of US$100 billion by 2025. This figure shows that the digital economy is no longer on the fringes of the economic system, but has become a new infrastructure for household consumption, MSMEs, public services, and financial activities [1], [2].

However, the expansion of the digital economy cannot only be read in terms of transaction value. Behind the growth of marketplaces, digital wallets, QRIS, social media, and artificial intelligence-based services, there is a more fundamental issue, namely trust. Consumers are willing to fill in identities, save cards, scan QR codes, buy items without meeting the seller, or accept algorithmic recommendations because they believe that their data and money are managed securely. When that trust is compromised, for example due to data leaks, digital fraud, review manipulation, or service failures, then digital adoption can be held back even though the technology infrastructure is already in place [3]-[6].

Indonesia has entered a new phase of data governance after Law Number 27 of 2022 concerning Personal Data Protection was passed. This regulation regulates the principles, types of personal data, rights of data subjects, obligations of data controllers and processors, data transfers, administrative, institutional, international cooperation, and criminal provisions related to the use of personal data [5]. The Komdigi stated that the PDP Law officially takes full effect from October 17, 2024 after a two-year transition period [6]. Thus, the issue of personal data protection is no longer just a business ethics, but a legal obligation that must be fulfilled by platforms, financial institutions, public service providers, and digital business actors.

The cybersecurity context reinforces this urgency. In 2024, a ransomware attack on the Temporary National Data Center disrupts various public services. Reuters reported that more than 230 public agencies were affected, and most of the data on one of the affected data centers did not have adequate backups [7]. Previously, BSSN also recorded hundreds of millions of cyber traffic anomalies throughout 2023 and mapped threats such as malware, ransomware, web defacement, phishing, and AI-based threats [8]. This event shows that the growth of the digital economy without data resilience can generate systemic risks, not just individual risks.

Theoretically, Davis' research on *the Technology Acceptance Model* explains that the acceptance of technology is influenced by the perception of usability and ease of use [13]. Venkatesh et al. through UTAUT expanded the framework to include performance expectations, business expectations, social influences, and supporting conditions [14]. However, in digital transactions, these two factors are not enough. Pavlou points out that trust and risk perception are important variables in e-commerce acceptance [15]. Gefen et al. also found that trust strengthens the relationship between perception of usability and online shopping intent [16]. Kim, Ferrin, and Rao assert that online purchasing decisions are influenced by a balance between *trust*, *perceived risk*, and *perceived benefit* [19]. The five studies are the foundation that digital adoption is not only technical, but also psychological, social, and institutional.

The literature on organizational trust is also relevant to reading the digital economy. Mayer, Davis, and Schoorman explain that trust is built through the ability, virtue, and integrity of the trusted party [18]. In the context of digital platforms, capabilities are evident from system reliability, security, and speed of service. Virtue can be seen from the platform's concern for the interests of users, for example complaint resolution and protection when transactions are problematic. Integrity can be seen from the consistency of rules, cost transparency, and honesty in the use of data. Thus, digital trust cannot be built on security slogans alone; It should be present in the daily user experience.

A blind spot that often appears in discussions of the digital economy is to consider data protection as a mere compliance cost. In fact, data protection can be read as a productive investment. Platforms that are transparent, secure, and responsive to consumer complaints have a greater chance of retaining users, lowering customer acquisition costs, and strengthening reputation. Conversely, a single incident of data leak can lead to financial losses, decreased trust, system recovery costs, and legal pressure. Therefore, digital trust must be placed as an economic asset that can be built, measured, and protected. The research problem in this article is how to formulate the relationship between the digital economy, personal data protection, and consumer trust in the Indonesian context. This article aims to: (1) explain the position of digital trust in the growth of the digital economy; (2) developing an evaluation framework for the Digital Trust Index; (3) identify key risks affecting trusts; and (4) formulate governance recommendations for digital MSME platforms, regulators, and actors.

The novelty of this article lies in the preparation of an integrative framework that combines technology acceptance theory, *trust-risk-benefit* theory, PDP Law regulation, and cyber risk indicators into the Digital Trust Index model. This framework not only explains why consumers use digital services, but also why they can stop, hold back, or switch platforms when data protection is considered weak. Thus, this article makes a conceptual and practical contribution to Indonesian digital economy research that is more sustainability-oriented, not just transaction growth.

