JOURNAL INFORMATIC, EDUCATION AND MANAGEMENT (JIEM)
Vol. 7, No. 1, February 2025, pp. 1 ~ 11
ISSN: 2716-0696, DOI: 10.61992/jiem.v7i1.107

Data Security Analysis in Electronic Health Information Systems

Adi Ahmad[1*], Yusmanidar[2], Juria Hastuti[3], Maudi Hijriatin[4], Sarno[5]
[1*] STMIK Indonesia Banda Aceh
[2,3,4,5]Sekolah Tinggi Ilmu Administrasi Pelita Nusantara

Article Info

Article history:
Received 15 December 2024
Revised 30 January 2025
Accepted 20 February 2025

Keywords:
Data Security, Electronic Health Information System, Vulnerability, Data Protection, Encryption, Multi-Factor Authentication.

ABSTRACT

This study aims to analyze data security in electronic health information systems (EHIS). With the increasing use of information technology in healthcare, data security issues are becoming increasingly important given the sensitivity of medical information. The research methodology involved an in-depth literature review as well as case study analysis on several hospitals that have implemented SIKE. Data analysis techniques included evaluation of system vulnerabilities, identification of potential threats, and assessment of data protection mechanisms in place. The results showed that despite various efforts to improve data security, there are still many vulnerabilities that can be exploited by irresponsible parties. The main threats include cyberattacks, data leakage, and unauthorized access. In addition, this study found that the implementation of security protocols such as data encryption, multi-factor authentication, and regular audits can significantly reduce these risks. However, this research has several limitations, including a limited sample of case studies that may not represent the entire SIKE landscape in Indonesia and limited access to internal hospital data. Nonetheless, this research makes a significant contribution in providing practical recommendations for SIKE managers to improve data security, as well as a basis for further research in this area.

Corresponding Author:
Adi Ahmad | STMIK Indonesia Banda Aceh
Email: adiahmad@stmikiba.ac.id

1. Introduction

Cybersecurity is becoming an increasingly important issue in the context of digital transformation. Malicious actors continue to develop new and more sophisticated methods to threaten and attack organizational information systems. Recognizing the importance of theoretical frameworks in facing these challenges, this research aims to provide a comprehensive analysis of cyber security challenges in the era of digital transformation, with a focus on information systems (Adi Ahmad et al, 2024).

Electronic Health Information Systems (EHIS) have become the backbone of medical data management in many hospitals and healthcare facilities. With SIKE, the collection, storage and processing of patient data is done electronically, which enables medical personnel to provide healthcare services quickly and efficiently. The system offers various benefits such as easy access to patient data, reduction in medical errors, and improved coordination between departments. However, along with the increased use of this technology comes a major challenge regarding data security.

Data security in SIKE is crucial as patient medical data is highly sensitive and personal information. Leakage or misuse of this data can have a devastating impact, not only on the individual whose data is leaked, but also on the reputation of the health institution concerned. Data leakage cases that have occurred in various parts of the world show that threats to health data security are global and require serious attention (Smith, 2020). For example, incidents involving cyber-attacks against hospitals can lead to operational disruption, extortion and loss of public trust in the health system.

In Indonesia, SIKE implementation has begun in various hospitals and clinics, but data security challenges are still an issue that needs to be addressed. According to a report from the Ministry of Health, although many hospitals have adopted SIKE, the implementation of security protocols is often overlooked or inadequate (MOH, 2021). This creates loopholes that can be exploited by irresponsible parties to illegally access patient data. Deficiencies in data security policies and practices also contribute to the increased risk of medical information leakage.

The main motivation for this study was to understand the extent to which data security is implemented in SIKE in Indonesia, identify gaps that still exist, and provide recommendations for improvement. This research seeks to fill the gap in the literature related to analyzing data security in SIKE in Indonesia and provide additional insights for health facility managers in improving data security. Based on reports from the Ministry of Health, many hospitals have not implemented adequate security measures, such as data encryption, multi-factor authentication, and regular security audits (MOH, 2021).

