Guarding the Digital Health Data as Front Gate: Strengthening Healthcare Data Security in Indonesian Smart Cities

Juan Anthonio SALAS,
Department of Information Engineering, Kun Shan University, Taiwan
s110003476@g.ksu.edu.tw

Muhammad IQBAL,
Department of Political Science, National Cheng Kung University, Taiwan
u18097019@ncku.edu.tw

Lakuntara PALLAHIDU,
Department of Information Engineering, Kun Shan University, Taiwan
s110003446@g.ksu.edu.tw

Abstract
In this modern world, data has become an important part of our daily lives, permeating every aspect of society. It serves as a gateway to knowledge, giving us access to important information that shapes our understanding of the world. Objectives In the healthcare field, data is becoming increasingly important as it empowers medical professionals to provide optimal care and improve patient outcomes. Prior Work However, Indonesia's fragmented digital health landscape presents many challenges, with a myriad of diverse and abundant health applications and databases. The proliferation of these systems creates vulnerabilities, leaving patient information vulnerable to attacks and cyber breaches. Approach To solve this problem, this research paper proposes implementing a centralized health data security system. Under this system, each hospital will have a designated data door, combining various data sources into a unified platform. This consolidation allows the establishment of robust, multi-layered security measures that can effectively protect patient information from unauthorized access and breach. Result This paper presents a comprehensive framework for implementing these centralized data systems, addressing the potential benefits and challenges associated with their adoption. Implications By adopting a centralized data system, smart cities in Indonesia can significantly improve the confidentiality, integrity, and availability of digital health data. This proactive approach not only strengthens data security but also increases the efficiency and effectiveness of managing data security protocols. Implementation of such a system is an important step towards ensuring the protection of sensitive healthcare information, fostering trust among patients, healthcare providers and stakeholders. Value The successful implementation of a centralized health data security system has the potential to revolutionize healthcare delivery in Indonesian smart cities. It enables better patient care, increased data privacy, and improved healthcare outcomes. By strengthening data security and promoting trust, this initiative acts as a front gate to guard the digital health data, ensuring its integrity and protecting patient privacy in Indonesian smart cities.

Keywords: Centralized Systems, Data Protection Measures, Security Protection, Data Security Framework.

1. Introduction
In today's digital age, data plays an increasingly vital role in our lives, particularly in the healthcare industry. As healthcare providers rely on digital platforms to store, process, and manage patient information, ensuring the security and privacy of healthcare data has become a critical concern. This issue is particularly relevant in Indonesian smart cities, where the proliferation of diverse digital health applications and databases presents challenges to safeguarding the confidentiality and integrity of patient data.

Numerous studies have underscored the urgent need to strengthen healthcare data security in Indonesian smart cities. For example, some study [1] found that the fragmented digital

health landscape in Indonesia creates vulnerabilities that leave patient information vulnerable to attacks and cyber breaches.

To address these challenges and fortify the security of digital health data in Indonesian smart cities, this research paper advocates the implementation of a centralized health data security system. The proposed approach aligns with the widely recognized National Institute of Standards and Technology (NIST) Cybersecurity Framework, which provides a comprehensive framework for managing and mitigating cybersecurity risks.

The NIST Framework offers a systematic and structured methodology for organizations to assess and enhance their cybersecurity [2]. By leveraging this framework, the proposed centralized health data security system seeks to consolidate disparate data sources from multiple hospitals into a unified platform. This consolidation enables the establishment of robust, multi-layered security measures that address the vulnerabilities stemming from fragmented systems, safeguarding patient information from unauthorized access and breaches.

However, implementing a centralized approach to healthcare data security also presents challenges. Ensuring data integration, interoperability, scalability, and stakeholder collaboration are crucial aspects that require careful consideration and resolution.

By strengthening healthcare data security in Indonesian smart cities, the proposed centralized health data security system can significantly enhance the confidentiality, integrity, and availability of digital health data. This will foster trust among patients, healthcare providers, and stakeholders, ultimately contributing to improved healthcare delivery and outcomes.