2. METHOD

This study uses a structured literature study design with a secondary data analysis approach. The main data sources come from official publications and trusted reports, namely APJII for internet penetration, BPS for e-commerce statistics, Bank Indonesia for digital payment systems, Google-Temasek-Bain for digital economy projections, BSSN for cybersecurity landscape, Komdigi and BPK for PDP Law regulations, as well as OECD, World Bank, NIST, ISO, and academic literature related to trust, privacy, and technology adoption [1]-[30].

The research procedure was carried out in four stages. The first stage is the identification of key literature with the keywords *digital trust*, *personal data protection*, *cybersecurity*, *e-commerce*, *digital payment*, *technology acceptance*, and *privacy risk*. The second stage is the extraction of concepts and indicators from the literature. The third stage is the preparation of the Digital Trust Index framework with six dimensions: data security, platform transparency, consumer protection, digital literacy, regulatory accountability, and service convenience. The fourth stage is the synthesis of results in the form of risk matrices, visualization of indicators, and policy recommendations.

Methodologically, this article does not claim to be a primary survey. The numbers used serve as macro context and an illustration of the evaluation framework. If this

framework is continued into empirical research, each dimension can be measured through consumer surveys, platform audits, complaint data, cyber incident data, and PDP Law compliance indicators. With this design, this article can be a bridge between conceptual studies and advanced quantitative studies.

The Digital Trust *Index* (DTI) is defined as a weighted composite score of several indicators that have been normalized. Notation indicates an individual, platform, region, or unit of analysis; indicates the dimensions of the indicator; is the weight of the indicator; and is the normalized indicator score.$ijw_j z_{ij}$

$$DTI_i = \sum_{j=1}^{k} w_j \, z_{ij}, \qquad \sum_{j=1}^{k} w_j = 1$$

Equation (1) shows that the value of digital trust is formed by a combination of indicators that have been normalized and weighted. Weights can be determined equally, through expert assessment, or through statistical methods such as *analytic hierarchy processes*, *principal component analysis*, or adoption outcome-based regression.

$$z_{ij} = \frac{x_{ij} - \min(x_j)}{\max(x_j) - \min(x_j)}$$

Equation (2) is used for indicators whose direction is positive. For risk indicators, the transformation can be reversed so that a higher value still means better, for example through $.z_{ij}^{*} = 1 - z_{ij}$

3. RESULTS AND DISCUSSION

3.1. Digital Growth Requires Trust Capital

Trust becomes an intangible capital that determines the depth of adoption. In the early stages, users try the service because of its utility and convenience. At the advanced stage, users consider data security, platform reputation, cost transparency, refund certainty, and protection in the event of a dispute. In this context, trust is not only a psychological variable, but also an economic mechanism that lowers transaction costs. The higher the trust, the less consumers need to over-verify each transaction.

The development of QRIS, e-commerce, and digital financial services increases the need for trust because transactions take place across actors: consumers, merchants, platforms, payment service providers, banks, regulators, and logistics providers. The failure of one actor can affect the perception of the entire ecosystem. Therefore, digital trust needs to be treated as a digital public good whose benefits go beyond the interests of one platform.

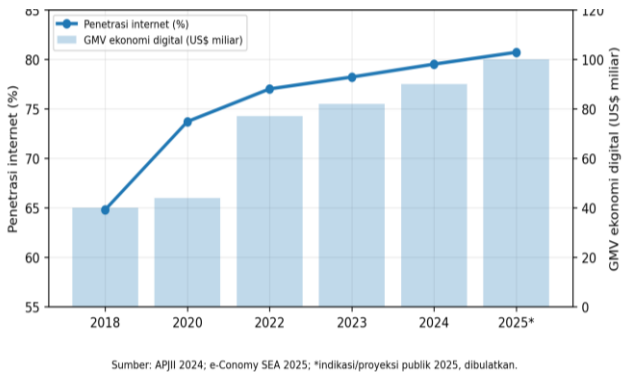

Figure 2. Connectivity and scale of Indonesia's digital economy.

