Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th February 2026. Vol. 5. No. 2; e-ISSN: 2808-4519

Cyber Threat Analysis to Personal Data in the Digital Era

A. Hamdani[1], Bilqis Sofia[2], Farah Salsabilla Aulia Rahmah[3], Ika Ariyanti[4]

[1]*Universitas Ibrahimy*
[2,3]*Teknologi Informasi, Fakultas Sains dan Teknologi*
[4]*Situbondo*

dan.kidz88@gmail.com[1], bilqissofia34@gmail.com[2], farahsalsabilla206@gmail.com[3], ikaariyanti809@gmail.com[4]

Abstract

The development of information technology provides convenience in daily life, but at the same time increases the risk of cyber threats to users' personal data. This study aims to analyze the level of user vulnerability to digital threats and the factors that influence personal data security, including the role of digital literacy and user behavior. The method used is descriptive qualitative, collecting data through a literature review, structured observation of digital device usage patterns, and semi-structured interviews with a number of selected users. The results show that weak password management practices, the tendency to share personal information, and low awareness of suspicious links or applications are the main causes of data vulnerability. The level of attention to vulnerability evaluation, security awareness, and security audits remains low, even though users are aware of potential threats. These findings confirm that digital literacy and user behavior play a crucial role in reducing risks. Therefore, improving cybersecurity education, implementing safe digital practices, and conducting regular security audits and evaluations are necessary to effectively protect personal data and build a safer digital culture.

Keywords: *Cybersecurity, Personal data, Digital literacy, Cyber threats, User behavior*

1. Introduction

The development of information technology in the digital era has brought very significant changes in people's lives. The use of digital technology has facilitated various activities, such as communication, education, health services, government administration, electronic commerce, and financial transactions. Digitalization encourages efficiency and acceleration of services, but on the other hand, it also poses serious challenges in the form of increasing cybersecurity threats, especially related to the protection of users' personal data. [1] Personal data currently has high economic and strategic value, making it a prime target for cybercrime. Information such as population identity, financial data, contact information, and digital activity history can be misused for fraud, identity theft, extortion, and other financial crimes. This condition makes the protection of personal data a crucial issue in the management of digital systems, both by the government and technology-based service providers. In Indonesia, the increasing cases of data leaks in government agencies and digital companies show that the money information management system implemented still has various weaknesses. The causative factors include the limitation of security infrastructure, the lack of regular supervision and auditing of the system, and the implementation of data security standards is not optimal. In addition, the rapid development of technology is often not balanced with the readiness of an adequate protection system.

Cybersecurity threats are also becoming more complex as phishing, malware, ransomware, and social engineering methods develop. These attacks not only exploit technical loopholes in the system, but also exploit psychological and behavioral aspects of users. This shows that cybersecurity does not solely depend on technology, but also on human awareness and behavior as users of digital systems. [2] The low level of cybersecurity literacy in the community also increases the risk of personal data leakage. Many users still use weak passwords, share personal information excessively on social media, and are less wary of potentially harmful links and apps. Lack of understanding of digital privacy makes users vulnerable to becoming victims of cybercrime. [3] Therefore, efforts to improve cybersecurity need to be carried out comprehensively and sustainably. From the technology side, it is necessary to strengthen the security system through the implementation of encryption, strict access management, and regular system updates. In terms of regulations, the government needs to check the existence of a firm and effective personal data protection policy. Meanwhile, increasing digital literacy through continuous education is an important step to shape safer and more responsible user behavior. Synergy between the government, digital service providers, and the public is the key to realizing optimal personal data protection in the digital era. [4]

2. Research Method

In this section, the research applied to analyze the types of cyber threats and weaknesses of personal data in the digital age is described. The methods used are literature review, observation, interviews, and data analysis, which aim to obtain a comprehensive and accurate informality of the phenomenon being studied. The following explanation will describe each step in a structured manner, so that the reader follows the research process from the beginning to the conclusion clearly and systematically. [5]

2.1. Research Design

This study applies a brief descriptive qualitative approach to analyze the types of real threats to personal data as well as the elements that contribute to its vulnerability in the digital age. [6]

2.1.1. Figure and Table

The figure below shows the steps in the research methods applied in this study, which range from the data collection phase to the drawing of conclusions. [7]

