West Science Interdisciplinary Studies
Vol. 4, No. 01, January and 2026: pp. 168-180

The Influence of IoT Data Governance Quality and Data Privacy Policies on Information Security Risk Mitigation and Customer Trust in IoT-Based Startups in Bandung

Ajub Ajulian ZM[1], Enda Wista Sinuraya[2], Bambang Winardi[3], Yuanis[4]
[1] Departemen Teknik Elektro, Fakultas Teknik, Universitas Diponegoro and ayub.ayul1an@gmail.com
[2] Departemen Teknik Elektro, Fakultas Teknik, Universitas Diponegoro and sinuraya_enda@elektro.undip.ac.id
[3] Departemen Teknik Elektro, Fakultas Teknik, Universitas Diponegoro and bbwinar@gmail.com
[4] Sekolah Tinggi Ilmu Ekonomi Muhammadiyah Tuban and yuanis42@gmail.com

ABSTRACT

The rapid adoption of Internet of Things (IoT) technologies by startups has intensified concerns related to data governance, privacy protection, and information security risks. This study investigates the effect of IoT data governance quality and data privacy policy on information security risk mitigation and customer trust in IoT-based startups in Bandung, Indonesia. Using a quantitative research approach, data were collected from 150 users of IoT-based startup services through a structured questionnaire measured on a Likert scale. The data were analyzed using Structural Equation Modeling–Partial Least Squares (SEM-PLS 3). The results indicate that IoT data governance quality has a significant positive effect on information security risk mitigation. In addition, data privacy policy and information security risk mitigation both have significant positive effects on customer trust. Furthermore, information security risk mitigation partially mediates the relationship between IoT data governance quality and customer trust. These findings highlight the importance of strengthening data governance frameworks and implementing transparent privacy policies to reduce security risks and enhance customer trust. This study contributes to the growing body of literature on IoT governance and provides practical insights for startup managers and policymakers in fostering secure and trustworthy IoT-based business environments.

Keywords: *Internet of Things (IoT), Data Governance Quality, Data Privacy Policy, Information Security Risk Mitigation, Customer Trust*

1. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has significantly transformed the way startups design products, deliver services, and interact with customers. By enabling real-time data collection, processing, and connectivity among physical devices, IoT technologies offer substantial opportunities for efficiency, innovation, and competitive advantage [1], [2]. In Indonesia, particularly in Bandung as one of the country's leading technology and startup hubs, IoT-based startups have emerged across various sectors, including smart homes, transportation, healthcare, manufacturing, and digital services [3], [4]. However, alongside these opportunities, the extensive use of connected devices and data-driven business models has also increased exposure to information security risks and heightened public concern regarding data privacy [5], [6].

IoT-based startups rely heavily on the collection, storage, and analysis of large volumes of data, much of which may contain sensitive personal or behavioral information. Weak data governance practices—such as unclear data ownership, poor data quality control, and lack of accountability—can lead to data misuse, unauthorized access, and system vulnerabilities. At the same time, insufficient or poorly communicated data privacy policies may undermine users' perceptions of safety and fairness, ultimately eroding customer trust [7]. For startups, which often operate with limited resources and evolving organizational structures, managing data governance and privacy effectively remains a critical yet challenging task.

Information security risks in IoT environments are inherently complex due to the heterogeneous nature of devices, decentralized architectures, and continuous data flows. Security

breaches, data leaks, or system failures not only result in financial losses but can also cause reputational damage that threatens the sustainability of startups [8], [9]. Consequently, effective information security risk mitigation has become a strategic priority. Prior studies suggest that strong data governance quality—reflected in clear policies, standardized procedures, data accuracy, and accountability—plays a vital role in reducing security vulnerabilities. Similarly, transparent and well-enforced data privacy policies can enhance users' confidence that their personal data are handled responsibly [10], [11].

Customer trust is a particularly crucial factor for IoT-based startups, as users must be willing to allow continuous data collection and device connectivity. Trust influences customer adoption, continued usage, and long-term relationships. In digital and IoT contexts, trust is not built solely through product functionality, but also through perceptions of security, privacy protection, and ethical data practices [12], [13]. When customers perceive that a startup is capable of mitigating information security risks and safeguarding their personal data, they are more likely to develop trust in the company and its services.

Although prior studies have examined data governance, privacy, information security, and trust in broader digital and organizational contexts, empirical research that specifically focuses on Internet of Things (IoT)–based startups—particularly in emerging economies such as Indonesia—remains limited, and the interrelationships among IoT data governance quality, data privacy policy, information security risk mitigation, and customer trust have not yet been adequately explored within a single integrated research model; this gap is especially salient in startup ecosystems such as Bandung, where rapid innovation often outpaces the development of robust governance and security frameworks, therefore this study aims to investigate the effects of IoT data governance quality and data privacy policy on information security risk mitigation and customer trust in IoT-based startups in Bandung using a quantitative approach with survey data, with the expectation that the findings will provide empirical evidence on how governance and privacy practices contribute to security risk mitigation and trust formation, as well as practical insights for startup founders, managers, and policymakers in strengthening data governance and privacy strategies to support secure, trustworthy, and sustainable IoT-based business development.