3.2. Digital Trust as a Mediation Variable

Figure 1 presents a conceptual framework that places digital trust as a bridge between infrastructure and adoption. Digital infrastructure provides access, but not enough access to generate repeat transactions. Data protection and cybersecurity shape the perception of security. The perception of security then strengthens trust, and trust drives the adoption of the digital economy. If security is weak, a good infrastructure can still fail to result in deep adoption. In the theory of technology acceptance, *perceived usefulness* and *perceived ease of use* explain most of the intention to use technology [13]. However, in transactions involving money and personal data, users also assess the risks. Risks can be financial risks, privacy risks, performance risks, and time risks. Trust plays a role as a mechanism that reduces this uncertainty. Consumers who trust the platform tend to be more willing to store data, make payments, and buy back. The following probabilistic models can be used in empirical research to explain the opportunities for digital service adoption. Variables represent digital trust, represent digital literacy, and represent risk perception. Theoretically, the DTI and literacy coefficients are expected to be positive, while the risk perception coefficient is expected to be negative.$DTI_i L_i R_i$

$$P(A_i = 1) = \frac{1}{1 + \exp[-(\alpha + \beta_1 DTI_i + \beta_2 L_i + \beta_3 R_i)]}$$

Equation (3) can be used to test whether digital trust increases the chances of digital service adoption after controlling for literacy and risk. In survey research, it can be in the form of decisions to use marketplaces, QRIS, digital wallets, or digital public services.A_i

3.3. Digital Trust Index and Measurement Dimensions

The DTI was designed to help researchers, regulators, and platforms read trust as a measurable construct. The six proposed dimensions are data security, platform transparency, consumer protection, digital literacy, regulatory accountability, and service convenience. Data security includes encryption, access control, data backup, and incident management. Platform transparency includes clarity of permissions, fees, recommendation algorithms, and data usage. Consumer protection includes complaint mechanisms, refunds, and dispute resolution. Digital literacy includes the ability for users to recognize fraud, read privacy policies, and keep accounts secure. Regulator accountability includes regulatory certainty, supervision, sanctions, and coordination. The convenience of the service includes convenience, speed, and reliability. Figure 3 provides an illustration of the radar scorecard for the six dimensions. This score is not the result of a primary survey, but rather an example of how the model can be used. In real implementation, scores can be obtained from questionnaires, compliance audits, complaint logs, incident data, and expert assessments. The advantage of a composite approach is its ability to simplify complex issues without eliminating the structure of indicators.

Indicator normalization is necessary because each indicator has a different unit. For example, the number of complaints, dispute resolution time, literacy level, and compliance level cannot be directly summed up. The min-max normalization equation changes the indicator to a proportional scale, usually 0 to 1. For indicators that are risky, the direction of the scale needs to be reversed so that a higher score still indicates better conditions.

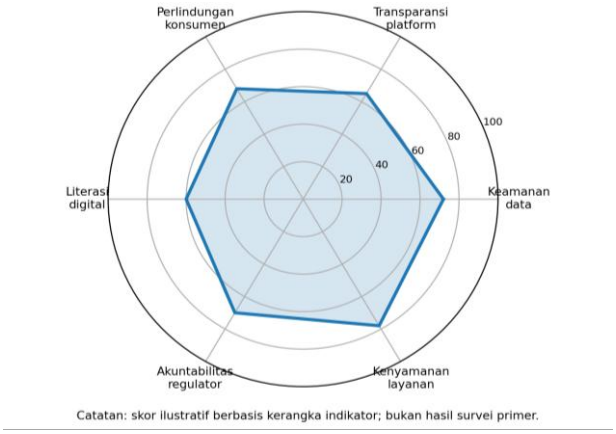

Figure 3. Illustration of the Digital Trust Index in six dimensions.

$$CAGR = \left(\frac{V_T}{V_0}\right)^{1/T} - 1$$

Equation (4) can be used to read the growth rate of the digital economy's value, transaction value, number of users, or number of incidents over a given period. Thus, the growth of the digital economy can be compared with the growth of data protection and digital literacy capacity.

Table 3. Digital Trust Index dimensions and indicators. Source: author's synthesis from [9]-[30].

DTI Dimensions	Example indicators	Direction of interpretation
Data security	Encryption, data backup, two-factor authentication, incident response time	The higher the safer
Platform transparency	Data permission clarity, fees, recommendation algorithms, privacy policy	The higher the clearer
Consumer protection	Complaints, refunds, dispute resolution, service ratings	The higher the protected
Digital literacy	Ability to recognize phishing, read permissions, safeguard accounts	The higher the the ready
Regulator accountability	Rules, audits, sanctions, incident reporting	The higher the stronger
Service convenience	Speed, availability, convenience, reliability	The higher the more comfortable it is

3.4. Cybersecurity and Personal Data Protection Risks

Figure 4 shows a risk matrix that maps probability, economic impact, trust impact, and mitigation readiness. Data leaks, phishing, ransomware, permission abuse, and algorithmic bias have different risk characters. Data leaks and ransomware tend to have a very high impact on trust as users feel they lose control of their identities and digital assets. Phishing has a high probability because it takes advantage of weaknesses in the user's literacy and habits. Algorithm bias has risks that are often less visible, but can affect the fairness of recommendations, credit access, pricing, and service.

