Young Journal
of Social Sciences and Humanities
| e-ISSN: 3090-2878
Vol 1, No 4 (2025)

Data Privacy Management Strategy in IoT-Based Management Information Systems

Nazwa Retno[1*], Muhammad Irwan Padli Nasution[2]
[12] Universitas Islam Negeri Sumatera Utara
Email: nazwaretno2006@gmail.com

Abstract

The development of the Internet of Things (IoT) has driven improvements in efficiency and effectiveness within management information systems (MIS) across various sectors, including industry, government, and education. However, increased connectivity and data exchange among devices introduce new risks related to data security and privacy. This article aims to identify strategies for managing data privacy in IoT-based management information systems through a conceptual approach and a review of recent literature. The findings indicate that effective strategies include implementing end-to-end encryption, multi-factor authentication, data anonymization, and strengthening data governance policies based on cybersecurity principles. In addition, integrating technical approaches with organizational policies is essential to ensure comprehensive privacy protection. This study contributes to the development of an adaptive data privacy management model in response to future IoT advances.

Keywords: *Data Privacy; Internet of Things; Cybersecurity; Data Governance*

Abstract: Perkembangan teknologi Internet of Things (IoT) telah mendorong peningkatan efisiensi dan efektivitas dalam sistem informasi manajemen (SIM) di berbagai sektor seperti industri, pemerintahan, dan pendidikan. Namun, peningkatan konektivitas dan pertukaran data antarperangkat membawa risiko baru terhadap keamanan dan privasi data. Artikel ini bertujuan untuk mengidentifikasi strategi pengelolaan privasi data dalam sistem informasi manajemen berbasis IoT melalui pendekatan konseptual dan studi literatur terkini. Hasil penelitian menunjukkan bahwa strategi efektif mencakup penerapan enkripsi end-to-end, otentikasi multi-faktor, anonimisasi data, serta penguatan kebijakan tata kelola data berbasis prinsip-prinsip keamanan siber. Selain itu, dibutuhkan integrasi antara pendekatan teknis dan kebijakan organisasi agar perlindungan privasi dapat diterapkan secara menyeluruh. Penelitian ini berkontribusi terhadap pengembangan model manajemen privasi data yang adaptif terhadap perkembangan IoT di masa depan.

Kata Kunci: *Privasi Data, Internet of Thing; Keamanan Siber; Tata Kelola Data*

INTRODUCTION

Advances in information technology have brought about a major transformation in data and information management. One of the most significant innovations is the emergence of the Internet of Things (IoT), a network of interconnected devices capable of communicating automatically

over the internet. In the context of management information systems (MIS), IoT plays a crucial role in collecting, processing, and analyzing real-time data to support faster and more accurate decision-making. IoT helps organizations improve operational efficiency, monitoring, and predicting specific conditions based on continuously updated sensor data.(Falenchia & Sumardjijati, 2023).

However, despite its benefits, IoT implementation poses serious challenges related to data privacy and security. Every IoT device has the potential to become a weak point that can be exploited by malicious parties to access or steal sensitive data. This problem becomes even more complex when the collected data originates from individuals, such as user location, activity, and preferences. This makes data privacy a key focus in the development of IoT-based management information systems (Ummah, 2019). Organizations' lack of preparedness in managing privacy can lead to data leaks, misuse of information, and loss of public trust.

Several previous studies have addressed the security aspects of IoT, but most have focused on technical aspects such as cryptography or intrusion detection systems. A gap remains in the holistic approach to privacy management, encompassing the integration of organizational policies, user education, and advanced security technologies. This article's novelty lies in developing a data privacy management strategy that emphasizes not only technical aspects but also policy and organizational governance (Ibnutama et al., 2024).

The purpose of this research is to analyze strategies that can be implemented to manage data privacy in an IoT-based management information system comprehensively. Therefore, this article is expected to contribute to strengthening an information security framework that adapts to the dynamics of today's digital technology.

METHOD

This research uses a qualitative method with a library research approach. Data were obtained from various secondary sources such as scientific journals, research reports, and academic publications relevant to the topic of data privacy and IoT. The research process was conducted through four main stages. First, identification of key issues related to data privacy management in an IoT environment. Second, analysis of security strategies that have been implemented in previous research or case studies. Third, comparisons between strategies to assess their effectiveness and integration in the context of management information systems. Finally, the development of a conceptual framework for data privacy management strategies that is adaptive and integrated (Purwanto et al., 2022).

This approach was chosen because it provides a deep understanding of the patterns, challenges, and solutions proposed by various previous researchers. The validity of the research was maintained through source

triangulation and thematic analysis of the literature. Therefore, the results of this study are not only descriptive but also analytical and reflective of the actual needs of organizations in addressing privacy risks in the IoT era.

RESULTS AND DISCUSSION

End-to-End Encryption (E2EE) Implementation

Based on a literature analysis of various recent studies on data security and privacy in Internet of Things (IoT)-based management information systems, several key strategies organizations can implement to maintain data integrity, confidentiality, and availability have been identified. These strategies encompass technical approaches, governance policies, and educational aspects focused on strengthening privacy awareness across all levels of the organization (Ibnutama et al., 2024).

End-to-end encryption is the most fundamental and crucial step in maintaining data confidentiality during transmission between devices in the IoT ecosystem. All data sent from one device to another must be encrypted using a strong cryptographic algorithm, such as Advanced Encryption Standard (AES) or Rivest–Shamir–Adleman (RSA).

With E2EE implementation, transmitted data can only be read by those with the appropriate decryption key, so that if interception occurs mid-transmission, unauthorized parties will not be able to understand the data's contents. This strategy is very effective in preventing man-in-the-middle attacks, which are often a major threat in IoT networks with thousands of connection points (Ibnutama et al., 2024).

Furthermore, encryption implementation must be accompanied by sound key management. Weak or unprotected encryption keys can create new security vulnerabilities. Therefore, organizations need to implement an automated and decentralized digital key management system (KMS) to maintain security at scale.(Sandy et al., 2023)

Multi-Factor Authentication (MFA) Implementation

Multi-Factor Authentication (MFA) is a mechanism that requires users to prove their identity through more than one layer of verification. In IoT-based management information systems, MFA implementation extends beyond a combination of passwords and verification codes, but can also involve biometric factors such as fingerprints, facial recognition, or even user behavioral authentication.(“Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan ISO 27001:2022 (Studi Kasus Data Center Dinas Komunikasi Dan Informatika Kota Tangerang Selatan),” 2023)

This approach significantly improves security by making it more difficult for unauthorized parties to gain unauthorized access. For example, even if a user's password is compromised, without additional factors such as a digital token or biometric confirmation, access will still be denied by the

system. MFA implementation is particularly relevant for organizations that manage sensitive data, such as hospitals, financial institutions, or educational institutions, where user personal data is of high value (Surbakti et al., 2023).

Furthermore, modern MFA systems can now be integrated with IoT technology itself. For example, wearable devices can serve as additional authentication tools, recognizing the physical location of the user and the device before granting access. This kind of integration strengthens the concept of context-aware security in the IoT world.(Wikarsa et al., 2022)

Data Anonymization and Pseudonymization Strategies

In IoT environments, the volume of data collected is enormous and often includes sensitive personal information, such as location, activity patterns, and even lifestyle habits. Therefore, anonymization and pseudonymization techniques are crucial strategies for maintaining privacy.(Betty Yel & M Nasution, 2022)

Data anonymization means permanently removing or obscuring identifying information so that it can no longer be linked to a specific individual. Pseudonymization, on the other hand, replaces a person's true identity with a temporary code or label that can only be identified by authorized parties.

The application of this technique is crucial for supporting data analysis activities without violating user privacy. For example, in the healthcare industry, patient data can be analyzed for medical research after undergoing an anonymization process, thus protecting patient identities.

However, the main challenge with this technique is maintaining a balance between privacy protection and data utility. Too much anonymization can reduce the analytical value of the data, while too little can increase the risk of identity leakage. Therefore, organizations must adopt dynamic anonymization policies that adjust the level of protection based on the context in which the data is used (Rifky, 2024).

Strengthening Data Governance Policy

In the context of Internet of Things (IoT)-based management information systems, policy aspects play a crucial role, no less significant than technical approaches. While the implementation of technologies such as encryption, authentication, and anonymization is the main foundation for maintaining data security, the existence of a data governance policy is an element that ensures that every process of data collection, storage, and distribution occurs in accordance with the principles of privacy, ethics, and security. Without a clear and structured policy, even the implementation of sophisticated security technology will not provide optimal protection due to weak internal regulations and coordination between organizational units.