2. LITERATURE REVIEW

2.1 Internet of Things (IoT) in Startup Contexts

The Internet of Things (IoT) refers to a network of interconnected physical devices embedded with sensors, software, and communication technologies that enable the collection and exchange of data over the internet, and in the startup context, IoT acts as a key driver of innovation by enabling the development of data-driven products, process automation, and personalized services within highly dynamic environments that require rapid scalability and continuous technological experimentation [14], [15]; however, this heavy reliance on constant data flows and device connectivity also introduces significant managerial and technological challenges, particularly related to data governance, security, and privacy management [16], [17], as IoT ecosystems differ from traditional information systems through their decentralized architectures, heterogeneous devices, and real-time data processing, which increase system complexity and expand the cyberattack surface, making it especially difficult for startups with limited financial and human resources to implement robust governance and security mechanisms, thereby highlighting the critical importance of understanding how governance quality and data privacy policies operate within IoT-based startups to ensure operational resilience and foster user acceptance [16].

2.2 *IoT Data Governance Quality*

Data governance refers to the set of policies, roles, standards, and processes that ensure data are managed effectively, securely, and ethically throughout their lifecycle, and in the context of IoT, data governance quality reflects the extent to which an organization clearly defines data ownership, maintains data accuracy, enforces access controls, and ensures accountability in data usage; however, the volume, velocity, and variety of data generated by interconnected devices make governance in IoT environments inherently more complex [18], [19], such that weak governance can lead to unclear responsibilities, inconsistent data standards, and insufficient oversight that heighten vulnerability to security breaches, whereas prior studies indicate that robust data governance frameworks support better risk management, higher data quality, and improved organizational performance [20], [21], leading to the expectation that for IoT-based startups, high-quality data governance plays a crucial role in mitigating information security risks through structured control over data access, processing, and storage.

2.3 *Data Privacy Policy*

A data privacy policy is a formal statement that outlines how an organization collects, uses, stores, and protects personal data, as well as the rights of data subjects, and within the digital economy it functions not only as a legal compliance instrument but also as a communication mechanism that signals an organization's commitment to responsible data practices; this role is especially critical for IoT-based startups [22], [23], as IoT devices continuously generate and process sensitive user data such as location information, behavioral patterns, and personal preferences, meaning that transparent and comprehensive privacy policies can reduce information asymmetry between firms and users, enhance users' perceived control over their data, and strengthen perceptions of fairness and trust, whereas vague or poorly implemented policies tend to heighten privacy concerns, hinder technology adoption [24], and erode customer confidence, thereby positioning data privacy policy quality as a key determinant of customer trust and perceived security in IoT-based services.

2.4 *Information Security Risk Mitigation*

Information security risk mitigation refers to the processes and controls implemented by organizations to identify, assess, and reduce risks associated with information assets, and in IoT systems these risks commonly stem from device vulnerabilities, insecure communication protocols [9], [25], weak authentication mechanisms, and human-related factors; effective mitigation therefore requires an integrated approach that combines technical measures such as encryption, access control, and system monitoring with managerial practices including clear policies, employee training, and incident response planning, as the literature consistently highlights that proactive security risk mitigation is vital for preventing data breaches and maintaining system integrity [26], [27], particularly because organizations with structured governance and security frameworks are better positioned to anticipate threats and respond to incidents, and for IoT-based startups specifically, information security risk mitigation is closely connected to data governance quality since governance mechanisms establish roles, responsibilities, and controls that enable secure

data handling, while successful risk mitigation not only safeguards organizational assets but also shapes external stakeholders' perceptions of reliability and professionalism [28], [29].

2.5 Customer Trust in IoT-Based Services

Customer trust can be defined as the belief that a service provider is competent, reliable, and acts in the best interests of its users, and in the context of IoT-based services this trust is especially critical because customers must permit devices to continuously collect and process personal data, often with limited transparency regarding data usage, making trust a key mechanism for reducing perceived risk and uncertainty and encouraging technology adoption and sustained engagement [13], [30]; prior research in electronic commerce and digital services consistently demonstrates that effective information security and strong privacy protection are fundamental antecedents of customer trust, as users who perceive that an organization successfully mitigates security risks and respects their privacy are more inclined to trust both the provider and its technology, which is particularly crucial for startups whose market penetration, survival, and reputation can be rapidly undermined by security breaches or privacy failures [31], [32].