This research was also triggered by several incidents of medical data leakage that occurred in various countries, indicating that threats to health data are global and require serious attention. For example, the WannaCry ransomware attack in 2017 that targeted healthcare services in various countries, including the UK, showed how vulnerable health systems are to cyberattacks (Jones & Ashford, 2019). This incident caused major disruptions in healthcare, demonstrating the importance of implementing robust security measures in SIKE.

In addition, this research was also inspired by the need to develop a better framework for protecting health data. Many developed countries have started to develop and implement strict data security policies to protect health information, such as the General Data Protection Regulation (GDPR) in Europe. In Indonesia, the adoption of similar policies can

help improve patient data protection and prevent harmful data leakage incidents (Lee, 2019).

In this context, this study aims to analyze existing vulnerabilities in SIKE in Indonesia, identify potential threats, and assess the effectiveness of data protection mechanisms that have been implemented. The data analysis techniques used include a literature review, case studies at several hospitals, and interviews with information security experts. The results of the research are expected to provide a clearer picture of the status of data security in SIKE in Indonesia and provide practical recommendations for SIKE managers to improve data security.

The main contribution of this research is to provide insights and recommendations that can be used by hospital managers and policy makers to improve data security in SIKE. This research is also expected to encourage further research in the field of cybersecurity in the health sector, as well as inspire the development of better data security policies and practices in Indonesia.

2. Theoretical Basis

Research on Data Security in Electronic Health Information Systems (EHIS) requires an in-depth understanding of various basic concepts of information security. This theoretical foundation will explain some key concepts relevant to data security, including the definition of data security, key aspects to consider, threats and risks, and the importance of implementing security technologies in electronic health systems.

Definition of Data Security

Data security is defined as an effort to protect information from threats that can cause loss or violation of the integrity, confidentiality, and availability of that information. According to Stallings and Brown (2021), data security is "the protection of data from threats that lead to information loss or damage." In the context of Electronic Health Information Systems (EHIS), data security aims to protect sensitive patient medical information from unauthorized access, unexpected data changes or data loss.

Key Aspects of Data Security

Data security is generally based on three basic principles known as the CIA Triad: Confidentiality, Integrity, and Availability. These three principles form the main basis for the design and implementation of information security systems.

a. Confidentiality: Ensuring that information can only be accessed by authorized parties. In SIKE, confidentiality is very important because patient medical data must be protected from access by unauthorized parties. Whitman and Mattord (2020) emphasize that maintaining confidentiality in health information systems is a top priority as breaches can lead to the leakage of sensitive information.
b. Integrity: Ensuring that data remains intact and unaltered without authorization. Integrity is essential to ensure that medical information remains accurate and

complete. If patient data is altered by an unauthorized party, this could compromise patient care and diagnosis (Stallings & Brown, 2021).

c. Availability: Ensuring that information can be accessed by authorized parties when needed. According to Kim and Solomon (2018), the availability of a health information system is essential so that medical data can be accessed when needed by doctors or other healthcare providers.

Data Security Threats and Risks

In this study, threats and risks to data security were identified as the main factors affecting the implementation of security in SIKE. According to Oltsik (2020), threats to data security can come from a variety of sources, including cyberattacks, system failures and human error. Threats such as cyberattacks are of great concern in health information systems due to the large amount of data exchanged electronically, which is often a target for hackers.

These threats can include malware attacks, ransomware, phishing and unauthorized access. Oltsik (2020) emphasizes that without proper protection, electronic health systems become easy targets for cyberattackers because the data being managed is of high value. Human error is also a major threat, where negligence in accessing or handling data can lead to leaks or security breaches.

Data Security Technologies and Tools

Data security technologies play an important role in maintaining the confidentiality, integrity, and availability of information. Encryption systems, multifactor authentication (MFA), firewalls, and intrusion detection systems (IDS) are some of the most common technology tools used to protect data in health information systems.

a. Encryption is a method used to protect data during transmission or storage. According to Kim and Solomon (2018), encryption helps ensure that data transmitted between systems remains protected, so that only those with the encryption key can access the information. The use of encryption on medical data is essential to prevent information theft.
b. Multifactor authentication (MFA) adds a layer of security by requiring users to provide more than one identity verification method before they can access the system. Whitman and Mattord (2020) state that the use of MFA can reduce the risk of unauthorized access by ensuring that only authorized users can log in to the health information system.
c. Firewalls and intrusion detection systems (IDS) are also important in monitoring network traffic and preventing outside attacks. Humphreys (2018) emphasizes that firewalls and IDS help keep hospital networks secure from attacks coming from outside.

Information Security Standards

Health information systems must also comply with various information security standards. International standards such as ISO/IEC 27001 are the main reference in designing and implementing information security policies in various organizations, including hospitals and health institutions. Humphreys (2018) explains that the ISO/IEC 27001 standard provides guidelines for designing a comprehensive and sustainable information security management system.

Adi Ahmad et al (2024), Cyber security is a discipline that focuses on securing computer systems and networks from threats arising from cyberspace. This concept is closely related to protecting data, information and networks that can be disrupted or infiltrated by cyber attacks. Research in the field of cybersecurity involves identifying and mitigating risks, monitoring security threats, and developing effective security policies and procedures.

3. Research Methodology

The purpose of this study was to evaluate the level of data security present in electronic health information systems (EHIS) used in Indonesian hospitals. This study conducted a survey using quantitative and qualitative approaches. In this study, data was collected through questionnaires, interviews, and analysis of documents relating to data security policies.

Research Objectives

This research aimed to examine the level of data security applied to SIKE, find existing security issues, and provide suggestions for improvement. To get a representative overview, the survey method allows data collection from many respondents.

Research Methodology

a. Quantitative
   Questionnaires are used to collect numerical data from medical personnel and hospital IT staff. This data will be statistically analyzed to find patterns and correlations between variables and the level of security protocol implementation.
b. Qualitative
   Conduct interviews and document analysis to gain an in-depth understanding of data security policies, staff training, and data leakage incidents. This method enhances the understanding of the context and basis of the quantitative findings.

Surveys and Questionnaires

Structured questionnaires allow for consistent and quantifiable data collection, while in-depth interviews provide details and particulars that cannot be achieved through questionnaires alone.

Data Analysis

Quantitative and qualitative data were analyzed using descriptive and inferential statistics to provide an overview of the level of SIKE data security. Key themes and insights into

security policies and practices were identified through coding techniques and thematic analysis.

Supporting Theory

Information security theories and standards such as ISO 27001 and NIST assisted the quantitative and qualitative survey methods, as both require an evaluation of how existing security controls are implemented and functioning.

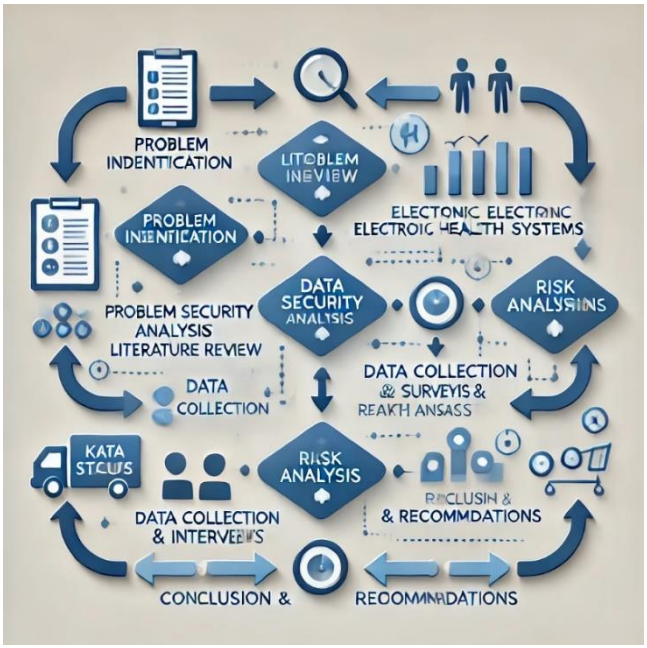

Figure 1. Research Methodology

From the picture of the research methodology, the method used is survey-based research. This can be seen from the stages that include data collection through surveys and interviews, followed by data analysis using statistical methods and risk assessment. This method relies on data collected directly from respondents to analyze data security in Electronic Health Information Systems. In addition, this approach also emphasizes on literature review and analysis of findings to produce conclusions and recommendations.

