International Journal of Social Science, Educational, Economics, Agriculture Research and Technology (IJSET) | ISSN (e) : 2827-766X
Volumes 4 No. 9 (2025)

USER DATA SECURITY IN E-COMMERCE APPLICATIONS: A CASE STUDY ON SHOOPE AND TOKOPEDIA

Niswatul Ajmi[1], Audya Cantika Putri[2], Rayyan Firdaus[3]
[1,2,3]Accounting Study Program, Faculty of Economics and Business, Universitas Malikussaleh, Indonesia
E-mail : niswatul.230420173@mhs.unimal.ac.id[1] Audya.230420169@mhs.unimal.ac.id[2] rayyan@unimal.ac.id[3]

Received	: 25 Mei 2025	Published	: 13 July 2025
Revised	: 5 Juni 2025	DOI	:https://doi.org/10.54443/ijset.v4i9.904
Accepted	: 30 Juni 2025	Publish Link	:https://www.ijset.org/index.php/ijset/index904

Abstract

The rapid growth of digital transactions in Indonesia has driven the expansion of major e-commerce platforms such as Shopee and Tokopedia. However, this growth also raises significant concerns regarding the security and privacy of user data. This study aims to examine and compare the data security policies implemented by these two platforms and assess their effectiveness in protecting personal data in accordance with national regulations, including the Indonesian Personal Data Protection Law (PDP Law) and the Electronic Information and Transactions Law (ITE Law). This research adopts a qualitative descriptive method with a case study approach. Data were collected through document analysis of privacy policies, security incident reports, and relevant literature. The findings reveal that although both platforms have applied security features such as two-factor authentication and data encryption, there remain gaps in policy execution and a lack of transparency in communicating risks to users, particularly highlighted by the 2020 Tokopedia data breach. This study recommends strengthening user data protection through better regulatory compliance and increased user privacy awareness. The results provide valuable insights for app developers and policymakers to develop more proactive and inclusive digital security frameworks.

Keywords: ***data security, e-commerce, Tokopedia, Shopee, personal data protection, data breach.***

INTRODUCTION

The development of information technology has brought about significant changes in various aspects of human life, one of which is trading activities through digital platforms, known as e-commerce. In Indonesia, the use of e-commerce applications such as Shopee and Tokopedia has experienced significant growth, not only in the number of users but also in the volume of daily transactions. The ease of shopping, product variety, and various digital features are major attractions for consumers. However, behind this convenience, there are serious challenges related to the security and protection of users' personal data. The personal data collected by e-commerce platforms is not limited to basic information such as name and address, but also includes shopping history, consumer preferences, and financial data such as account or credit card numbers. This information is a valuable asset but also vulnerable to misuse, especially if security systems are not properly managed. Several data breach incidents that have occurred in Indonesia in recent years demonstrate that this issue is not just a potential issue, but a real risk that could harm millions of users.

According to a 2023 report by iPrice and DataIndonesia.id, Shopee averaged 157 million monthly visits, followed by Tokopedia with around 129 million. This large user base places both platforms as prime targets for various personal data breach risks. Law No. 27 of 2022 concerning Personal Data Protection was enacted to demonstrate the state's responsibility to protect citizens' digital rights. However, implementation at the platform level still shows gaps, both in terms of policy transparency, user education, and system readiness in dealing with cyber threats. Therefore, it is important to evaluate the extent to which e-commerce applications such as Shopee and Tokopedia implement data security principles and their compliance with applicable regulations. This study aims to analyze and compare data security policies and practices on Shopee and Tokopedia, with an emphasis on user protection. Using a case study approach and qualitative analysis methods, this study is expected to contribute to strengthening the digital security

literature in the e-commerce sector and serve as a basis for consideration for platform developers, regulators, and users in building a safe and trusted digital ecosystem.