2.6 Hypothesis Development

High-quality IoT data governance establishes clear structures, rules, and controls for managing data, thereby reducing ambiguity and vulnerabilities in IoT systems and enhancing an organization's ability to mitigate information security risks through improved data accuracy, access control, and accountability; in parallel, a clear and transparent data privacy policy serves as a signal of an organization's commitment to protecting user data, which increases customer trust when users understand how their data are handled and feel that their privacy is respected, while effective information security risk mitigation further strengthens this trust by lowering the likelihood of data breaches and service disruptions and enhancing perceptions of safety and reliability, such that information security risk mitigation functions as a key mechanism through which IoT data governance quality can indirectly influence customer trust by translating strong governance structures into effective security practices that foster user confidence in IoT-based startups.

H1: IoT data governance quality has a positive effect on information security risk mitigation.

H2: Data privacy policy has a positive effect on customer trust.

H3: Information security risk mitigation has a positive effect on customer trust.

H4: Information security risk mitigation mediates the relationship between IoT data governance quality and customer trust.

3. METHODS

3.1 Research Design

This study employs a quantitative research design with a causal approach to examine the relationships between IoT data governance quality, data privacy policy, information security risk mitigation, and customer trust in IoT-based startups. A quantitative method is considered appropriate because the research aims to test hypotheses and measure the strength and direction of relationships among variables using numerical data. The study adopts a cross-sectional survey

design, where data are collected at a single point in time to capture respondents' perceptions of governance, privacy, security, and trust in IoT-based startup services.

3.2 Population and Sample

The population of this study comprises users or customers of IoT-based startups operating in Bandung, Indonesia, specifically individuals who have experience using IoT-enabled products or services such as smart home devices, wearable technologies, smart mobility solutions, or other applications developed by startups, and due to the absence of a comprehensive sampling frame for IoT startup users, a non-probability sampling technique is employed; the study involves a total sample of 150 respondents, which is considered adequate for analysis using Structural Equation Modeling–Partial Least Squares (SEM-PLS), as this method is appropriate for small to medium sample sizes and the number of respondents also satisfies the minimum requirement of the "10-times rule," which suggests that the sample size should be at least ten times the maximum number of structural paths directed at any construct within the research model.

3.3 Data Collection Method

Data were collected through a structured questionnaire distributed online to respondents who met the sampling criteria in order to efficiently reach users across various IoT-based startup services in Bandung, with the instrument designed to capture respondents' perceptions of IoT data governance quality, data privacy policy, information security risk mitigation, and customer trust; prior to full-scale distribution, the questionnaire items were adapted from relevant literature and tailored to the IoT startup context to ensure content validity, followed by a pilot test involving a small group of respondents to evaluate the clarity, readability, and relevance of the items, the feedback from which was then used to refine the questionnaire before the final data collection process.

3.4 Measurement of Variables

All constructs in this study were measured using multiple indicators assessed on a five-point Likert scale, where respondents indicated their level of agreement with each statement ranging from 1 (strongly disagree) to 5 (strongly agree), with IoT Data Governance Quality captured through indicators related to the clarity of data ownership, data quality management, access control, accountability, and compliance with internal data management standards; Data Privacy Policy measured by indicators reflecting the transparency of privacy statements, clarity of data usage purposes, user consent mechanisms, and perceived protection of personal data; Information Security Risk Mitigation assessed through indicators representing the effectiveness of security controls, risk prevention measures, incident handling, and overall protection against data breaches or system misuse; and Customer Trust measured using indicators that reflect users' confidence in the startup's reliability, integrity, and ability to protect data while delivering secure IoT-based services.

3.5 Data Analysis Technique

Data analysis in this study was conducted using Structural Equation Modeling–Partial Least Squares (SEM-PLS) with SmartPLS 3 software, which was chosen due to its suitability for predictive research, its ability to accommodate complex models with multiple constructs and indicators, and its flexibility in handling data without strict normality assumptions; the analysis followed two main stages, beginning with the evaluation of the measurement model (outer model) to assess construct reliability and validity through tests of indicator reliability, internal consistency reliability using Cronbach's alpha and composite reliability, convergent validity using average variance extracted, and discriminant validity, followed by the assessment of the structural model (inner model) to examine the hypothesized relationships among constructs by analyzing path coefficients, coefficients of determination (R^2), effect sizes, and predictive relevance, with hypothesis testing

conducted using a bootstrapping procedure to determine the statistical significance of the structural paths.

4. RESULTS AND DISCUSSION

4.1 Respondent Profile

This study involved 150 respondents who are active users of IoT-based startup products or services in Bandung, Indonesia. The respondent profile was analyzed to ensure that the participants possessed sufficient experience and relevance to provide reliable perceptions regarding IoT data governance quality, data privacy policy, information security risk mitigation, and customer trust. The demographic characteristics include gender, age, educational background, type of IoT service used, and duration of IoT service usage.