Data governance serves as a control system that regulates the entire data lifecycle, from collection, use, storage, and destruction. In the connected digital era, organizations manage vast amounts of data, including personal user data, operational data, and sensitive organizational data. Therefore, policies are needed to ensure that this data is managed responsibly. Good data governance serves not only to meet regulatory compliance but also as a means of building public trust in the organization's commitment to protecting user privacy Wardihani et al., 2021).

One of the most crucial aspects of data governance is access authorization. This authorization serves to limit who has the right to access certain data, the context in which that access is granted, and the extent to which the data can be used or shared. This authorization setting should not be general, but rather based on the classification of data according to its level of sensitivity. For example, customer personal data should be placed in the data category with the highest level of protection, where only certain individuals or departments have direct access rights. Implementing a role-based access control (RBAC) system can help ensure that each user can only access data according to their responsibilities and job requirements. With this system, the risk of internal data misuse can be significantly minimized (Rifky, 2024).

In addition to access authorization, a transparent audit mechanism is also a crucial element of data governance. Audits serve as a means of monitoring and evaluating all activities related to data management. Through audits, organizations can determine who accessed specific data, when the access occurred, and whether the actions complied with applicable policies. These audits also help detect potential breaches or suspicious activity early before they escalate into serious data breach incidents. Audit transparency also fosters a culture of accountability within the organization, where every action related to data can be clearly accounted for.

Data governance policies should also include data retention, which defines how long data is retained and when it should be destroyed. In practice, many organizations retain data indefinitely, citing potential future needs. However, this is a high-risk practice, as the longer data is retained, the greater the risk of misuse or hacking. Therefore, data retention policies should be based on the principle of data minimization, where data is only retained for as long as it is operationally or legally relevant. After the retention period, data must be securely destroyed, such as through encryption, destruction, or secure deletion, to prevent it from being accessed by any party.

To ensure the effective implementation of these policies, organizations need to establish a dedicated institutional structure responsible for overseeing and implementing data governance. Establishing a position such as *a Data Protection Officer (DPO)* or a dedicated committee, such as *the Information Security Committee,* is a crucial step in ensuring consistent implementation of privacy policies. A DPO is responsible for ensuring that all data management

processes comply with applicable laws and assessing potential privacy risks. In Indonesia, this role has become even more crucial following the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which requires organizations to implement comprehensive data protection practices. With a DPO, organizations are not only focused on complying with regulations but also promoting an ethical culture in data use (Pratama et al., 2019).

In addition to having an oversight structure, data governance policies must also be accompanied by the regular implementation of *Privacy Impact Assessments* (PIAs). A PIA is a systematic process used to assess the potential privacy impacts of implementing new technologies or projects involving the processing of personal data. Through a PIA, organizations can map risks from the planning stage, allowing mitigation measures to be taken before they escalate into actual breaches. For example, before implementing a new IoT system for customer monitoring, organizations need to analyze how data is collected, stored, and used, as well as whether users are given control over their personal information. With this approach, data governance is no longer reactive but proactive in preventing privacy breaches.

A good data governance policy must also adapt to evolving international and national regulations. Globally, standards such as the European Union's General Data Protection Regulation (GDPR) serve as the primary reference for personal data protection. The GDPR regulates individuals' rights over their data, such as the right to erasure, the right to rectification, and the right to access personal data held by an organization. In Indonesia, a similar regulation has been implemented through the Personal Data Protection Law (PDP), which shares the same protection principle: ensuring that every individual has control over their personal data. Therefore, organizations operating in multiple jurisdictions must ensure their data governance policies align with the legal principles applicable in each region.

Furthermore, data governance focuses not only on protecting against external breaches but also on building an internal privacy culture. This culture can be achieved by instilling privacy awareness values throughout the organization. Every employee must understand their responsibility to maintain data confidentiality and the importance of adhering to established policies. Internal training and outreach programs regarding data security are highly effective ways to strengthen this awareness. Thus, data governance is no longer seen solely as the responsibility of the IT department, but rather as a shared responsibility of all members of the organization (Mudana, 2019).

Beyond institutional and cultural aspects, data governance also needs to consider supporting technology. Implementing automated data management systems, such as *Data Loss Prevention (DLP)* and *Identity and Access Management (IAM)* , can help organizations monitor and control data flows in real time. These systems can detect suspicious activity, prevent data

transfer to unauthorized parties, and provide regular compliance reports. This integration of policy and technology makes data governance more robust and adaptive to evolving threats.

Data governance policies are the primary foundation for the sustainability of IoT-based management information systems. In an increasingly complex digital environment, these policies serve not only as administrative guidelines but also as strategic instruments that determine an organization's reputation and public trust. Organizations that manage data transparently and responsibly will gain a significant competitive advantage, as modern society increasingly judges an institution's credibility by how it protects personal data. Therefore, robust, integrated, and ethically based data governance will be a key pillar in realizing a secure, trustworthy, and sustainable management information system in the Internet of Things era.

User Education and Training

The human factor is often the weakest link in the security chain. Many privacy breaches occur not due to technological failures, but rather due to user negligence, such as using weak passwords, clicking phishing links, or sharing personal data without permission. Therefore, an effective data privacy management strategy must include increasing digital awareness through regular education and training for all parties involved.

This training can include cybersecurity workshops, phishing attack simulations, and the development of ethical data usage guidelines. By building a strong security culture, organizations rely not only on technology but also on strengthening behavioral aspects that support privacy protection.

It's also crucial for organizations to involve all levels of employees in this education process, from management to operational staff. Comprehensive privacy awareness will help reduce the risk of data breaches due to human error (Monica Situmeang et al., 2023).

The study's findings demonstrate that effective data privacy management requires a synergistic approach between technical approaches and organizational policies. Technical approaches such as encryption, MFA, and anonymization do provide strong protection against direct attacks. However, without consistent governance support, these strategies will not be optimal. Conversely, good policies without the implementation of advanced technology only result in a false sense of security that is easily compromised. Therefore, an integrated data privacy management model is needed that combines technology, policy, and human resources within a single framework (an *integrated privacy management framework*). This integrated approach will ensure that security and privacy are not solely the responsibility of the IT department but become part of the overall organizational culture.

Practical Implementation in Various Sectors

In practical implementation, IoT-based data privacy strategies have proven effective in several sectors. In healthcare, for example, IoT devices are used to monitor patient conditions in real time, with encryption systems maintaining the confidentiality of medical data. Hospitals are also implementing multi-level authentication to prevent unauthorized access to patient medical records. In the industrial sector, IoT systems are used to monitor production machinery and detect potential breakdowns before they occur. The collected data is analyzed through a cloud platform protected by firewalls, *intrusion detection systems* , and data encryption. This approach increases efficiency without compromising security. Meanwhile, in the government sector, IoT is being utilized in smart city systems, such as traffic monitoring and energy management. However, its implementation is always accompanied by transparency policies and access restrictions to prevent misuse of public data (Nuraisyah, 2017).

From the discussion above, it can be concluded that managing data privacy in IoT-based management information systems is not only a technological issue, but also a management and organizational culture issue. A successful strategy is one that comprehensively integrates technical safeguards, governance policies, and user education. By implementing this strategy, organizations can not only protect data from cyber threats but also increase user trust and create a more secure and sustainable digital environment.

CONCLUSIONS

Managing data privacy in IoT-based management information systems is a significant challenge that requires a comprehensive and adaptive approach. This article demonstrates that an effective management strategy must involve a combination of security technologies such as encryption, authentication, and anonymization with robust data governance policies. User education and increased digital awareness are also key factors in maintaining privacy. Therefore, organizations in the digital era need to adopt a privacy strategy that is sustainable and responsive to evolving cyber threats. Future research is expected to develop a strategic implementation model based on real-world case studies, so that these recommendations can be effectively applied in various industry contexts.

REFERENCES

Betty Yel, M., & M Nasution, MK (2022). Personal Data Information Security on Social Media. *Kaputama Informatics Journal (Jik)* , *6* (1).