LITERATURE REVIEW

Data security in information systems is based on the CIA (Confidentiality, Integrity, Availability) principle, which serves as the foundation for securing user data in a digital environment (Stallings & Brown, 2018). Confidentiality ensures information is only accessed by authorized parties, Integrity guarantees the integrity and accuracy of data, and Availability emphasizes that data must be accessible whenever needed. Personal data protection is also reflected in the principles stipulated in Law No. 27 of 2022 concerning Personal Data Protection and the ITE Law, which emphasize the right to consent, restrictions on collection, and user access to their personal data. A study by Hapsari & Widodo (2020) revealed that many e-commerce platforms still focus on technical aspects without adequate education or transparency. Handayani et al. (2020) stated that the absence of reporting channels and user controls is a fundamental weakness of current security policies. ISO/IEC 27001, as an international standard, also encourages audit transparency and systematic risk mitigation. Shopee and Tokopedia have different privacy policies in terms of delivery, transparency, and completeness of user control features, which affect user perception and level of trust in the platform.

RESEARCH METHODS

This research uses a descriptive qualitative approach with a case study design. The subjects were Shopee and Tokopedia, two of the most popular e-commerce platforms in Indonesia. Data collection techniques were conducted through content analysis of online privacy policies, as well as supporting literature from scientific journals and official documents such as the PDP Law and the ITE Law. Data were analyzed thematically and compared using CIA principles and personal data protection indicators based on national regulations.

RESEARCH RESULT

This research uses a descriptive qualitative approach with a case study design on two of Indonesia's largest e-commerce platforms, Shopee and Tokopedia. Data were obtained through an analysis of privacy policy documents, security incident reports, and relevant scientific literature from January to April 2024. Based on the analysis of privacy policy documents available on each platform's official website, it was found that Shopee and Tokopedia have implemented several technical security features such as two-factor authentication, transaction data encryption, and suspicious activity notifications via email or SMS. However, the study results show that Shopee demonstrates a more systematic approach in conveying privacy and data protection information, including providing a user education center, an incident reporting channel, and regular digital security campaigns. This aligns with the principle of availability within the CIA framework, where information is easily accessible to users. Conversely, Tokopedia is considered less transparent, particularly regarding user data control. Features such as permanent account deletion, granular settings for the types of data collected, and security audit information are not yet publicly available. This is confirmed by a comparison of the content structure of the two platforms' privacy policies, which shows that Shopee is more detailed and communicative in explaining user rights. Furthermore, literature and incident reports indicate that Tokopedia experienced a data breach in 2020, impacting over 91 million accounts. This incident serves as a key evaluation point in this study, as no follow-up information or long-term mitigation system was publicly published by the company. Therefore, based on the data collected and analyzed, it is concluded that the implementation of data protection principles is not yet optimal, particularly in terms of transparency, user empowerment, and documentation of accountable data protection practices.

DISCUSSION

This discussion is structured based on the main findings from the analysis of relevant documents, literature, and incident reports, with a focus on six key aspects that are in line with the objectives and focus of the research, namely: data security, e-commerce, Tokopedia, Shopee, personal data protection, and data leaks.

Data Security

Data security is a key pillar in managing digital information systems, particularly in the context of e-commerce applications that collect a variety of sensitive user information. This user data is not limited to names, addresses, and contact numbers, but also includes transaction history, payment methods, consumption preferences, and even credit

card or bank account data. With the high volume of data processed by platforms like Shopee and Tokopedia, the responsibility of data managers to maintain the integrity and confidentiality of this data becomes increasingly significant. The CIA (Confidentiality, Integrity, Availability) principle, as explained by Stallings and Brown (2018), provides a basic framework for data security. Confidentiality emphasizes the importance of information confidentiality, Integrity maintains data accuracy and consistency, while Availability ensures data can be accessed when needed by authorized parties. In practice, the CIA principle has not been optimally implemented across all e-commerce platforms in Indonesia. Gaps remain regarding transparency in system audits, minimal user involvement in personal data control, and irregularity in periodic security evaluations.

Some platforms have implemented technical safeguards such as data encryption and two-factor authentication. However, these technical safeguards do not necessarily guarantee data security if they are not accompanied by strong and accountable internal policies. Research by Handayani et al. (2020) noted that the majority of digital companies in Indonesia do not yet have a structured security incident monitoring system and do not provide an incident reporting mechanism that is openly accessible to users. Specifically, in the case of Shopee and Tokopedia, although both have privacy policy documents, the effectiveness of their implementation remains questionable. The platforms are considered to have not provided adequate access control to users to manage their data independently, including regarding permanent data deletion or regulating data that can be shared with third parties. Therefore, data protection efforts are not sufficient from a technical perspective alone; they also require strengthening internal regulations and systematic public education.