Table 1. Respondent Profile

Category	Description	Frequency	Percentage (%)
Gender	Male	82	54.7
	Female	68	45.3
Age	21–30 years	63	42.0
	31–40 years	45	30.0
	41–50 years	28	18.7
	> 50 years	14	9.3
Education	Senior High School	12	8.0
	Diploma	34	22.7
	Bachelor's Degree	78	52.0
	Postgraduate Degree	26	17.3
Type of IoT Service	Smart Home	47	31.3
	Wearable / Health IoT	38	25.3
	Smart Transportation	35	23.3
	Others	30	20.0
Length of Usage	< 6 months	22	14.7
	6–12 months	41	27.3
	> 1 year	87	58.0

In terms of gender, the respondents were relatively balanced, with 82 respondents (54.7%) being male and 68 respondents (45.3%) being female, indicating that IoT-based services are utilized by both genders with comparable intensity and reducing the likelihood of gender bias in perception-related responses; regarding age, most respondents were in the 21–30 years age group with 63 respondents (42.0%), followed by those aged 31–40 years with 45 respondents (30.0%), 41–50 years with 28 respondents (18.7%), and above 50 years with 14 respondents (9.3%), reflecting the dominance of productive and technologically adaptive age groups within startup-driven IoT environments, while in terms of educational background, the majority held a bachelor's degree (78 respondents; 52.0%), followed by diploma holders (34 respondents; 22.7%), postgraduate degree holders (26 respondents; 17.3%), and senior high school graduates (12 respondents; 8.0%), suggesting that respondents generally possessed sufficient educational capacity to understand issues related to data governance, privacy, and information security.

With respect to the types of IoT-based startup services used, smart home applications were the most common, reported by 47 respondents (31.3%), followed by wearable and health-monitoring devices (38 respondents; 25.3%), smart transportation and mobility services (35 respondents; 23.3%), and other IoT-based services such as smart energy and environmental monitoring (30 respondents; 20.0%), indicating that the sample represents a broad spectrum of IoT applications; furthermore, in terms of duration of IoT service usage, 87 respondents (58.0%) had used IoT-based services for more than one year, 41 respondents (27.3%) for 6–12 months, and 22 respondents (14.7%) for less than six

months, with the predominance of long-term users suggesting sufficient experience to evaluate security practices, privacy policies, and trust-related aspects, and overall, the diversity of the respondent profile and the dominance of well-educated, experienced users enhance the reliability of the data and support the robustness of subsequent analyses on data governance, data privacy, information security risk mitigation, and customer trust among IoT-based startups in Bandung.

4.2 Measurement Model Evaluation (Outer Model)

The measurement model (outer model) evaluation was conducted to assess the reliability and validity of the constructs used in this study before testing the structural relationships. Using SmartPLS 3, the evaluation focused on indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. All constructs were modeled reflectively, in line with the theoretical foundations of IoT data governance quality, data privacy policy, information security risk mitigation, and customer trust.

1. Indicator Reliability

Indicator reliability was examined by assessing the outer loading values of each indicator on its respective construct. An outer loading value of 0.70 or higher indicates that the indicator adequately represents the construct.

Table 2. Indicator Loadings

Construct	Indicator	Outer Loading
IoT Data Governance Quality	DGQ1	0.786
	DGQ2	0.823
	DGQ3	0.867
	DGQ4	0.742
	DGQ5	0.795
Data Privacy Policy	DPP1	0.817
	DPP2	0.882
	DPP3	0.855
	DPP4	0.747
Information Security Risk Mitigation	ISRM1	0.712
	ISRM2	0.845
	ISRM3	0.857
	ISRM4	0.781
Customer Trust	CT1	0.763
	CT2	0.836
	CT3	0.897
	CT4	0.842

Table 2 presents the outer loading values for all indicators used to measure the study constructs and demonstrates that the measurement model exhibits satisfactory indicator reliability. All indicators show outer loading values above the commonly accepted threshold of 0.70, indicating that each indicator has a strong contribution in representing its respective latent construct. For IoT Data Governance Quality, the indicators load between 0.742 and 0.867, suggesting that aspects such as data ownership clarity, data quality management, access control, and accountability are consistently captured and reliably reflect the underlying governance construct. Similarly, the Data Privacy Policy indicators display high loadings ranging from 0.747 to 0.882, indicating that transparency, clarity of data usage, consent mechanisms, and perceived data protection are well perceived by respondents and strongly define the privacy policy construct.

Furthermore, the Information Security Risk Mitigation construct shows outer loading values between 0.712 and 0.857, confirming that the indicators related to security controls, risk prevention, incident handling, and protection against misuse effectively represent the organization's security

mitigation efforts in IoT-based startups. The Customer Trust construct demonstrates particularly strong indicator loadings, ranging from 0.763 to 0.897, with the highest loading observed for CT3, indicating that users' confidence in the startup's ability to protect data and provide secure services is a dominant dimension of trust.

2. Internal Consistency Reliability

Internal consistency reliability was evaluated using Cronbach's Alpha (CA) and Composite Reliability (CR), with both measures required to exceed the recommended threshold of 0.70 to confirm construct reliability, and as shown in the results, all constructs demonstrate strong internal consistency, with IoT Data Governance Quality recording CA of 0.885 and CR of 0.918, Data Privacy Policy showing CA of 0.871 and CR of 0.926, Information Security Risk Mitigation achieving CA of 0.853 and CR of 0.903, and Customer Trust presenting CA of 0.895 and CR of 0.931, thereby indicating that all measurement scales used in this study are reliable and suitable for further structural model analysis.

3. Convergent Validity

Convergent validity was assessed using the Average Variance Extracted (AVE), where a value of 0.50 or higher indicates that a construct explains more than half of the variance of its indicators, and the results show that all constructs meet this criterion, with IoT Data Governance Quality achieving an AVE of 0.638, Data Privacy Policy 0.709, Information Security Risk Mitigation 0.606, and Customer Trust 0.739, thereby confirming that all constructs in the measurement model exhibit satisfactory convergent validity and are appropriate for further analysis.

4. Discriminant Validity

Discriminant validity was assessed using the Fornell–Larcker criterion, which requires that the square root of each construct's AVE be greater than its correlations with other constructs.

Table 3. Fornell–Larcker Criterion

Construct	DGQ	DPP	ISRM	CT
IoT Data Governance Quality (DGQ)	0.797			
Data Privacy Policy (DPP)	0.562	0.845		
Information Security Risk Mitigation (ISRM)	0.624	0.493	0.772	
Customer Trust (CT)	0.516	0.651	0.684	0.856

Table 3 presents the Fornell–Larcker criterion results, which are used to assess discriminant validity by comparing the square root of the AVE for each construct with its correlations with other constructs, and the findings indicate that discriminant validity is well established, as the diagonal values representing the square roots of AVE for IoT Data Governance Quality (0.797), Data Privacy Policy (0.845), Information Security Risk Mitigation (0.772), and Customer Trust (0.856) are all higher than the corresponding inter-construct correlations in the same rows and columns, demonstrating that each construct shares more variance with its own indicators than with other constructs, thereby confirming that the latent variables are empirically distinct and that the measurement model adequately differentiates between data governance, privacy policy, security risk mitigation, and customer trust in the context of IoT-based startups.

4.3 Structural Model Evaluation (Inner Model)

After confirming that the measurement model met all reliability and validity requirements, the structural model (inner model) was evaluated to test the hypothesized relationships among the constructs. The evaluation of the structural model in SEM-PLS focuses on assessing the coefficient of determination (R^2), path coefficients, hypothesis testing, effect size (f^2), predictive relevance (Q^2), and

mediation effects. The analysis was conducted using SmartPLS 3 with a bootstrapping procedure of 5,000 resamples.

1. Coefficient of Determination (R^2)

The coefficient of determination (R^2) reflects the proportion of variance in endogenous constructs explained by the exogenous variables in the research model, and the results show that Information Security Risk Mitigation has an R^2 value of 0.387, indicating a moderate level of explanatory power whereby IoT Data Governance Quality and Data Privacy Policy jointly explain 38.7% of the variance in security risk mitigation, while Customer Trust achieves an R^2 value of 0.544, which is considered substantial, suggesting that the combined effects of data governance quality, data privacy policy, and information security risk mitigation account for 54.4% of the variance in customer trust within IoT-based startups.

2. Path Coefficients and Hypothesis Testing

Hypothesis testing was conducted by examining the path coefficients (β), t-statistics, and p-values obtained from the bootstrapping analysis. A path is considered significant if the t-value exceeds 1.96 and the p-value is less than 0.05.

Table 4. Path Coefficients and Hypothesis Testing

	Path	β Coefficient	t-value	p-value	Decision
H1	IoT Data Governance Quality → Information Security Risk Mitigation	0.628	8.475	0.000	Supported
H2	Data Privacy Policy → Customer Trust	0.412	5.963	0.000	Supported
H3	Information Security Risk Mitigation → Customer Trust	0.474	6.886	0.000	Supported

Table 4 presents the results of the structural model analysis and hypothesis testing, showing that all proposed relationships are statistically significant and supported, as evidenced by high t-values and p-values below 0.001. The path from IoT Data Governance Quality to Information Security Risk Mitigation ($\beta = 0.628$; $t = 8.475$) exhibits a strong positive effect, indicating that higher-quality data governance substantially enhances an organization's ability to mitigate information security risks in IoT-based startups. The relationship between Data Privacy Policy and Customer Trust ($\beta = 0.412$; $t = 5.963$) is also significant, suggesting that clear and transparent privacy policies play an important role in strengthening users' trust. Additionally, Information Security Risk Mitigation has a significant positive effect on Customer Trust ($\beta = 0.474$; $t = 6.886$), highlighting that effective security practices directly enhance perceptions of safety and reliability. Collectively, these findings confirm that governance and privacy mechanisms are critical drivers of security and trust in IoT-based startup environments.