The PDP Law clarifies that personal data is data about an individual who is identified or can be identified, either directly or indirectly [5]. The implication is that it is not enough for the platform to simply ask for user consent. The Platform must ensure the basis of data processing, restriction of purposes, processing security, access and correction rights, data deletion, incident notification, and the responsibilities of controllers and processors. In economic language, the PDP Law changed data protection from voluntary choice to a minimum market standard. The ransomware incident at the Provisional National Data Center shows that data governance cannot be separated from operational risk management. The issue of data backup, system segmentation, access auditing, and disaster recovery readiness is not just a technical matter, but part of the resilience of the digital economy. When public services are disrupted, the costs arise not only in the cost of system recovery, but also in the loss of public time, the decline in the reputation of institutions, and reduced trust in public digitalization.

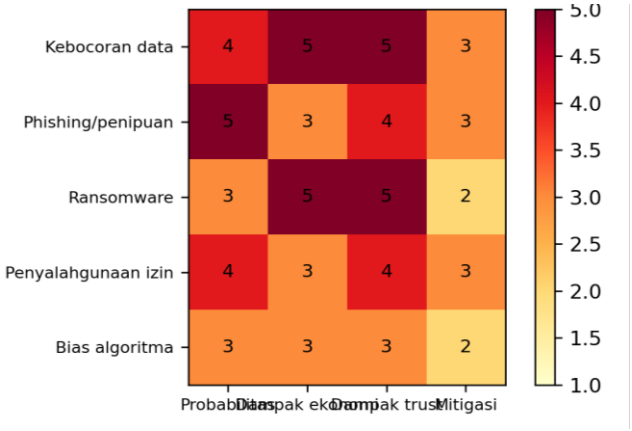

Figure 4. Digital trust risk matrix.

Table 4. Digital trust risks and their mitigation. Source: author's synthesis.

Risks	Main impact	Priority mitigation
Data leaks	Loss of identity control and declining platform reputation	Data minimization, encryption, access audits, incident notifications
Phishing/penipuan	Financial losses and fear of transactions	Education, anomaly detection, quick reporting channels
Ransomware	Service interruptions and high recovery costs	Backup, network segmentation, disaster recovery simulation
Permission abuse	Excessive data collection and loss of trust	Privacy dashboard, granular consent, destination restrictions
Bias algoritma	Unfairness of recommendations, pricing, or service access	Algorithm audit, model documentation, human review

3.5. Implications for Platforms, Regulators, and MSMEs

For digital platforms, the trust strategy must start from service design. The principles *of privacy by design* need to be translated into simple language: request data as necessary, explain the purpose of data use, provide privacy settings, secure logins,

display costs clearly, and provide easy-to-find helplines. Platforms also need to periodically measure trust through retention indicators, complaints, security incidents, service ratings, and consumer perception. For regulators, the main challenge is coordination. The digital economy involves the sectors of communication, trade, finance, taxation, consumer protection, cybersecurity, and business competition. Regulations that are too fragmented can confuse business actors, while regulations that are too loose can increase risks for consumers. Regulators need to provide operational guidelines for the implementation of the PDP Law, clear incident reporting mechanisms, and proportionate but firm sanctions. For MSMEs, digital trust is a way to move up. MSMEs that sell through marketplaces or social media need to maintain their reputation through honest product information, quick response, proof of transaction, on-time delivery, and customer data protection. MSMEs may not have sophisticated security systems, but they can start from basic practices: not sharing customer data, using strong passwords, enabling two-factor authentication, segregating business accounts, and understanding digital fraud modes.

Table 5. Recommendations for actions based on digital economy actors

Actors	Priority agenda	Success indicators
Platform digital	Privacy by design, account security, cost and data transparency	Reduced complaints, increased retention, compliance audits
Regulator	PDP Law Guidelines, cross-sectoral coordination, proportional sanctions	Incident reporting, compliance, dispute resolution
MSMEs	Basic security practices and transaction reputation	Positive reviews, quick response, customer data protected
Colleges	Trust research, digital literacy, security training	Modules, publications, surveys, community partnerships
Consumers	Privacy literacy and transaction security	Use of 2FA, phishing alerts, fraud reporting

3.6. Privacy Paradox and Digital Consumer Behavior

One of the important findings in the privacy literature is *the privacy paradox*, which is a condition when users express concern about privacy, but still share personal data for convenience, discounts, service access, or social pressure. In Indonesia's digital economy, this paradox appears when users accept terms of service without reading, allow applications to access contacts or locations without understanding the consequences, or use the same password for multiple accounts. This phenomenon does not necessarily indicate that users do not care about privacy. More precisely, users often do not have sufficient time, knowledge, or service options to make rational privacy decisions. The privacy paradox makes the responsibility of data protection should not be completely imposed on consumers. If consumers have to read lengthy privacy policy documents for every small transaction, then the cognitive costs are too high. Because of this, platforms and regulators need to build healthier choice architectures. Examples include a summary of data permissions in plain language, clear opt-in options, risk reminders when users share sensitive data, and dashboards that allow users to view,

download, repair, or delete data. In the context of marketplaces and digital wallets, the privacy paradox is also related to the promotion of personalization. Consumers love relevant product recommendations, but they don't necessarily feel comfortable knowing that they're built on search tracks, location, transactions, and social interactions. The critical point is not on personalization itself, but on transparency and user control. Transparent personalization can increase the value of a service, while hidden personalization can create a sense of being watched and lower trust.

Digital literacy is an important moderation variable. Users who understand digital risks better tend to be more selective in providing data, but still need platform design support. Therefore, digital literacy should not be understood only as the ability to use applications, but also as the ability to understand the consequences of data. At the higher education level, this literacy can be included in the curriculum of digital entrepreneurship, business statistics, information systems, and digital economy. At the community level, literacy can be done through MSME training, anti-phishing campaigns, and secure transaction guides.

3.7. Data Governance Architecture: From Compliance to Economic Value

Figure 5 presents the personal data governance cycle. The cycle starts with data collection and ends with data deletion, correction, or update. Each stage contains risks. At the collection stage, risks arise when the platform requests data that is not relevant to the purpose of the service. At the consent stage, risks arise when the user does not understand the consent language. At the processing stage, risks arise when data is used for new purposes without a clear basis. At the storage stage, risks arise from unauthorized access and weaknesses of data backups. At the sharing stage, risks arise from the transfer of data to third parties. At the deletion stage, a risk arises when the user is not actually able to retrieve his data.

Compliance with the PDP Law should not be seen as an administrative document, but as a management system. The platform needs to list data assets, define the basis for processing, classify sensitive data, set up retention, test security, and log incidents. This practice is very close to information security standards such as ISO/IEC 27001 and the NIST framework. The difference is that in the digital economy, data governance must be oriented towards the user experience. A good policy but not visible to users does not necessarily build trust. Therefore, transparency should translate into a clear interface. From an economic perspective, data governance produces three values. First, the defensive value, which is to reduce losses due to data leaks, fines, disputes, and service interruptions. Second, reputation value, which is increasing loyalty, positive reviews, and consumer trust. Third, the value of innovation, which is to allow data to be used responsibly to improve services, market segmentation, fraud detection, and decision-making. These three values explain why data protection is not the opponent of innovation, but rather a prerequisite for sustainable innovation. Governance architecture also needs to pay attention to the scale of business actors. Large companies can form data protection officers, security operation centers, and independent audits. MSMEs may not be able to do all of that, but they can still apply basic principles: data minimization, access restriction, two-factor authentication, periodic backups, and honest communication with customers. Regulators can help by providing step-by-step guidance on the size of the business.

Table 6. Control data governance based on the processing cycle.

Data cycle stage	Key risks	Suggested controls
Collection	Data redundancy and fuzzy destinations	Data minimization and concise notifications
Consent	Unconscious consent	Explicit opt-in and simple language
Processing	Off-purpose use	Goal restrictions and activity audits
Storage	Unauthorized access and data loss	Encryption, backups, access control
Transfer	Third parties are out of control	Processing and due diligence agreements
Deletion/correction	Data subject rights are ineffective	User rights portal and response SLA

3.8. Empirical Hypothesis Design for Advanced Research

Figure 6 proposes a hypothetical model that can be tested through surveys or micro-data platforms. This model places digital literacy and platform transparency as antecedents, risk perception and digital trust as mediating variables, and adoption intention as outcomes. This design is important because much of digital economy research stops at usage statistics, whereas decisions to use services are influenced by more complex psychological and institutional processes.

The first hypothesis is that digital literacy reduces risk perception. Users who understand authentication, phishing, privacy settings, and digital footprints tend to be better able to distinguish between real risks and controllable risks. However, these relationships are not always linear. Increased literacy can also make users more aware of risks, so that in the early stages risk perception can increase. Therefore, further research needs to distinguish between *risk awareness* and *risk anxiety*. The second hypothesis is that platform transparency increases digital trust. The transparency in question includes clarity of language, ease of finding information, explanation of fees, complaint mechanisms, and control over data permissions. Overly technical transparency can fail to build trust because it is not understood by users. Thus, the quality of communication becomes an important variable, not just the existence of a privacy policy. The third hypothesis is that risk perception decreases digital trust, while digital trust increases adoption intentions. This relationship can be tested using logistic regression, *structural equation modeling*, or *partial least squares*. If the data is panel, researchers can examine whether privacy policy changes, security incidents, or literacy campaigns change user behavior over time. This design opens up space for robust and policy-relevant statistical research.

Table 7. Design of a follow-up research hypothesis.

Code	Hipotesis	Signs of hope
H1	Digital literacy lowers the perception of uncontrolled risk	Negatives
H2	Platform transparency increases digital trust	Positive
H3	Risk perception lowers digital trust	Negatives
H4	Digital trust increases digital service adoption intention	Positive
H5	Risk perception lowers the intention to adopt directly	Negatives

3.9. Sectoral Implications: E-Commerce, Digital Payments, Public Services, and Education

In the e-commerce sector, trust is mainly related to product authenticity, payment security, review honesty, address data protection, and certainty of dispute resolution. Marketplaces need to keep the rating mechanism not manipulated, costs not hidden, and ads not misleading. Trust in this sector is particularly sensitive to negative experiences as consumers easily move to other platforms. Thus, the cost of losing trust can arise in the form of decreased retention and increased promotional costs to attract customers. In the digital payment sector, trust is related to balance security, speed of transaction completion, fraud protection, and clarity of responsibility when transactions are problematic. QRIS as a national standard has the advantage of simplifying transactions across providers. However, the wider the use of digital payments, the more important it is to educate against fake QRs, social engineering, and transfer errors. Technical security must be complemented by user behavioral literacy.

In digital public services, trust has a civic dimension. The public not only assesses whether the application is easy to use, but also whether the state is able to maintain identity, education, health, tax, and population administration data. Incidents in public services can undermine trust not only in certain applications, but in the government's digital transformation agenda. Therefore, government data governance requires disaster recovery standards, independent audits, and honest public communication when incidents occur. In the education sector, digital trust literacy needs to be a basic competency. Students of economics, statistics, management, and information technology need to understand the relationship between data, risk, ethics, and economic value. Learning can use data leak case studies, phishing simulations, privacy policy audits, and digital trust index analysis. Thus, universities not only produce technology users, but also critical thinkers who are able to design a safe and responsible digital economy.

Table 8. Sectoral implications of digital trust. Source: author's synthesis.

Sectors	Forms of sensitive data	Dominant risk	Agenda trust
E-commerce	Address, phone number, shopping history	Fraud, fake reviews, data misuse	Seller transparency and dispute protection
Digital payments	Balance, account, transaction history	Fraud, QR palsu, social engineering	Strong authentication and secure transaction education
Public services	Identity, health, education, taxes	Ransomware, data leaks, service disruptions	Backup, audit, incident communication
Education	Student data, grades, learning accounts	Phishing, illegal access, profiling	LMS privacy and governance literacy

3.10. Synthesis: Trust as a Soft Infrastructure of the Digital Economy

If the hard infrastructure of the digital economy is networks, data centers, devices, and payment systems, then digital trust is its soft infrastructure. This soft infrastructure is invisible, but determines whether the technology is used widely and sustainably. Without trust, consumers will hold back; MSMEs will be hesitant to be digitized; the government will face resistance; and the platform has to spend more on promotion as well as risk compensation. Figure 7 shows that incident response is not just a technical process. The stages of prepare, detect, contain, recover, and learn must be communicated to the public appropriately. Users don't always demand a system that never fails, as technical failures can occur. What they demand is accountability, speed of response, clarity of information, and real improvements. When the organization is able to demonstrate this, trust can be restored. If an organization covers up an incident, the trust can be damaged more deeply than the technical breakdown. The synthesis of this article yields three principles. First, personal data is an economic asset as well as an individual right. Second, data protection should be built from the design of the service, not added after the problem arises. Third, digital economy indicators need to be equipped with trust and risk indicators. With these three principles, the success of the digital economy is not only measured by GMV, number of users, or transaction volume, but also by the security, fairness, transparency, and resilience of the ecosystem.