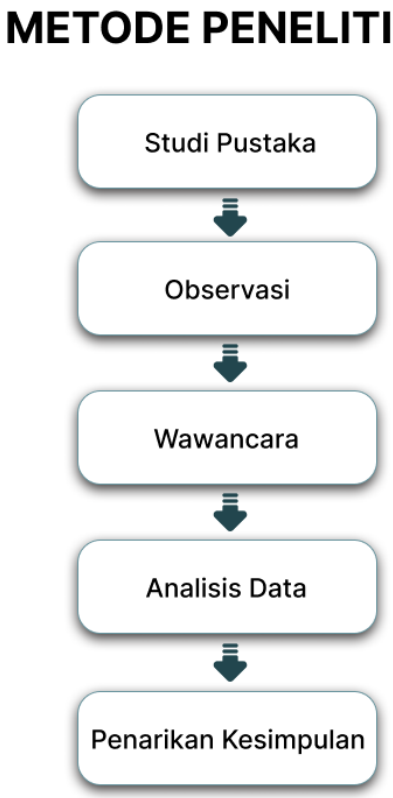

Fig. 1: Research methods

2.2. Data source and Data collection

Data is collected through:

1. Literature review from journals, scientific articles, and literature related to personal data security and cyber threats, to build a strong theoretical foundation and enrich understanding of the issues being studied.
2. Structured observation of the patterns of use of digital devices and data management practices of personal data by users, so as to identify habits, risks, and potential security loopholes in real terms.
3. Semi-structured interviews with selected information to explore understanding and experience related to cybersecurity, so that the data obtained is more in-depth and contextual.

2.3. Data Analysis Technique

The analysis is carried out through the following stages:

1. Data reduction to identify relevant information about attack types, hacking techniques, and patterns of personal data leaks, so that important information can be focused and less sophisticated data can be filtered.
2. The presentation of data in the form of thematic narratives or threat category tables, so that the patterns, relationships, and trends of cyber threats can be understood more clearly and systematically.
3. Conclusions are drawn based on the vulnerability patterns and causative factors found, so that the results of the analysis provide a comprehensive picture of the risks and weaknesses in the management of personal data.

2.4. Data Validity

The reliability of the data is maintained through triangulation of sources (Literature, Observations, and interviews) and cross-checks between information to ensure the consistency of findings and minimize bias. This approach allows for data validation from multiple perspectives so that research results are more accurate and trustworthy.

2.5. Results and Discussion

The results of this study indicate that the level of user attention to the cybersecurity aspect still varies on several important points. From the graph, it can be seen that the majority of respondents rate threats as the most important thing (85%), which shows that they are quite sensitive to the possibility of digital attacks that can compromise their data and privacy. In addition, attention to data protection and risk management is also relatively high (70%), which indicates that many users are aware of the importance of maintaining the confidentiality of personal data and carrying out basic risk management in their digital activities. However, some other factors indicate a lower level of attention. The likelihood of evaluation only reaches (55%), which indicates that they still haven't regularly checked for security vulnerabilities on the devices or accounts they use. In addition, user awareness (45%) and security audits (30%) were recorded as the lowest scoring aspects, which indicated that safe behavior and conducting periodic security checks were still not optimally carried out. These findings confirm that the security of personal data does not only depend on technology, but also on user behavior and knowledge. Low security awareness and security audits indicate the need for more intensive cybersecurity education in order to understand and implement better security practices. With the increase in digital knowledge and changes in safer habits, the risk of threats and leaks of personal data can be significantly reduced, creating a more secure and secure digital environment for all users.

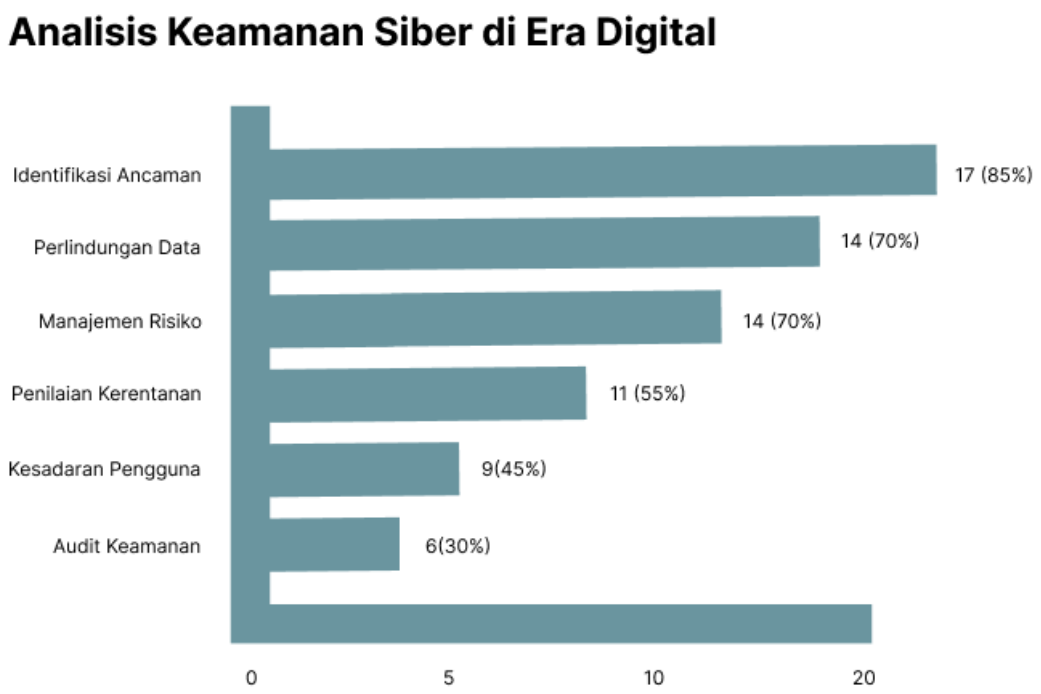

Fig. 2: Comparison chart

3. Conclusion

The study shows that even if users are sufficiently aware of cyber threats, their overall digital security practices are still not optimal. Aspects such as vulnerability evaluation, security awareness, and security audits are noted to have relatively low levels of concern, increasing the

potential for personal data leaks. These findings confirm that data security is not only dependent on technology, but is also heavily influenced by digital literacy and user behavior itself. Therefore, education about cybersecurity and the implementation of safe digital habits need to be continuously improved so that threat risks can be effectively minimized.

4. Suggestion

To predict and anticipate cyber threats, users need to increase their understanding of good digital security practices. This includes getting used to implementing safer digital behaviors, such as using stronger and unique passwords, regularly updating systems and software, and checking device security and conducting security audits on a regular basis with these measures, potential threats can be more quickly identified and mitigated, so that the protection of personal data and sensitive information can be significantly improved.

Expression of gratitude

The author would like to express his gratitude to all parties who have contributed to the preparation of this journal. It is hoped that this work can provide benefits for the advancement of cybersecurity in the digital age.

References

[1] Z. J. Wantania, "(Analysis of The Development of Legal Protection For Personal Data Security In The Digital Era)," vol. 14, no. 87, pp. 179–194, 2025.
[2] S. Hasrina, I. Sari, T. Tri, F. Manguma, and E. Fatra, "Analisis Hukum Pidana Atas Keamanan Data Dan Serangan Siber Terhadap Pertahanan Nasional," vol. 2, no. 1, pp. 1–5, 2025.
[3] Y. Daeng, N. Linra, A. Darham, D. Handrianto, and R. R. Sianturi, "Perlindungan Data Pribadi dalam Era Digital : Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi," vol. 3, pp. 2898–2905, 2023.
[4] S. T. Zahwani and M. I. P. Nasution, "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital," vol. 2, no. 2, pp. 105–109, 2024.
[5] A. A. Ardelia, Q. Amiroh, and R. Aisy, "Analisis Keamanan dan Privasi Data Instagram Terhadap Ancaman Phishing di Era Digital," pp. 366–370, 2024.
[6] S. Agustin, "Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber," vol. 1, no. 6, pp. 500–504, 2024.
[7] "Ath-Thariq ; Jurnal dakwah dan komunikasi, Vol. 06, No. 02, Juli-Desember 2022 220," vol. 06, no. 02, pp. 220–235, 2022.