3. Effect Size (f^2)

Effect size (f^2) was calculated to assess the relative impact of each exogenous construct on the endogenous constructs. According to established guidelines, f^2 values of 0.02, 0.15, and 0.35 indicate small, medium, and large effects, respectively.

Table 5. Effect Size (f^2)

Relationship	f^2	Effect Size
IoT Data Governance Quality → Information Security Risk Mitigation	0.625	Large
Data Privacy Policy → Customer Trust	0.212	Medium
Information Security Risk Mitigation → Customer Trust	0.295	Medium to Large

Table 5 presents the effect size (f^2) results, which indicate the relative impact of each exogenous construct on its corresponding endogenous construct within the model. The relationship between IoT Data Governance Quality and Information Security Risk Mitigation shows a large effect size ($f^2 = 0.625$), demonstrating that data governance quality plays a dominant role in strengthening security risk mitigation capabilities in IoT-based startups. Meanwhile, the effect of Data Privacy Policy on Customer Trust yields a medium effect size ($f^2 = 0.212$), suggesting that while privacy policies are an important driver of trust, they operate alongside other influential factors. Similarly, the relationship between Information Security Risk Mitigation and Customer Trust exhibits a medium to large effect size ($f^2 = 0.295$), indicating that effective security practices substantially enhance customer trust.

4. Predictive Relevance (Q^2)

Predictive relevance was evaluated using the Stone–Geisser Q^2 values obtained through the blindfolding procedure, where a Q^2 value greater than zero indicates that the model possesses predictive capability, and the results show that Information Security Risk Mitigation has a Q^2 value of 0.244 while Customer Trust records a Q^2 value of 0.366, with both values exceeding zero, thereby confirming that the structural model demonstrates good predictive relevance in explaining variations in information security risk mitigation and customer trust among IoT-based startup users.

5. Mediation Analysis

Mediation analysis was conducted to test whether Information Security Risk Mitigation mediates the relationship between IoT Data Governance Quality and Customer Trust. The indirect effect was evaluated using bootstrapping.

Table 6. Mediation Effect

Relationship	Indirect Effect (β)	t-value	p-value	Mediation Type
IoT Data Governance Quality → Information Security Risk Mitigation → Customer Trust	0.299	4.733	0.000	Partial Mediation

Table 6 presents the mediation analysis results, indicating that Information Security Risk Mitigation partially mediates the relationship between IoT Data Governance Quality and Customer Trust, as shown by a significant indirect effect ($\beta = 0.299$; $t = 4.733$; $p < 0.001$). This finding suggests that high-quality IoT data governance enhances customer trust not only through its direct influence but also indirectly by strengthening the organization's ability to mitigate information security risks. The presence of partial mediation implies that while effective data governance directly contributes to trust formation, a substantial portion of its impact operates through improved security risk mitigation practices, highlighting the central role of security as a transmission mechanism linking governance structures to users' trust perceptions in IoT-based startups.

Discussion

This study provides empirical evidence on the interrelationships between IoT data governance quality, data privacy policy, information security risk mitigation, and customer trust within IoT-based startups in Bandung, highlighting the strategic importance of governance and privacy practices in managing security risks and fostering trust in highly data-intensive and technology-driven startup environments. The findings underscore that beyond technological innovation, organizational mechanisms related to data management and protection play a crucial role in shaping both internal security capabilities and external user perceptions [32], [33].

First, the results demonstrate that IoT data governance quality has a strong and significant effect on information security risk mitigation, indicating that startups with clear data ownership structures, standardized data management procedures, and robust accountability mechanisms are

better positioned to identify, manage, and reduce information security risks. In IoT contexts characterized by continuous data generation and transmission across interconnected devices, weak governance can quickly lead to systemic vulnerabilities. The strong relationship identified in this study supports prior research that positions data governance as a foundational control mechanism for managing complex security risks, suggesting that for IoT-based startups in Bandung, investments in data governance should be viewed as a core component of operational risk management rather than a purely administrative function.

Second, the findings reveal that data privacy policy has a significant positive influence on customer trust, emphasizing the critical role of transparency and clarity in communicating how customer data are collected, used, and protected. Given that IoT-based services often involve continuous and sometimes intrusive data collection, customers tend to face higher perceived risks and uncertainty. A well-defined and clearly communicated privacy policy helps reduce information asymmetry, reassures users about responsible data handling, and enhances their sense of control over personal information. This result is consistent with existing literature in digital services and e-commerce, which consistently identifies privacy protection as a key antecedent of trust, and suggests that for startups in emerging markets, effective privacy communication can function as an important competitive advantage [31], [32].