Table 9. The principle of digital trust synthesis. Source: compiled by the author.

Principle	Meaning	Implementation examples
Data as a right and asset	Data has economic value, but is inherent in individual rights	Explicit permissions, access rights, data deletion
Protection from design	Security is not an additional feature	Privacy by design, security by default
Trust as a performance indicator	Digital success is not only transaction volume	Trust surveys, security audits, incident reporting

3.11. Relevance of Results to Relevant Research

The results of this study are consistent with Davis and Venkatesh et al. that usability and convenience are the starting doors for technology adoption [13], [14]. However, this article expands on that framework by placing trust and data protection as a condition for sustainable adoption. These findings are in line with Pavlou, Gefen et al., and Kim et al. who show that trust and risk influence online transaction decisions [15], [16], [19]. Thus, digital consumers are not only asking whether the service is useful, but also whether it is safe and responsible. This article also reinforces the literature of Acquisti et al. regarding *privacy calculus*, i.e. users often exchange personal data for the benefits of digital services [22]. However, such calculations are not always rational because users often do not understand the long-term consequences of data processing. Therefore, transparency and digital literacy are needed so that consumers can make more conscious decisions. In the policy context, this framework is in line with the OECD, NIST, and ISO which emphasize risk management, privacy protection, and information security as part of digital governance [9], [10], [25]-[27]. Compared to research that only discusses technology adoption, this article places trust as a variable that links the growth of the digital economy to systemic risk. Rather than legal studies that only highlight the PDP Law, this article shows that legal compliance needs to be translated into economic indicators and consumer behavior. Compared to cybersecurity studies that focus on technical threats, this article emphasizes that cybersecurity has economic consequences through reputation, loyalty, and sustainability of transactions. The close link between the results of this study and previous studies lies in the idea that digital behavior is the result of an interaction between benefits, risks, and trust. Transaction growth is not enough to state that the digital economy is healthy. If this growth is accompanied by increased fraud, data leaks, and low privacy literacy, then economic benefits can be eroded. Therefore, the results of this article drive a shift in success indicators from mere adoption to safe, conscious, and protected adoption.

4. CONCLUSION

Digital trust is the foundation of the sustainability of Indonesia's digital economy. The growth of internet users, marketplaces, QRIS, and digital financial services shows great economic opportunities, but these opportunities will be fragile if they are not supported by personal data protection, cybersecurity, platform transparency, and digital literacy. A healthy digital economy is not only an economy that is quick to transact, but an economy that makes users feel safe, have control over data, and gain protection when problems occur. This article proposes the Digital Trust Index as a six-dimensional evaluation framework: data security, platform transparency, consumer protection, digital literacy, regulatory accountability, and convenience of service. This framework can be used to assess platform readiness, compare regions, compile consumer surveys, and design data protection policies. The PDP Law, which has been in full force since October 2024, is a momentum to change data protection from a formal obligation to a strategy to build market trust. The next research is recommended to test the Digital Trust Index using primary surveys on marketplace users, QRIS, and digital wallets. Further studies need to compare the level of digital trust between regions and between generations in Indonesia. The next study also needs to integrate data on cyber incidents, consumer complaints, and PDP Law compliance to produce a predictive model of digital trust risk.

Acknowledgments
The author expressed his gratitude to all parties who assisted in the literature search process, secondary data management, and manuscript arrangement according to journal format.

Funding Information
Authors state no funding involved.

Author Contributions Statement
Syarifah Inayati: conceptualization, methodology, data curation, formal analysis, visualization, writing-original draft, writing-review and editing. All authors discussed the results and contributed to the final manuscript.

Conflict of Interest Statement
Authors state no conflict of interest.

Informed Consent
Not applicable because this study uses secondary data and published literature without collecting personal data from human participants.

Ethical Approval
Not applicable because this study does not involve experiments with humans or animals.

Ethical Approval
Not applicable because this study does not involve experiments with humans or animals.

Data Availability
The data supporting the findings of this study are available in the public reports and official publications listed in the References section. Derived data supporting figures and tables are available within the article.

Declaration of Generative AI and AI-assisted Technologies
Generative AI tools were used to improve drafting, language consistency, and formatting. The analysis framework, source selection, tables, figures, and conclusions must be reviewed and validated by the author before submission.