Falenchia, M., & Sumardjijati, S. (2023). Adolescent Digital Literacy in Roleplay Games on Twitter. *Jiip - Scientific Journal of Educational Sciences* , *6* (6). https://Doi.Org/10.54371/Jiip.V6i6.1585

Hassan St, MO, Fatahillah, MA, Fahresi, MD, & Kaswar, AB (2020). Design and Construction of an IoT-Based Dam Monitoring and Management System. *Jurnal Media Elektrik* , *17* (3). https://Doi.Org/10.26858/Metrik.V17i3.14965

Hernandes, D. (2023). Development of an IoT-Based Library Management Information System: A Case Study of the ABC High School Library. *Journal of Computer Science (Jilkom)* .

Ibnutama, K., Suryanata, MG, Pane, DH, Al Hafiz, A., & Lubis, Z. (2024). Development of the Darul Adib Tahfiz Academic System. *Abdimas Iptek* , *4* (1). Https://Doi.Org/10.53513/Abdi.V4i1.9502

Monica Situmeang, Alif Fahrezy, M., Shella Fahdilla Sari, & Aidil Halim Lubis. (2023). Implementation of a State-Owned Inventory Management Information System: A Case Study of the Medan Religious Education and Training Center. *Journal of Informatics, Technology, and Science (Jinteks)* , *5* (4). https://Doi.Org/10.51401/Jinteks.V5i4.3504

Mudana, IW (2019). The Role of Libraries in Literacy Development for School Library Managers in Buleleng Regency. *Acarya Pustaka* , *5* (2). Https://Doi.Org/10.23887/Ap.V5i2.17413

Nuraisyah, A. (2017). Analysis of Business Incubators' Performance in Mentoring Tenant Businesses (Fostered Businesses) (Case Study of Solo Technopark Technology Business Incubator). *Faculty of Economics and Business, Uns* , *1* .

Design of Information Security Management System (ISMS) Based on ISO 27001:2022 (Case Study of Data Center of Communication and Informatics Department of South Tangerang City). (2023). *Scientific Journal of Computing* , *22* (4). Https://Doi.Org/10.32409/Jikstik.22.4.3447

Pratama, AR, Rahmah, A., & Arief, B. (2019). Bus Terminal Performance Analysis Study (Case Study: Type A Terminal Kh. Ahmad Sanusi, Sukabumi City). *Online Journal of Civil Engineering Students (Jom)* , *1* (1).

Purwanto, H., Prasatya, JD, Cahyadi, TA, & Maharani, YN (2022). Knowledge Management for Tsunami Disaster Risk – Literature Review. *Racic: Rab Construction Research* , *7* (2). https://Doi.Org/10.36341/Racic.V7i2.3001

Riskiyah, I. (2023). Salt Pond Irrigation Management System Based on the Internet of Things (IoT). *Journal of Informatics and Applied Electrical Engineering* , *11* (3). https://Doi.Org/10.23960/Jitet.V11i3.3184

Sandy, F., Adi Palangi, W., Liling, D., Putra Pratama, M., Studi, P., Pendidikan, T., Keguruan, F., & Pendidikan, I. (2023). Implementation of the Use of Artificial Intelligence in Higher Education. *National Seminar on Educational Technology Uki Toraja* .

Surbakti, TB, Fauzi, A., & Khair, H. (2023). Rivest Shamir Adleman (Rsa) Hybrid Algorithm System And The Deep Blum Blum Shub (Bbs) Algorithm Securing E-Absence Database Files. *Indonesian Journal Of Education And Computer Science* , *1* (2). https://Doi.Org/10.60076/Indotech.V1i2.59

Ummah, NI (2019). Management of Gender-Responsive Educational Facilities and Infrastructure: A Study at Jember Islamic Boarding School. *An-Nisa Journal of Women and Islamic Studies* , *12* (2). https://Doi.Org/10.35719/Annisa.V12i2.14

Wardihani, ED, Supriyo, B., & Sayekti, I. (2021). Implementation of an IoT-Based Library Information and Management System at Sdn Kramas, Tembalang, Semarang City. *Bhakti Persada* , *7* (1). Https://Doi.Org/10.31940/Bp.V7i1.2160

Wikarsa, L., Suwanto, T., & Lengkey, C. (2022). Implementation of the Proof-Of-Work Consensus Algorithm in Blockchain for Medical Records. *Jurnal Pekommas* , *7* (1). https://Doi.Org/10.56873/Jpkm.V7i1.4403

Yustira, A. (2017). Hospital Information System of Gumawang Regional General Hospital Using Java Server Pages (JSP). *Information System* .