Third, the study confirms that information security risk mitigation has a significant and positive effect on customer trust, indicating that trust is shaped not only by formal privacy statements but also by customers' perceptions of a startup's actual security performance. When users believe that an IoT-based startup is capable of preventing data breaches, cyberattacks, and system failures through effective security controls and risk management practices, their confidence in the reliability and integrity of the service increases. Moreover, the mediation analysis shows that information security risk mitigation partially mediates the relationship between IoT data governance quality and customer trust, suggesting that governance improvements translate into trust both directly and indirectly through enhanced security outcomes that are visible or perceived by customers.

CONCLUSION

This study concludes that IoT data governance quality and data privacy policy play critical roles in mitigating information security risks and building customer trust in IoT-based startups in Bandung. High-quality data governance significantly enhances a startup's ability to manage and reduce security risks, while transparent and well-defined data privacy policies directly strengthen customer trust. Moreover, effective information security risk mitigation not only influences customer trust directly but also acts as an important mediating mechanism through which data governance quality contributes to trust formation. These findings suggest that IoT-based startups should prioritize the integration of governance, privacy, and security practices as part of their strategic management. By doing so, startups can reduce vulnerability to security threats, increase user confidence, and support sustainable growth in increasingly competitive and data-driven markets.

REFERENCES

[1] C. Musanase, A. Vodacek, D. Hanyurwimfura, A. Uwitonze, and I. Kabandana, "Data-Driven Analysis and Machine Learning-Based Crop and Fertilizer Recommendation System for Revolutionizing Farming Practices," *Agriculture*, vol. 13, no. 11, p. 2141, 2023, doi: 10.3390/agriculture13112141.

[2] M. Altalak, M. A. Uddin, A. Alajmi, and A. Rizg, "Smart Agriculture Applications Using Deep Learning Technologies: A Survey," *Appl. Sci.*, vol. 12, no. 12, 2022, doi: 10.3390/app12125919.

[3] I. W. K. Suwastika, "Pengaruh E-Learning sebagai Salah Satu Media Pembelajaran Berbasis Teknologi Informasi Terhadap Motivasi Belajar Mahasiswa," *J. Sist. dan Inform.*, vol. 13, no. 1, pp. 1–5, 2018.

[4] E. Hadjielias, M. Christofi, P. Christou, and ..., "Digitalization, agility, and customer value in tourism," *… Forecast. Soc. …*, 2022.

[5] A. Sarfaraz and H. Hämmäinen, "5G transformation: How mobile network operators are preparing for transformation to 5G?," *2017 Internet Things Bus. …*, 2017.