Building upon the existing research, this paper proposes a centralized health data security system, like the concept of Satu Sehat. This system envisions each hospital having one data door, consolidating various data sources into a single platform. The paper presents a framework for implementing the centralized data system, highlighting its design and functionality. Additionally, the potential benefits and challenges associated with this approach are discussed. By adopting a centralized data system, Indonesian smart cities can achieve not only improved data security but also greater efficiency and effectiveness in managing healthcare data.

2. Literature Review

2.1. Introduction to Healthcare Data Security

Healthcare data security has become an important concern because large amounts of sensitive information are stored and transmitted electronically. The protection and integrity of healthcare data is critical due to the increasing reliance on digital platforms and technology in the healthcare industry [3]. Healthcare data security refers to measures and practices implemented to protect patient information, electronic health records (EHR), and other sensitive data from unauthorized access, breach, and misuse.

The significance of healthcare data security cannot be overstated. Patient data contains highly sensitive information, including personal details, medical history, diagnosis, treatment plan and financial data. Any unauthorized access to or breach of this information can result in severe consequences such as identity theft, fraud, damage to reputation and impaired patient care. Ensuring strong safety measures is critical to maintaining trust between patients and healthcare. Patients should be assured that their personal information will be treated in the strictest confidence and that their right to privacy will be respected.

Compliance with legal and regulatory requirements is another important aspect of healthcare data security. Many countries have enacted data protection laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, to protect patient information and maintain privacy standards. Complying with these regulations is very important for healthcare organizations to avoid legal repercussions and financial penalties [4].

In addition, healthcare data security has a direct impact on the overall quality of patient care. Access to accurate and secure patient data enables healthcare professionals to make informed decisions, collaborate effectively, and provide personalized and timely care. This facilitates the smooth exchange of information among different healthcare entities, resulting in better care coordination, reduced medical errors and better patient outcomes.

In summary, healthcare data security plays a critical role in protecting sensitive information, building trust between patients and healthcare providers, complying with legal requirements, and ultimately enhancing the delivery of high-quality, patient-centric care. Strong security measures, guided by industry standards and best practices, are critical to protecting healthcare data from unauthorized access and breach.

2.2. Key Challenges in Healthcare Data Security

Healthcare data security in Indonesia's smart cities faces several major challenges. First, the fragmented digital healthcare landscape prevalent in these cities contributes to interoperability issues and a lack of standard systems [5], [6]. This fragmentation makes it difficult to seamlessly integrate and share data, hindering the establishment of comprehensive security measures. Second, privacy and security risks raise significant concerns in managing healthcare data [7]. Patient privacy must be protected, and the risks of unauthorized access and breach need to be effectively mitigated. Healthcare data is vulnerable to cybersecurity threats and attacks, which have the potential to have severe consequences [8], [9]. Cyber-attacks targeting healthcare data have increased, emphasizing the need for strong security measures to secure sensitive information. Another challenge is the Effective control and robust data protection are critical challenges that must be carefully addressed during the guarding of data [10].

To address this challenge and strengthen health data security in Indonesia's smart cities, it is imperative to establish strong measures to safeguard digital health data as the front gate. Implementing a centralized health data security system can be a good solution. By consolidating multiple data sources into one unified platform, this approach enables the establishment of effective and efficient multi-layered security measures that protect patient

information from unauthorized access and data breaches. A centralized system offers advantages such as increased data confidentiality, increased data integrity, and increased availability [11]. This can streamline data management processes, facilitate standardized security protocols, and encourage collaboration between healthcare providers and stakeholders. Implementing such a system is an important step towards ensuring the protection of sensitive healthcare information and building trust in the healthcare ecosystem.