4. Results and Discussion

Research Results

This research aims to analyze data security in Electronic Health Information Systems (EHIS) by identifying threats, evaluating security levels, and providing recommendations for improvement. Data was collected through surveys, in-depth interviews, and document analysis of security policies from several large hospitals. The results showed some important findings as follows:

1. Data Security Awareness Level
    a. From the survey conducted, it was found that about 70% of the respondents realized the importance of data security but lacked understanding of the techniques and best practices to protect the data.
    b. Only 45% of the medical personnel have received formal data security training.
2. Data Security Policy Implementation
    a. Analysis of policy documents shows that although 85% of hospitals have a data security policy, the implementation of the policy varies. Some hospitals have not fully complied with international standards such as ISO/IEC 27001.
    b. Data encryption policies are only implemented by 60% of the surveyed hospitals.
3. Data Security Threats and Incidents
    a. From the in-depth interviews, it was found that cyberattacks and human error are the two biggest threats. 65% of respondents reported having experienced a data security incident in the last two years.
    b. The most common types of incidents were unauthorized access (40%) and malware attacks (30%).
4. Use of Security Technology
    a. Most hospitals use firewalls and intrusion detection systems (IDS), but only 50% use end-to-end encryption for patient data.
    b. The use of multifactor authentication (MFA) is only implemented by 35% of hospitals.

Table 1. Research Results on Data Security in SIKE

Research Aspects	Key Findings
Data Security Awareness Level	70% of respondents are aware of the importance of data security, 45% have received formal training.
Security Policy Implementation	85% of hospitals have policies in place, only 60% have implemented data encryption.
Security Threats and Incidents	65% of hospitals have experienced a data security incident; unauthorized access (40%), malware attack (30%).
Use of Security Technology	50% use end-to-end encryption, 35% use multifactor authentication (MFA).

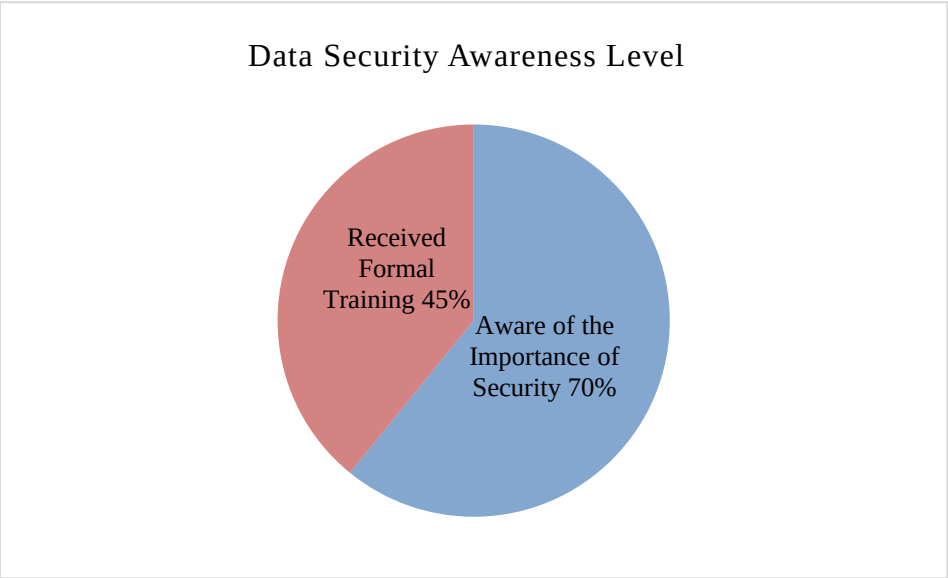

Figure 2. Graph of Data Security Awareness Level

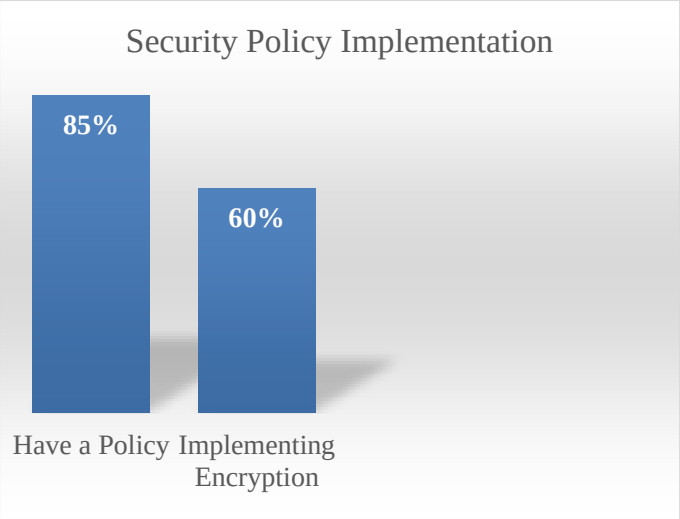

Figure 3. Security Policy Implementation

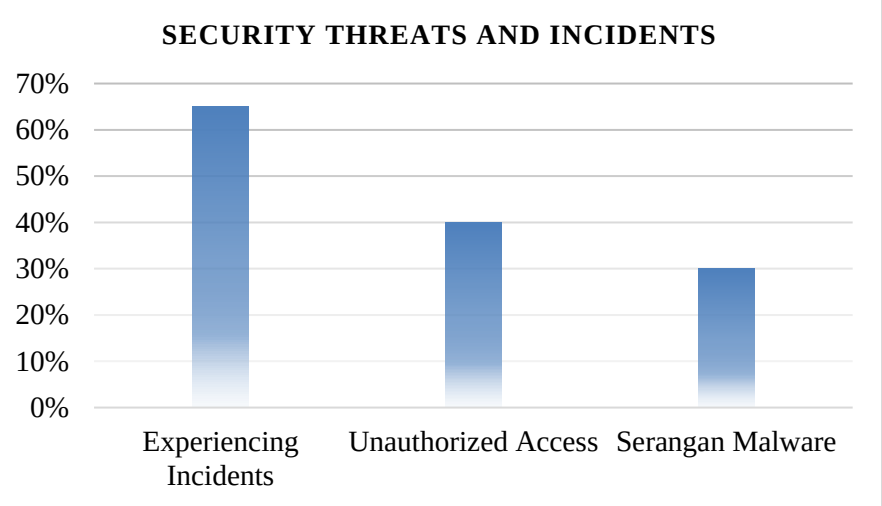

Figure 4. Security Threats and Incidents

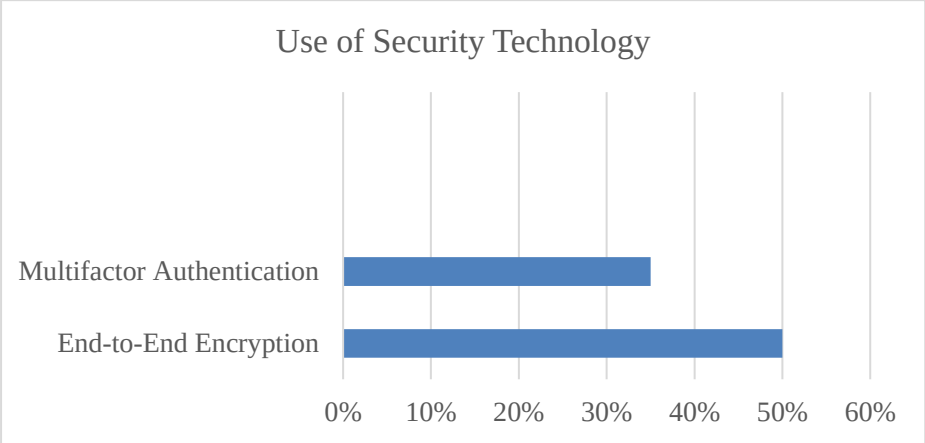

Figure 5. Use of Security Technology

Discussion

This study shows that while people know how important data security is, practices are still suboptimal. Adequate knowledge and training are not matched by a high level of awareness. This is in line with Gordon and Fairhall's (2018) research that emphasizes the importance of security training and awareness among medical personnel to prevent security accidents. There is a need for stricter standardization as various data security policies have been implemented. Humphreys (2018) states that the ISO/IEC 27001 standard has the ability to offer assistance to companies as they build efficient information security management systems. However, the surveyed hospitals are still not implementing this standard equally.

Cyberattacks and human error are the biggest threats identified in this study. Oltsik (2020) states that if these threats are to be mitigated, a comprehensive risk management strategy is required. Training and security awareness programs need to be improved as human error is often caused by a lack of training. Security technologies such as firewalls, intrusion detection, and encryption are still not optimally used. However, only 50% of hospitals use end-to-end encryption, indicating that wider adoption of security technologies and consistent implementation are needed, as stated by Kim and Solomon (2018). The fact that multifactor authentication (MFA) can improve data security by ensuring that only authorized users can access sensitive information is something that has not been widely used. Whitman and Mattord (2020) emphasize that MFA is one of the important methods to maintain data confidentiality and integrity.

Overall, this research shows that although there is increased awareness and some good first steps in protecting data, there is still much to be done to achieve optimal data security in SIKE. Some recommendations for improving data security in a healthcare setting include stricter policy implementation, more frequent training, and wider use of security technologies.

5. Conclusion

The research shows that while awareness of the importance of data security is high, it has not been matched by sufficient implementation and training. Cyberattacks and human error are the main threats that require special attention. Training programs and increased security awareness are needed. Better data protection for Electronic Health Information Systems requires improved policy standards and the use of security technologies such as encryption and multifactor authentication.The purpose of this study was to assess and analyze the data security of Indonesia's Electronic Health Information System (EHIS). The research identified various vulnerable areas, potential threats, and successes of data security systems that have been implemented so far through a thorough literature review, interviews with information security experts, and case studies of several hospitals.

The study shows that, despite the efforts made to improve data security, there are still many gaps and vulnerabilities that can be exploited by irresponsible parties. Cyberattacks, data breaches and illegal access are the main threats. Moreover, this study found that taking security measures such as data encryption, multi-factor authentication, and regular audits can significantly reduce these threats. However, there are some limitations in this study, such as the limited sample size of the case study and the difficulty in obtaining internal hospital data. Nevertheless, this research does a significant job by providing practical suggestions for SIKE administrators to improve their data security. In addition, the findings of this research can be used as a basis for future studies in this area. Overall, this study shows that Indonesia needs to develop better data security protocols for SIKE. It also emphasizes how important it is for health professionals to be trained continuously on best practices in data security.

Reference

Adi Ahmad, Riyan Maulana, & Muhammad Yassir. (2024). Cybersecurity Challenges In The Era Of Digital Transformation A Comprehensive Analysis Of Information Systems. *Journal Informatic, Education and Management (JIEM)*, *6*(1), 7-11. https://doi.org/10.61992/jiem.v6i1.57

Adi Ahmad, Maulana, R., & Akmal, K. (2024). Data Privacy and Security in the Age of IoT A Comprehensive Study on Information System Vulnerabilities. *Journal Informatic, Education and Management (JIEM)*, *6*(2), 1-7. https://doi.org/10.61992/jiem.v6i2.78

Gordon, W. J., & Fairhall, A. (2018). Security and privacy of patient information and electronic health records. *Journal of the American Medical Informatics Association, 25*(3), 408-412.

Humphreys, E. (2018). Information security management standards: Compliance, governance and risk management. *Information Security Journal: A Global Perspective, 27*(2), 52-61.

Jones, T., & Ashford, R. (2019). Cybersecurity threats in healthcare: An urgent call for action. *Journal of Healthcare Information Management, 34*(3), 112-118.

Kementerian Kesehatan Republik Indonesia. (2021). Laporan keamanan data kesehatan di Indonesia. Jakarta: Kementerian Kesehatan RI.

Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning.

Lee, A. (2019). Global perspectives on health data breaches. *International Journal of Medical Informatics, 127*, 57-63.

Miller, K., Smith, L., & Anderson, J. (2020). Data security in electronic health records. *Healthcare Management Review, 45*(4), 231-239.

Oltsik, J. (2020). The state of cybersecurity. *Journal of Cybersecurity*, *6*(1), 1-12.

Smith, J. (2020). Protecting patient information in the digital age. *Healthcare Security Insights*, *22*(2), 45-53.

Stallings, W., & Brown, L. (2021). *Computer Security: Principles and Practice* (5th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2020). *Principles of Information Security* (6th ed.). Cengage Learning.