E-Commerce

The e-commerce industry in Indonesia has grown exponentially over the past decade. Digital transformation has driven changes in consumer consumption patterns, leading to an increasing reliance on online platforms for shopping. According to data from iPrice and DataIndonesia.id (2023), Shopee and Tokopedia are the two platforms with the highest user traffic, with 157 million and 129 million visits per month, respectively. This high transaction volume indicates that these two platforms play a significant role in the national digital economy. However, this growth also brings challenges related to consumer protection, particularly regarding personal data security. As the number of users increases, the risk of data leaks and misuse increases. According to Ardiansyah (2021), e-commerce is not only a transaction medium but also a complex data collection ecosystem. Therefore, a data management system is needed that can guarantee data confidentiality, accuracy, and continuous availability. Although e-commerce companies like Shopee and Tokopedia claim to use high-security systems, this doesn't always translate into actual protection experienced by users. In many cases, users don't understand how their data is collected, stored, and distributed. This is exacerbated by the platform's lack of initiatives to provide adequate education about user rights and data protection mechanisms. Therefore, e-commerce management in the digital era must encompass not only service efficiency but also guarantee digital security. Collaboration between businesses, regulators, and the public is needed to build an e-commerce ecosystem that is not only economically profitable but also safe and reliable for users.

Tokopedia

Tokopedia, one of the largest e-commerce platforms in Indonesia, has faced significant challenges related to data security. A data breach in 2020 demonstrated that the platform's digital security system was not fully prepared for cyberattacks. The incident involved the breach of over 91 million user accounts, including information such as email addresses, birth dates, and phone numbers. This incident raised public concern and sparked widespread debate about the technology company's readiness to safeguard user privacy. Hapsari and Widodo (2020) highlighted the company's weak audit system and the lack of transparent follow-up. Following the incident, no official report or long-term mitigation system was publicly disclosed. This demonstrates a weak principle of integrity and accountability in user data management. Furthermore, the lack of user education about post-incident steps exacerbated the impact. In terms of privacy policies, Tokopedia is considered to have inadequate data control features. Important features such as permanent account deletion, restrictions on the types of data collected, and user access to data audits are not yet fully available. When users lack full control over the personal information they provide, this potentially violates the principle of confidentiality as outlined in the CIA model. Having experienced a significant data breach, Tokopedia should take serious steps to improve its internal security systems and strengthen policy transparency. These efforts are crucial not only for reputation restoration but also to ensure user trust in the platform remains intact amidst increasingly fierce industry competition.

Shopee

Shopee, Tokopedia's main competitor, demonstrates a more progressive approach to managing user data security. The platform provides a more comprehensive and easily accessible privacy policy document. Furthermore, Shopee actively educates users through digital campaigns and provides an integrated security incident reporting channel within the app. In its technical implementation, Shopee has also implemented various layers of security, such as data encryption, two-factor authentication, and a suspicious activity detection system. This aligns with the Availability and Integrity principles of the CIA model, as users are provided with protection and information in the event of a breach. However, Shopee has not yet fully met the Confidentiality principle. Despite the availability of a privacy policy, users still lack full control over their data, such as the ability to permanently delete accounts and data or restrict the collection of certain data. Indrawati (2021) stated that user trust in a platform is highly dependent on the level of control they have over their personal data. Therefore, Shopee still needs to strengthen user control and build an open security reporting and evaluation system to maintain a competitive advantage in the e-commerce industry.