2.3. Cybersecurity Threats and Attacks

The healthcare industry is increasingly becoming the target of multiple cybersecurity threats and attacks, which pose significant risks to the confidentiality, integrity, and availability of patient and hospital data and care systems. Malware and ransomware attacks have become prevalent, exploiting vulnerabilities in healthcare systems and wreaking havoc on patient records. For example, the increasing threat of ransomware in the Internet of Things (IoT) domain, including healthcare devices and systems [12]. They discussed the challenges of ransomware attacks, which can encrypt critical healthcare data and demanded a ransom for its rollout. The importance of detecting malware using deep learning techniques, such as long short-term memory, to improve the security of healthcare systems [13].

Insider threats pose another important challenge to healthcare data security. the risks associated with insiders having authorized access to sensitive healthcare information [14]. These people may intentionally or unintentionally engage in activities that compromise data security. In addition, data breaches due to unauthorized access and incidents of data leakage are the main concerns that must be watched out for. Additional damage that deep learning-based malware detection systems can cause to adversary attacks [15]. Their research highlights the need for strong defenses to minimize the impact of insider threats on the security of healthcare data.

Social engineering and phishing attacks continue to be a significant threat to healthcare cybersecurity. The detection of spear-phishing emails using transformer-based text classification [16]. Social engineering techniques, including phishing attacks, exploit human vulnerabilities to trick individuals into divulging sensitive information or granting unauthorized access. The importance of addressing security, privacy, and trust in the Internet of Things (IoT) domain [17]. Their work highlights the need for comprehensive action, including employee awareness programs and robust security protocols, to counter social engineering attacks and protect healthcare data.

To ensure the security of healthcare data in Indonesia's smart cities, it is imperative to develop an effective strategy to mitigate this cybersecurity threat. Organizations or governments should invest in advanced threat detection and prevention systems, conduct regular training and awareness programs for employees to recognize and respond to potential threats, and implement robust access control mechanisms to limit unauthorized access. Additionally, collaboration between hospitals, healthcare institutions, government agencies and cybersecurity experts are needed to share best practices and respond effectively to emerging threats.

By understanding and addressing the challenges posed by malware and ransomware attacks, insider threats, as well as social engineering and phishing attacks, smart cities in Indonesia can strengthen their healthcare data security infrastructure, increase patient confidence, and ensure the confidentiality and integrity of health care information. sensitive.

3. Methodology

The methodology used in this research comes from the National Institute of Standards and Technology Cybersecurity Framework (NIST Framework). The NIST Framework serves as the basic structure to guide the development and implementation of research methodologies. It provides a systematic and comprehensive approach to managing cybersecurity risks, specifically adapted to the context of healthcare data security in Indonesia's smart cities.

Fig. 1. NIST Framework

Adapting to the NIST Framework, the methodology covers the core functions of Identify, Protect, Detect, Respond, and Recover. The Identification Phase involves identifying specific healthcare data security risks and vulnerabilities that exist within the fragmented digital health landscape of Indonesia's smart cities. The Protect phase focuses on implementing appropriate security measures to protect patient information and ensure data confidentiality, integrity, and availability. The Detect phase emphasizes establishing mechanisms for proactive monitoring and detection of potential cyber threats and breaches. The Response phase requires the development of a response strategy and incident management protocol to address and mitigate cybersecurity incidents promptly. Finally, the Recovery phase focuses on establishing data recovery procedures and plans in the event of a breach or breach of security.

By leveraging the NIST Framework, this study ensures a structured and comprehensive methodology that addresses the unique challenges and requirements of healthcare data security in smart cities in Indonesia. This provides a solid foundation for systematically managing cybersecurity risks, protecting patient information, and improving the overall data security posture in Indonesia's healthcare system.

4. Results and Analysis

4.1. Important to Guard the Data

Confidentiality and privacy protection are critical in the healthcare sector, where the security of patient data is paramount. Unauthorized access or breach can lead to severe consequences, including compromised patient privacy and potential misuse of sensitive information. To overcome this problem, researchers have proposed various solutions. For example, a privacy-protecting data collection framework for the medical Internet of Things (IoT) in smart healthcare, using techniques such as encryption to protect patient data [18]. Transmission can use blockchain and homomorphic encryption to maintain the privacy of healthcare data, ensuring secure and confidential storage the data [19]. This approach contributes to maintaining patient confidentiality, protecting against unauthorized access, and instilling trust in the healthcare system.

Mitigating data breaches and cybersecurity threats is critical to protecting healthcare data. The integration of advanced technologies, such as blockchain and smart contracts, has shown promise in increasing the security of healthcare systems. A framework utilizing blockchain and smart contracts to guarantee the security and integrity of e-healthcare systems while prioritizing trustworthiness and privacy [20]. By leveraging a combination of cryptography and blockchain techniques, electronic medical records can be safeguarded, mitigating the potential risks linked to unauthorized alterations or destruction [21]. This approach not only mitigates cybersecurity threats but also provides a secure and immutable environment for healthcare data, enhancing overall data protection and system integrity.

Ensuring the integrity and availability of data is very important for the health care system in patients, because accurate and accessible data is essential for making good decisions so that patient care is very effective. A comprehensive survey was conducted to explore data integrity and security concerns in cloud-based healthcare, addressing the issues surrounding the topic [22]. They highlight the challenges associated with maintaining data integrity in cloud environments and discuss strategies for mitigating these risks. Dynamic data replication techniques were proposed to guarantee data availability in healthcare cloud systems, thereby decreasing the potential for data loss or unavailability [23]. Furthermore, a review was carried out to examine data storage and security in cloud healthcare systems, exploring various approaches and technologies for the effective protection and management of healthcare data [24]. This contributes to maintaining the accuracy, accessibility, and availability of data, thus facilitating efficient health service delivery and decision-making processes so that the steps taken can be appropriate, effective, and efficient.

Implementing an effective data security system is essential to safeguard healthcare data in Indonesia's smart cities. The concept of a centralized health data security system, often referred to as a "one-stop-shop", offers a promising approach. This system, as envisioned by the Satu Sehat concept, consolidates multiple data sources into a single platform, enabling the implementation of strong security measures. By adopting a unified platform, healthcare providers can create layered security protocols, combining encryption, access control, and authentication mechanisms to protect patient data.

One-stop systems address some of the key challenges in healthcare data security. It maps out the risks associated with a fragmented digital health landscape, ensuring standardized security measures across healthcare institutions. In addition, it strengthens privacy and confidentiality protection by mitigating vulnerabilities stemming from diverse and abundant health applications and databases. Consolidating data sources into a unified platform improves data integrity, minimizing the risk of data tampering or unauthorized modification.

The implementation of a centralized health data security system not only strengthens data security but also makes data management processes more precise, leading to increased efficiency and effectiveness. The system facilitates seamless data integration, enabling healthcare professionals to securely access comprehensive patient information, resulting in better healthcare services and outcomes. Additionally, it fosters trust among patients, healthcare providers, and stakeholders, promoting the confident exchange of sensitive healthcare information.

Safeguarding health service data in smart cities in Indonesia is very important to protect patient privacy, prevent unauthorized access, and mitigate cyber security threats so that safe, effective, and efficient data is created. The concept of a centralized health data security system, exemplified by a one-stop system, offers a more comprehensive approach to addressing these challenges. By adopting this system, healthcare institutions can improve data security, ensure data integrity and availability, and improve overall healthcare delivery. Effective healthcare data security through the implementation of a one-stop system is a significant step towards a safe and efficient healthcare system in smart cities in Indonesia.

4.2. NIST Framework Implementation and the Effectiveness of Centralized System

4.2.1. Identification

By implementing a one-stop-shop system, which combines multiple data sources into a unified platform, healthcare organizations can identify and understand their data landscape in a timely, efficient, and effective manner. The centralized nature of the one-stop system aids in the identification process by providing a comprehensive view of the healthcare data ecosystem, enabling healthcare organizations to prioritize security measures and allocate resources more efficiently and effectively.

4.2.2. Protect

This protection function focuses on implementing measures to protect healthcare data from unauthorized access, data breaches, and cyber threats. One-stop systems enhance healthcare data protection by implementing strong access controls, strict encryption mechanisms, and authentication protocols. By consolidating data sources into a unified platform, the one-stop system enables healthcare organizations to establish standard security measures across institutions. This approach ensures consistent protection of sensitive patient data and reduces the potential vulnerabilities associated with diverse and fragmented data sources.

4.2.3. Detect

We analyze the application of the NIST Framework's "Detect" functionality in healthcare organizations and the role of one-stop systems in enhancing detection capabilities. This function involves continuous monitoring, intrusion detection mechanisms, and real-time alerts to identify potential cybersecurity incidents or breaches. The one-stop system facilitates centralized monitoring and detection by providing a comprehensive view of data activity across multiple healthcare sources. This centralized approach enhances the ability to detect anomalies, unauthorized access attempts, or suspicious behavior, enabling healthcare organizations to respond quickly in case of erroneous data, and mitigate potential security threats to patient and hospital data.

4.2.4. Respond

In this section, we discuss the "Respond" function of the NIST Framework and the role of a one-stop shop in responding to healthcare data security incidents. This function focuses on creating an incident response process to address and mitigate the impact of a data breach or unauthorized access. One-stop systems streamline incident response by consolidating data sources, facilitating efficient coordination among stakeholders, and enabling fast action. With a unified platform, healthcare organizations can respond effectively to security incidents, minimize the potential for data loss, and ensure a coordinated and timely incident management process.

4.2.5. Restore

We evaluate the adoption of the NIST Framework's "Restore" function and the one-stop-shop system's contribution to data recovery and system recovery. This function involves establishing strategies and procedures for recovering healthcare data and recovering systems after a cybersecurity incident. One-stop systems help data recovery by centralizing backup and disaster recovery mechanisms. By combining data sources, a one-stop system ensures the availability and integrity of healthcare data, facilitating a faster recovery process. This centralized approach minimizes disruption to patient care and can ensure patients have precise and accurate data.

4.3. Implementation of the One-Door System in Indonesian Smart Cities

Implementing a one-stop system in smart cities in Indonesia has proven to be an effective way to protect health data and improve data security. The "One Health Plan" initiated by the Indonesian government is an important example of the successful implementation of the "One School System". By consolidating healthcare data from multiple institutions into a centralized platform, the one-stop system ensures standardized security measures and mitigates vulnerabilities associated with fragmented digital health applications and databases. This approach, aligned with the NIST framework, incorporates key elements of the "response" phase by implementing strong security protocols such as encryption, access control, and authentication mechanisms. With a one-stop system, healthcare providers can effectively respond to potential breaches and unauthorized access, protecting patient data from malicious threats. The implementation of the one-stop system not only improves data security, but also facilitates the seamless integration of data, making the data management process more accurate and efficient. This in turn improves the overall efficiency of healthcare delivery and supports data-driven decision-making in smart cities in Indonesia.

4.3.1. One-Door System and Initiation from Indonesian Government

The Initiation of the One Stop System in managing health data is a significant step to improve data security and streamline data access in smart cities in Indonesia. The concept of a centralized data system, often referred to as a "one-stop shop", emerged in response to the challenges posed by the country's fragmented digital health landscape. The Indonesian government recognizes the need to address the vulnerabilities associated with diverse and abundant health applications and databases, which place patient information at risk of unauthorized access and breach. To address this challenge, the government is introducing a "Satu Sehat" as part of a larger effort to strengthen health data security and improve the overall quality of health services. This aims to consolidate multiple data sources from different healthcare institutions into a unified platform, creating a single entry point or "one door" for accessing and managing healthcare data. By establishing this centralized system, governments are trying to standardize security measures, improve data protection, and ensure better interoperability between healthcare providers, ultimately benefiting both patients and healthcare professionals.

4.3.2. Benefits and Outcomes

The implementation of the One Stop System in Indonesia's smart cities brings many benefits and positive outcomes for both patients and hospitals. One of the main goals of this is to prioritize patient well-being and satisfaction. By combining healthcare data into a single platform, the One Stop System enables healthcare providers to quickly access comprehensive and up-to-date patient information. This leads to better coordination of care, as healthcare professionals have a thorough view of a patient's medical history, medications, allergies, and treatment plan. As a result, patient outcomes are improved, with reduced medical errors, greater treatment accuracy and better decision making.

In addition, the One Stop System facilitates efficient data exchange and interoperability between hospitals so as to create a secure system. The centralized platform eliminates the need for complex data transfers between different institutions, saving time and resources. This efficient sharing of data promotes collaboration and improves communication among healthcare providers, leading to a more coordinated and integrated care delivery.

For hospitals, the One Stop System provides a real advantage. It simplifies data management and reduces administrative burden by providing a unified interface for data access, retrieval, and storage. This increases operational efficiency, enabling hospitals to allocate resources more effectively and focus on delivering high-quality care. In addition, the centralized system improves data security and privacy through standard security measures, reducing the risk of data breaches and unauthorized access. This instills confidence in patients and helps hospitals comply with regulatory requirements, maintain their reputation and ensure compliance with data protection laws.

Overall, the One Stop System resulted in significant benefits for both patients and hospitals. By promoting seamless data exchange, improving care coordination, and improving data security, this centralized approach improves healthcare quality, optimizes resource utilization, and ultimately contributes to better patient outcomes and satisfaction.

4.3.3. Challenges and Lessons Learned

The implementation of the One Stop System in Indonesia's smart cities is not without its challenges. One of the main challenges faced is the integration of various data sources and systems from various health institutions. The process of consolidating and standardizing complex data formats, structures and protocols requires extensive coordination and collaboration among stakeholders. Additionally, ensuring interoperability between disparate electronic health record (EHR) systems and legacy applications creates technical complexities that need to be addressed.

Another challenge is the need to address concerns about data privacy and security. By consolidating healthcare data into a single platform, ensuring adequate protection against unauthorized access, data breaches and cyberthreats is paramount. Strong security measures, including encryption, access control, and authentication mechanisms, must be implemented to protect patient information and maintain compliance with data protection regulations.

Lessons from implementing the One Stop System provide valuable insights for future projects. First, effective stakeholder engagement and collaboration is critical to success. Engaging with all relevant parties, including healthcare providers, IT professionals, policy makers and patients, fosters a sense of ownership, encourages knowledge sharing and facilitates the alignment of goals and objectives.

Second, training and continuing education are essential for healthcare professionals and staff. Introduction of centralized systems requires familiarity with new technologies, processes, and security protocols. Investing in training programs and workshops ensures that personnel are equipped with the necessary skills to navigate and use the One Stop System effectively.

Finally, continuous monitoring and evaluation is essential to identify and address any system gaps or vulnerabilities. Regular assessments of data quality, system performance and security measures help identify areas for improvement and prompt and timely corrective action. Additionally, seeking feedback from end users, such as patients and healthcare providers, provides valuable insights to refine and enhance the functionality and user experience of One Stop System.

By addressing these challenges and applying lessons learned, the One Stop System can continue to grow and adapt to the changing needs of the healthcare landscape in Indonesia's smart cities, ensuring sustainable benefits for patients, healthcare providers, and the healthcare ecosystem.

4.4. Future Works

The implementation of the One Stop System has become a solid foundation for maintaining health data in Indonesia's smart cities. However, there are still potential areas for further development and improvement. First, expanding the scope of the One Stop System to include other healthcare stakeholders, such as pharmacies, diagnostic centers and insurance providers, can contribute to a more comprehensive and interconnected healthcare

ecosystem. This will facilitate complex data exchange and improve continuity of care across multiple healthcare settings.

In addition, taking advantage of new technologies can enhance the capabilities of the One Stop System. Exploring the integration of artificial intelligence (AI) and machine learning algorithms can help identify patterns, detect anomalies and provide predictive insights to improve patient care and early disease detection. Additionally, the use of blockchain technology can increase the security and transparency of healthcare data by enabling tamper-resistant and auditable records.