[6] H. Jain, V. Chamola, and Y. Jain, "5G network slice for digital real-time healthcare system powered by network data analytics," *Internet of Things and Cyber-Physical …*. Elsevier, 2021.
[7] D. Basu, R. Datta, and U. Ghosh, "Softwarized network function virtualization for 5g: Challenges and opportunities," *Internet Things Secur. Smart …*, 2020.
[8] B. Wirajovi Aulia, M. Rizki, and P. Prindiyana, "Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital," *J. Sist. Inf. dan Teknol. Informasi)*, vol. 1, no. 1, pp. 9–20, 2023, doi: 10.33197/justinfo.vol1.iss1.2023.1253.
[9] A. Daif and A. Jalal, "The Contribution of Internal Audit to the Performance of the Internal Control System," *Eur. Sci. Journal, ESJ*, vol. 18, no. 25 SE-ESJ Social Sciences, Aug. 2022, doi: 10.19044/esj.2022.v18n25p32.
[10] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage learning, 2021.
[11] A. Wicaksono, M. Kartikasary, and N. Salma, "Analyze cloud accounting software implementation and security system for accounting in MSMEs and cloud accounting software developer," in *2020 International Conference on Information Management and Technology (ICIMTech)*, IEEE, 2020, pp. 538–543.
[12] S. Akter, S. Ali, M. Fekete-Farkas, C. Fogarassy, and Z. Lakner, "Why Organic Food? Factors Influence the Organic Food Purchase Intension in an Emerging Country (Study from Northern Part of Bangladesh)," *Resources*, vol. 12, no. 1, 2023, doi: 10.3390/resources12010005.
[13] M. Q. Shabbir, A. A. Khan, and S. R. Khan, "Brand Loyalty Brand Image and Brand Equity: the Mediating Role of Brand Awareness," *Int. J. Innov. Appl. Stud.*, vol. 19, no. 2, pp. 416–423, 2017.
[14] Y. MAZ and B. S. GAZİOĞLU, "Mentoring As a Support Mechanism in Turkish Entrepreneurship Ecosystem," *İstanbul Ticaret Üniversitesi Girişimcilik Derg.*, vol. 7, no. 13, pp. 155–167, 2023, doi: 10.55830/tje.1255980.
[15] Dr.Geeta J, "Green Intiatives of Indian Startups To Achieve Sustainability – a Step Forward," *Int. J. Eng. Technol. Manag. Sci.*, vol. 7, no. 2, pp. 884–888, 2023, doi: 10.46647/ijetms.2023.v07i02.099.
[16] T. Graziano, "Rural entrepreneurship, innovation, and technology: narratives from the italian agrifood startup ecosystem," in *Handbook of Research on Agricultural Policy, Rural Development, and Entrepreneurship in Contemporary Economies*, IGI Global, 2020, pp. 334–353.
[17] R. Verma, J. Verma, and R. Kumari, "Role of Technology Business Incubator (TBI) in Sustaining Start-Ups: The Case of Startup Incubation and Business Innovation Lab (SIBIL)," *Manag. Disruptions Bus. Causes, Conflicts, Control*, pp. 421–432, 2022.
[18] D. Fitriani, "Navigating dual logics: A framework for integrating financial performance and social impacts in Indonesian village-owned enterprises (BUMDES)," *Int. J. Innov. Res. Sci. Stud.*, vol. 8, no. 3, pp. 3492–3500, 2025, doi: 10.53894/ijirss.v8i3.7279.
[19] G. Makridou, M. Doumpos, and C. Lemonakis, "Relationship between ESG and corporate financial performance in the energy sector: empirical evidence from European companies," *Int. J. Energy Sect. Manag.*, vol. ahead-of-p, no. ahead-of-print, Jan. 2023, doi: 10.1108/IJESM-01-2023-0012.
[20] J. D. Kellerer, M. Rohringer, and D. Deufert, "Factors influencing nursing competence of registered nurses in the European Union: A scoping review," *J. Nurs. Educ. Pract.*, vol. 13, no. 1, p. 6, 2022, doi: 10.5430/jnep.v13n1p6.
[21] H. A. Al-Jaifi, A. H. Al-Rassas, and A. Al-Qadasi, "Institutional investor preferences: do internal auditing function and audit committee effectiveness matter in Malaysia?," *Manag. Res. …*, 2019, doi: 10.1108/MRR-11-2016-0258.
[22] A. Beduschi, "Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations," *Data Policy*, vol. 3, p. e15, 2021.
[23] S. S. Duri, J. G. Elliott, X. Liu, P. A. Moskowitz, and ..., "Method, system, and apparatus for dynamic data-driven privacy policy protection and data sharing," *US Pat. …*, 2008.
[24] G. D'Anna, "Law, Policy, Cybersecurity, and Data Privacy Issues by Simon Hartley," 2019.
[25] A. Derossi, B. Bhandari, K. van Bommel, M. Noort, and C. Severini, "Could 3D food printing help to improve the food supply chain resilience against disruptions such as caused by pandemic crises?," *Int. J. Food Sci. Technol.*, vol. 56, no. 9, pp. 4338–4355, 2021, doi: 10.1111/ijfs.15258.
[26] S. M. Rîndașu, "Emerging information technologies in accounting and related security risks–what is the impact on the Romanian accounting profession," *… Account. Manag. Inf. Syst.*, 2017.
[27] L. V Astakhova, "Transformation of strategic models for managing human risks of information security of an enterprise as an imperative of the digital industry," *Scientific and Technical Information Processing*. Springer, 2021. doi: 10.3103/S0147688221020027.
[28] S.-M. Rîndașu, "Emerging information technologies in accounting and related security risks–what is the impact on the Romanian accounting profession," *J. Account. Manag. Inf. Syst.*, vol. 16, no. 4, pp. 581–609, 2017.
[29] Q. A. Al-Fatlawi, D. S. Al Farttoosi, and A. H. Almagtome, "Accounting information security and it governance under cobit 5 framework: A case study," *Webology*. webology.org, 2021.
[30] M. S. Sembiring and S. M. R. Sembiring, "Do customer knowledge and customer trust in IDIC affect bank customer retention? Evidence from Indonesia," *J. Enterp. Dev.*, vol. 5, no. 3, pp. 535–552, 2023.
[31] L. Grassi, N. Figini, and L. Fedeli, "How does a data strategy enable customer value? The case of FinTechs and traditional banks under the open finance framework," *Financial Innovation*. jfin-swufe.springeropen.com, 2022. doi: 10.1186/s40854-022-00378-x.
[32] R. Verma, V. Arya, A. Thomas, E. Bolognesi, and J. Mueller, "Does startup culture in the emerging country grow around societal sustainability? An empirical study through the lens of co-creational capital and green intellect," *J. Intellect. Cap.*, vol. 24, no. 4, pp. 1047–1074, 2023, doi: 10.1108/JIC-07-2022-0162.
[33] D. P. Lazirkha, J. Hom, and V. Melinda, "Quality Analysis Of Digital Business Services In Improving Customer

Satisfaction," *Startupreneur Bus. Digit. (SABDA Journal)*, vol. 1, no. 2, pp. 156–166, 2022.