REFERENCES

[1] Indonesian Internet Service Providers Association, *Indonesian Internet Penetration Survey 2024*. Jakarta, Indonesia: APJII, 2024.
[2] Google, Temasek, and Bain & Company, *e-Conomy SEA 2025: From Digital Decade to AI Reality*. Singapore: Google, Temasek, Bain & Company, 2025.
[3] Central Statistics Agency, *E-Commerce Statistics 2024*. Jakarta, Indonesia: BPS, 2025. [Online]. Available: https://www.bps.go.id/
[4] Bank Indonesia, *Blueprint for Indonesia's Payment System 2030*. Jakarta, Indonesia: Bank Indonesia, 2025.
[5] Republic of Indonesia, *Law Number 27 of 2022 concerning Personal Data Protection*. Jakarta, Indonesia: State Secretariat, 2022.
[6] Ministry of Communication and Digital of the Republic of Indonesia, *New Era of Personal Data Protection*. Jakarta, Indonesia: Komdigi, 2024.
[7] Reuters, *Indonesia president orders audit of data centres after cyberattack*. London, U.K.: Reuters, Jun. 2024.
[8] State Cyber and Cryptography Agency, *Indonesian Cybersecurity Landscape 2023*. Jakarta, Indonesia: BSSN, 2024.
[9] OECD, *The OECD Privacy Framework*. Paris, France: OECD Publishing, 2013.
[10] OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. Paris, France: OECD Publishing, 2015.
[11] World Bank, *World Development Report 2016: Digital Dividends*. Washington, DC, USA: World Bank, 2016, doi: 10.1596/978-1-4648-0671-1.

[12] UNCTAD, *Digital Economy Report 2021: Cross-border Data Flows and Development*. Geneva, Switzerland: United Nations, 2021.
[13] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319-340, 1989, doi: 10.2307/249008.
[14] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, vol. 27, no. 3, pp. 425-478, 2003, doi: 10.2307/30036540.
[15] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," *Int. J. Electron. Commerce*, vol. 7, no. 3, pp. 101-134, 2003, doi: 10.1080/10864415.2003.11044275.
[16] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Quarterly*, vol. 27, no. 1, pp. 51-90, 2003, doi: 10.2307/30036519.
[17] D. H. McKnight, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: An integrative typology," *Information Systems Research*, vol. 13, no. 3, pp. 334-359, 2002, doi: 10.1287/isre.13.3.334.81.
[18] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review*, vol. 20, no. 3, pp. 709-734, 1995, doi: 10.5465/amr.1995.9508080335.
[19] D. J. Kim, D. L. Ferrin, and H. R. Rao, "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision Support Systems*, vol. 44, no. 2, pp. 544-564, 2008, doi: 10.1016/j.dss.2007.07.001.
[20] A. Beldad, M. de Jong, and M. Steehouder, "How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust," *Computers in Human Behavior*, vol. 26, no. 5, pp. 857-869, 2010, doi: 10.1016/j.chb.2010.03.013.
[21] N. Kshetri, "The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply," *Telecommunications Policy*, vol. 41, no. 1, pp. 49-67, 2017, doi: 10.1016/j.telpol.2016.11.002.
[22] A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of Economic Literature*, vol. 54, no. 2, pp. 442-492, 2016, doi: 10.1257/jel.54.2.442.
[23] K. Martin, "The penalty for privacy violations: How privacy violations impact trust online," *Journal of Business Research*, vol. 82, pp. 103-116, 2018, doi: 10.1016/j.jbusres.2017.08.034.
[24] European Union, *Regulation (EU) 2016/679: General Data Protection Regulation*. Brussels, Belgium: Official Journal of the European Union, 2016.
[25] National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0*. Gaithersburg, MD, USA: NIST, 2020.
[26] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD, USA: NIST, 2024, doi: 10.6028/NIST. CSWP.29.
[27] International Organization for Standardization, *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection*. Geneva, Switzerland: ISO, 2022.
[28] Bank Indonesia, *Quick Response Code Indonesian Standard (QRIS)*. Jakarta, Indonesia: Bank Indonesia, 2025. [Online]. Available: https://www.bi.go.id/
[29] Financial Services Authority, *National Survey of Financial Literacy and Inclusion 2024*. Jakarta, Indonesia: OJK, 2024.
[30] OECD, *Consumer Policy in the Digital Age*. Paris, France: OECD Publishing, 2020.