To ensure the long-term sustainability and effectiveness of the One Stop System, it is important to establish a strong governance and regulatory framework. Clear guidelines and policies should be developed to address data privacy, security and ethical considerations. Collaboration with regulatory agencies and relevant stakeholders can facilitate the development of standardized protocols and guidelines for data sharing, privacy protection and interoperability.

In addition, ongoing research and development efforts should focus on improving the usability and user experience of the One Stop System. User-centric design principles must be applied to ensure that the system is intuitive, easy to navigate, and accessible to all users, including healthcare professionals and patients with varying levels of digital literacy.

Finally, cultivating a culture of data-driven decision-making and innovation is critical. Encouraging data sharing for research purposes while ensuring privacy protection can lead to valuable insights and advances in healthcare. Collaboration with academic institutions and research organizations can drive further innovation and promote evidence-based practice in healthcare delivery.

By focusing on potential areas for further development and implementing the recommendations mentioned above, the One Stop System can continue to develop as a strong and secure platform for maintaining health service data in smart cities in Indonesia. This will ultimately contribute to improving patient outcomes, enhancing healthcare delivery, and advancing the healthcare ecosystem.

5. Conclusions

The increasing reliance on data in our modern world makes healthcare data security a priority, especially in the context of smart cities in Indonesia. Indonesia's fragmented digital healthcare landscape poses significant challenges, exposing patient information to cyber vulnerabilities and threats. To overcome this problem, the implementation of a centralized health data security system is proposed as an effective and efficient solution.

The concept of a centralized data system, exemplified by the "one door" approach, offers many advantages. By consolidating multiple data sources into a unified platform, robust and layered security measures can be created to protect patient information from unauthorized access and breach. This comprehensive framework ensures the confidentiality, integrity, and availability of digital health data.

Adopting a centralized data system in Indonesia's smart cities not only improves data security, but also improves the efficiency and effectiveness of managing data security protocols. This enables standardized security measures across healthcare institutions, reduces vulnerabilities arising from diverse healthcare applications and databases, and fosters trust among patients, healthcare providers, and stakeholders.

The successful implementation of a centralized health data security system has broad implications. This is revolutionizing healthcare delivery in Indonesia's smart cities, resulting in better patient care, increased data privacy, and better healthcare outcomes. This proactive approach acts as a front gate, safeguarding digital health data and ensuring its integrity while protecting patient privacy.

However, challenges and lessons must be considered in the process. Diverse system integration, stakeholder collaboration, and addressing privacy issues are important factors that must be addressed. Future work should focus on further developing one-stop systems and exploring potential upgrades to strengthen healthcare data security in Indonesia's smart cities.

In short, effective guarding of health data in Indonesia's smart cities requires the implementation of a centralized health data security system. This proactive approach not only protects patient information but also enhances data privacy, increases trust, and paves the way for a safe and efficient healthcare system. By prioritizing data security, smart cities in Indonesia can ensure the protection of sensitive healthcare information, leading to better healthcare outcomes and overall healthcare improvements.

References

[1] Rosadi, S. D., Suhardi, S., & Kristyan, S. A. (2021), *Data Privacy Law in the Application of Smart City in Indonesia*, Journal of Legal, Ethical and Regulatory Issues, 24(S4), 1-9.

[2] National Institute of Standards and Technology (2018, April), NIST Releases Version 1.1 of Its Popular Cybersecurity Framework [Press release], Retrieved from *https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework*

[3] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li (2017), *"Integrating blockchain for data sharing and collaboration in mobile healthcare applications,"* 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, pp. 1-5, doi: 10.1109/PIMRC.2017.8292361.

[4] AHIMA (2018), *Fundamentals of Law for Health Informatics and Information Management (3rd ed.)*, American Health Information Management Association.

[5] Hodapp, D., & Hanelt, A. (2022), *Interoperability in the era of digital innovation: An information systems research agenda*, Journal of Information Technology, 37(4), 407–427. https://doi.org/10.1177/02683962211064304

[6] Kocabas, V. (2020), *Interoperability and Standardization in Health Information Systems*, In Handbook of Research on Artificial Intelligence Techniques and Algorithms (pp. 300-312). IGI Global.

[7] Chikhaoui, E., Sarabdeen, J., & Parveen, R. (2017), *Privacy and Security Issues in the Use of Clouds in e-Health in the Kingdom of Saudi Arabia*, Communications of the IBIMA, 18.

[8] Fayans, I., Motro, Y., Rokach, L., Oren, Y., & Moran-Gilad, J. (2020), *Cyber security threats in the microbial genomics era: implications for public health*, Eurosurveillance, 25(6), 1900574.

[9] Ahmed, Y., Naqvi, S., & Josephs, M. (2019, May), *Cybersecurity metrics for enhanced protection of healthcare IT systems*, In 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT) (pp. 1-9). IEEE.
[10] Neisse, R., Steri, G., Fovino, I. N., & Baldini, G. (2015), *SecKit: A Model-based Security Toolkit for the Internet of Things*, Computers & Security, 54, 60-76. http://dx.doi.org/10.1016/j.cose.2015.06.002
[11] E. Bertino and R. Sandhu (2005), *"Database security - concepts, approaches, and challenges,"* in IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 1, pp. 2-19, doi: 10.1109/TDSC.2005.9.
[12] Thomas B. Slayton (2018), *Ransomware: The Virus Attacking the Healthcare Industry*, Journal of Legal Medicine, 38:2, 287-311, DOI: 10.1080/01947648.2018.1473186
[13] Sarker, I. H. (2021), *Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective*, SN Computer Science, 2(3), 154.
[14] Humphreys, E. (2008), *Information security management standards: Compliance, governance, and risk management*, Information security technical report, 13(4), 247-255.
[15] Huang, S., Papernot, N., Goodfellow, I., Duan, Y., & Abbeel, P. (2017), *Adversarial attacks on neural network policies*. arXiv preprint arXiv:1702.02284.
[16] Yurtseven, İ., Bagriyanik, S., & Ayvaz, S. (2021, September), *A review of spam detection in social media*, In 2021 6th International Conference on Computer Science and Engineering (UBMK) (pp. 383-388). IEEE.
[17] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015), *Security, privacy and trust in Internet of Things: The road ahead*, Computer networks, 76, 146-164.
[18] Perera, C., Barhamgi, M., Bandara, A. K., Ajmal, M., Price, B., & Nuseibeh, B. (2020), *Designing privacy-aware internet of things applications*, Information Sciences, 512, 238-257.
[19] Shrestha, R., & Kim, S. (2019), *Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities*, In *Advances in computers* (Vol. 115, pp. 293-331). Elsevier.
[20] Naveen, N., & Thippeswamy, K. (2020), *A Framework for Secure eHealth Data Privacy Preserving on Block chain with SHA-256 in Cloud Environment*,Turkish Journal of Computer and Mathematics Education (TURCOMAT), 11(3), 1118-1128.
[21] Ansari, M. F., Dash, B., Swayamsiddha, S., & Panda, G. (2023, January), *Use of Blockchain Technology to Protect Privacy in Electronic Health Records-A Review*, In 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) (pp. 144-149). IEEE.
[22] Butpheng, C., Yeh, K. H., & Xiong, H. (2020), *Security and privacy in IoT-cloud-based e-health systems—A comprehensive review*, Symmetry, 12(7), 1191.
[23] Kuo, M. H. (2011), *Opportunities and challenges of cloud computing to improve health care services*, Journal of medical Internet research, 13(3), e1867.
[24] Jee, K., & Kim, G. H. (2013), *Potentiality of big data in the medical sector: focus on how to reshape the healthcare system*, Healthcare informatics research, 19(2), 79-85.