Personal Data Protection

Personal data protection in Indonesia has a strong legal basis through Law No. 27 of 2022. This regulation provides comprehensive protection for user rights, such as the right to access, correction, deletion, restriction of processing, and the right not to be subject to automated decision-making. However, its implementation at the e-commerce platform level still shows gaps. Neither Shopee nor Tokopedia fully provides features that allow users to exercise these rights independently. For example, features for deleting data or controlling the type of data collected are still limited and difficult for ordinary users to access. Handayani et al. (2020) emphasized that regulations will not be effective if not accompanied by internal systems that support the implementation of data protection principles. In this regard, companies must develop operational policies that not only comply with the law but also take into account the public's digital literacy. Strengthening personal data protection must be a shared priority, especially given the increasing dependence of society on digital platforms in their daily lives. Existing regulations also need to be accompanied by increased capacity of supervisory institutions and the existence of effective sanctions for violators.

Data Leak

Data breaches are one of the biggest risks facing digital companies. Incidents like the one at Tokopedia not only impact technical and legal aspects but also create a crisis of public trust. According to Riyanto (2020), data breach management must begin with preventative measures such as regular system evaluations and penetration testing. Unfortunately, there is no requirement to publish security audit results publicly, resulting in low accountability for digital companies. Companies also need to have clear incident management protocols, including timely notification to users, provision of information on recovery steps, and prompt and responsive complaint support. Transparency in handling security breaches will be a key indicator of a platform's credibility. In the context of Shopee and Tokopedia, data breach mitigation measures are still not fully visible. Therefore, systemic improvements are needed, including internal education, the development of security SOPs, and public reporting to demonstrate corporate social responsibility to users.

CONCLUSION AND SUGGESTIONS

Conclusion

Based on an analysis of the two largest e-commerce platforms in Indonesia, Shopee and Tokopedia, it was concluded that both have privacy policies and basic technical mechanisms to maintain user data security, such as data encryption and two-factor authentication. However, the effectiveness of implementing these policies remains suboptimal. Shopee demonstrates a more systematic approach to user education, the dissemination of privacy information, and the provision of an incident reporting channel. Meanwhile, Tokopedia still faces limitations related to transparency, user control over personal data, and lacks an open audit system. The 2020 Tokopedia data breach is clear evidence that strengthening data security and risk mitigation must be a top priority. Both platforms have also not fully implemented data security principles based on the CIA model. Gaps remain regarding Confidentiality (user control), Integrity (availability of audit processes and incident follow-up), and Availability (access to information in emergencies).

Suggestion

Improved User Control: Shopee and Tokopedia need to provide features that allow users to independently manage, access, and delete personal data in accordance with personal data protection principles. Audit and Transparency: Both platforms need to commit to publishing internal audit policies and incident handling reports to demonstrate accountability to the public. Digital Security Education: Platforms must actively educate users on how to safeguard their personal data and provide guidance on how to respond to data breaches. Implementation of International Standards: Shopee and Tokopedia are advised to align their security systems with standards such as ISO/IEC 27001, including conducting regular penetration testing. Collaboration with Regulators: It is crucial for e-commerce platform providers to strengthen cooperation with the government and data protection authorities to ensure the effective implementation of the Personal Data Protection Law.

By implementing these steps, it is hoped that Indonesia's digital ecosystem can grow sustainably while upholding security and user trust.

REFERENCES

Ardiansyah, M. (2021). Perlindungan Data Konsumen dalam Transaksi E-Commerce: Tinjauan Praktik dan Tantangan. Jurnal Ekonomi Digital, 4(1), 23–34.

Handayani, S., Nugroho, P. D., & Prasetyo, Y. (2020). Perlindungan Data Pribadi dalam Era Ekonomi Digital: Tinjauan Regulasi dan Implementasi. Jurnal Ilmiah Teknologi Informasi, 18(2), 102–111.

Hapsari, D., & Widodo, W. (2020). Tinjauan Kebijakan Keamanan Data pada Layanan E-Commerce di Indonesia. Jurnal Sistem Informasi dan Keamanan Siber, 5(1), 1–10.

Indrawati, R. (2021). Perlindungan Privasi Pengguna dalam Platform Digital: Kewajiban Hukum dan Praktek di Indonesia. Jurnal Hukum dan Teknologi, 7(2), 45–59.

Riyanto, B. (2020). Audit Keamanan Informasi pada Sistem E-Commerce di Indonesia: Perspektif ISO/IEC 27001. Jurnal Keamanan Siber dan Informasi, 3(2), 75–85.

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson.