P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105

Protection of patient data privacy on IoT devices for healthcare in the era of smart cities: a health law perspective

Yuris Tri Naili[1*], Marlia Hafny Afrilies[1], Evis Garunja[2], Purwono[3]

[1] *Department of Law, Universitas Harapan Bangsa, Indonesia*
[2] *Faculty of Political Sciences and Law, Aleksandër Moisiu University, Albania*
[3] *Department of Informatics, Universitas Harapan Bangsa, Indonesia*

*Corresponding Author: *yurist@uhb.ac.id*

Abstract

Introduction to the Problem: The Internet of Things (IoT) has enabled the use of medical devices in healthcare sector while presenting challenges in regard to the security and privacy of the patients' medical data. This article conducts a systematic literature review to evaluate the existing regulations related to the security and privacy of the patients' medical data in real-time data collection through IoT in the context of a Smart City.
Purpose/Study Objectives: This study aims to identify gaps in the existing regulations, analyze the implementation of these regulations in practice, and evaluate the impact of IoT technology on the privacy and security rights of the patients' medical information in healthcare sector.
Design/Methodology/Approach: The research employed a systematic literature review, by analyzing relevant articles, legal documents, and regulations. Data were examined from a case study of the implementation of IoT devices for healthcare in Smart Cities as well as interviews with legal experts in the field of healthcare services.
Findings: The existence of the Electronic Information and Transaction Law, Personal Data Protection Law, and the latest Health Law provides the initial regulatory foundation for ensuring the security of personal data in the integrated governance of Smart Cities, especially in telemedicine services. Implementing regulations for these laws are necessary to technically accommodate the needs for security of the patients' data, ensuring that there is no imbalance between the provisions of the laws that are enacted and their implementation in the community.
Paper Type: Research Article
Keywords: IoT; Data Security; Patients' Privacy; Healthcare Regulation; Smart City

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Introduction

In the era of rapid digital transformation, the concept of smart cities has taken the center stage, marking the technological advancements that have penetrated various sectors of human life, including healthcare services. The development of Internet of Things (IoT) technology is the primary driver behind this revolution (Karale, 2021), as it has opened up new opportunities to improve the efficiency, affordability, and quality of healthcare services (Alekya et al., 2020). The Internet of Things (IoT) is one of the revolutionary innovations that deeply transforms various aspects of human life in the growing digital era (Nahari et al., 2023). IoT enables data transfer between connected devices in real-time without the need for human intervention (Azbeg et al., 2022) (Sivasankari & Varalakshmi, 2022). This creates a promising environment for executing actions automatically (Arora et al., 2019). Along with the increasing adoption of IoT in the healthcare sector, various conveniences have been materialized, from patient tracking, disease prediction, remote monitoring to automation of medical procedures (Al-Nbhany et al., 2024). In addition, it improves the quality of life (Mishra & Singh, 2023) by providing benefits to the community that by offering the possibility to save time and money in obtaining the desired medical facilities thanks to its flexible access (Kumar et al., 2023).

However, behind these positive potentials, critical issues aris relating to the security and privacy of the patients' medical data (Sereda & Jaskolka, 2022). A number of studies have highlighted that, in the implementation of IoT in the healthcare sector, privacy and security of medical data remain posing the major challenges (Lu & Xu, 2019)(Popoola et al., 2023). The successful implementation of these technologies relies heavily on an in-depth understanding of the relevant regulations and security standards.

The importance of medical data security becomes even more apparent in the context of information transfer between healthcare institutions. The process of sending the patient's data from one hospital to another involves the risks of data leakage or misuse. Therefore, a comprehensive understanding of the regulations governing the privacy and security of medical data is crucial in the utilization of IoT in healthcare.

The purpose of this literature review is to present a brief assessment of the previously proposed solutions, as well as highlighting the strengths and limitations of these studies. By acquiring an in-depth understanding of the existing regulatory framework, the primary weaknesses of previous researches become identifiable, hence determining the direction of the present research. With a focus on the said aspects, this paper aims to address those weaknesses and provide some new insights into the realm of privacy and security of medical data in the utilization of IoT in the healthcare sector.

This review is anticipated to enhance the understanding of the challenges posed in regard to the privacy and security in the use of IoT in healthcare services.

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 1, 2024, pp. 87-105

Additionally, it aims to contribute new scientific insights by proposing the more relevant and up-to-date solutions. The emphasis on the importance of problem identification and research objectives stresses the urgency and relevance of this research in the face of dynamic changes in healthcare technology.

There remain major obstacles in place when it comes to protecting the security and privacy of medical data, even with all the improvements and advantages that IoT has to offer to the healthcare industry. The discovery and study on the vulnerabilities of security and privacy in the existing IoT for healthcare systems is the main issue this research attempts to address. In particular, this research looks into:

1. Data Vulnerability: In what ways do IoT-based healthcare systems currently expose the patients' data to security risks during transport and storage?
2. Regulatory Compliance: In what ways do the current practices of IoT in healthcare diverge from the legally-established standards for data protection and privacy?
3. Technological Restraints: What are the technological restraints and limits impeding the successful deployment of secure Internet of Things solutions in the healthcare industry?
4. Proposed Solutions: Considering the improvements for data security and privacy in IoT-based healthcare services, what are the advantages and disadvantages of the current remedies as put forward in the reviewed literatures?

The goal of outlining these concerns is to provide a platform for future research and development of more resilient IoT-based healthcare systems by methodically exploring and addressing the important issues.

Methodology

This study uses the normative juridical methods and Systematic Literature Review (SLR) to identify and evaluate the scientific literatures relating to IoT in the healthcare sector from a legal perspective. Normative juridical research is carried out by examining library materials or secondary data, such as books, statutory regulations and other documents related to the present research. This method is used to identify and to analyze the legal norms that are applicable in a legal problem. Literature searches were conducted in major scientific databases, including ScienceDirect, Google Scholar, PubMed, IEEExplore, and MDPI, using specific keywords such as "IoT-based healthcare" and "legal perspective of IoT-based healthcare". The literature review was limited to the timeframe from 2019 to the present to ensure that the information obtained remain relevant to the current circumstances.

Inclusion and exclusion criteria were established to ensure that the selection of the papers to be reviewed was aligned with the focus of the research. Submitted papers were selected based on their relevance to the topic, legal perspective, and year of publication. This method ensures that the analyzed literatures reflect the latest developments in IoT implementation and regulation in the healthcare sector.

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Qualitative analysis was conducted to evaluate the key findings, the legal approaches used, and their impact on IoT implementation in healthcare services. The findings were then crafted to provide a thorough insight into the legal perspective of IoT in the context of healthcare, focusing on the relevant time period. This approach ensures that the research results contribute to an up-to-date legal understanding related to IoT in the healthcare sector.

Results and Discussion

Development of IoT in Healthcare Services

The Internet of Things has significantly changed the patient monitoring in healthcare services by enabling the real-time and remote tracking of vital signs and other health parameters, which improves the patient care and reduces the healthcare costs. IoT-based systems can collect and analyze various physiological data, such as blood or oxygen levels, heart rate, body temperature, and ECG signals, providing real-time feedback to medical professionals for timely intervention (Islam et al., 2023). These systems are particularly beneficial in managing chronic diseases and monitoring elderly patients, as they ensure continuous observation without the need for constant physical human supervision (Alshammari, 2023).

The integration of wearable IoT and the Internet of Medical Things (IoMT) has further improved the quality and satisfaction of healthcare by enabling early detection of diseases and reducing mortality (Chakraborty & Kishor, 2022). For example, IoT-enabled platforms combined with advanced machine learning algorithms can predict heart disease with high accuracy, thereby facilitating an early diagnosis and treatment. In addition, IoT systems can manage large volumes of data efficiently, providing healthcare professionals with intuitive dashboards for real-time monitoring and anomaly detection (Khan et al., 2023).

During the COVID-19 pandemic, the wearable IoT for healthcare monitoring systems proved to be invaluable by enabling remote monitoring of quarantined individuals, thus reducing the burden on healthcare providers and ensuring timely medical attention for those in need (Wu et al., 2023). In addition, IoT platforms integrated with fog computing and blockchain technology offer increased security and reduced latency, making them suitable for the applications of critical real-time health monitoring (Alam et al., 2022). AI-powered IoMT infrastructure further streamlines the processes by automating data analysis and alerting healthcare workers in case of abnormalities, thereby improving the overall efficiency and effectiveness of the patient monitoring (A et al., 2023).

The increasing use of electronic health records (EHR), the internet of medical things (IoMT) and cloud computing become the important features which consequently lead to the need to maintain the security and privacy of the patients' data. The transition to digital systems, in addition to improving accuracy, reliability and patient accessibility, can also pose significant risks such as unauthorized access to EHRs that can lead to data breaches and compromise the confidentiality of the patients' data (Mohan, 2023). IoT security has the primary goal of ensuring the privacy, confidentiality, integrity, and availability of the services offered (Schiller et al., 2022).

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105

Protection of the patients' data requires certain solutions such as authentication, access control, and solid regulation.

IoT and Blockchain Technology

Blockchain technology with a decentralized concept has several advantages over previous security technologies, including the ability to prevent various cyberattacks such as ransomware that can damage the system (Haleem et al., 2021). Blockchain guarantees the integrity and immutability of the data by providing a secure ledger, wherein the data added to the blockchain will be permanent and irremovable or inalterable by anyone (Qose et al., 2023).

The implementation of blockchain is proposed to be a solution to improve the security and integrity of medical data. In the context of healthcare services, blockchain is able to secure electronic medical records (EMRs) by ensuring that any medical records added to the blockchain cannot be altered, ultimately increasing trust between the patients and the healthcare providers. Additionally, the ability of blockchain to duplicate data across different nodes in the network makes medical data more resilient to loss or damage that may occur due to hardware failure or cyberattacks.

The integration of blockchain and IoT offers significant improvements in the security of large-scale data storage (Alruwaill et al., 2023). In IoT-connected systems, medical devices can transmit data directly to the blockchain, ensuring that any data received remains secure and cannot be manipulated. This is especially important in the context of real-time monitoring of a patient, wherein accurate and inalterable data are crucial information for medical decision-making.

Blockchain also supports the use of smart contracts that automate and secure the procedures such as the processing of medical claims and various other data, thereby reducing administrative costs and increasing efficiency (Singh et al., 2023). Smart contracts can ensure that medical claims are processed automatically once all pre-defined conditions are satisfied, reducing human error and potential fraud. In addition, the use of smart contracts can speed up payment process for the claims and reduce waiting times for patients as well as the healthcare providers.

Regulation for the Protection of the Patients' Privacy

The administrative functions of the government per the Law Number 30 of 2014 on Government Administration, as enshrined in Article 1 Paragraph 2, include regulation, service, development, empowerment, and protection. The function of serving the community aims to satisfy the needs of the community in various aspects. The concept of government service derives from the mandate of the 1945 Constitution of the Republic of Indonesia, Article 34 paragraph (3), which states that the state is responsible for providing proper service facilities. This means that the state is obliged to serve every citizen without discrimination, ensuring their rights and needs are met, including in the current era of digitalization.

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105
P-ISSN: 1412-6834
E-ISSN: 2550-0090

The era of digitalization represents a shift from the modern era towards the formation of a digital society. All forms of services, both government and private, have become paperless, replaced by the use of applications that not only save the papers but also reduce the service times. The bureaucratic system, previously known for its sluggishness and complexity, requiring numerous documents, has now become more effective and efficient. The internet has emerged as a vital necessity for the digital society, prompting the government to prioritize the utilization of information technology in public services.

Along with the emergence of the digitalization era, humans have also experienced significant changes in various aspects of life. One example of the impact of changes in the digitalization era is the realm of public services, which currently utilizes the internet to meet the needs of the community. The massive use of information technology has given rise to the concept of the smart city, which has become a trend in many countries around the world over the past few years. In 2019, the Ministry of Communication and Information launched the "Movement Towards 100 Smart Cities" program. A smart city integrates information and communication technology (ICT) to enhance the quality and efficiency of urban services like healthcare, energy, transportation, and utilities. Its goal is to decrease the consumption of resource, waste, and overall costs.

The smart city concept aims to use technology and information-based solutions to improve the quality of life for the citizens, enhance interactions between the citizens and the government, and promote sustainable development (Ismagilova et al., 2022). A Smart City can be simply interpreted as a city that uses smart solutions to provide a better quality of life and comfort for its citizens (Pratiwi et al., 2021).

Smart City is essentially a Cyber-Physical-Social system within the scope of the city, which integrates the city's physical, social, and digital systems through the cyber media. The city's physical system includes various infrastructure supporting the city life, such as buildings, bridges, electricity networks, rivers, roads, offices, stations, terminals, airports, communication infrastructure, the list goes on. Meanwhile, the city's social system includes various human environments and individuals in the city, including the city government, community, family, market, general public, and individual residents of the city. The city's digital system includes sensors, computer networks, computing and control, data centers, and the likes (Febrianti et al., 2021).

The current digitalization in the healthcare sector is growing rapidly, especially after the COVID-19 pandemic. The smart city concept emphasizes a digital system that can enhance the speed and accuracy of healthcare service management, encourage the development of effective and efficient health solutions, and improve the quality, equity, and accessibility of healthcare.

Healthcare services encompass activities aimed at enhancing, preventing, curing, and restoring health. In the present digital era, these services are increasingly supported

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105

by the technology to improve their effectiveness, efficiency, and accessibility by the patients. This aligns with the government's strategic healthcare development plan and the goal of realizing the Healthy Indonesia Vision of 2025 (Ardiansyah & Ardiana, 2023).

The management of information systems for healthcare services developed based on digitalization can enable major healthcare breakthroughs such as telemedicine, online diagnostics, e-pharmacy, and robotic surgery. The benefits of digitizing health services include a quicker identification of the source of diseases, thus reducing the time required for treatment and increasing the likelihood of recovery. Patients spend less time in healthcare services, leading to the reduced costs for both the healthcare services providers and the patients themselves (Syaefuddina et al., 2022).

Telehealth, as defined in Health Law Number 17 of 2023, involves delivering and supporting health services, such as public health, health information services, and self-service, through telecommunications and digital communication technology. Additionally, according to Law No. 17 of 2023, telemedicine is the delivery and support of clinical services through telecommunications and digital communication technology. The technology used in telemedicine is IoT. IoT in healthcare services is based on the flow of service processes at healthcare facilities (hospitals, healthcare centers, pharmacies) that are commonly carried out in Indonesia. This includes the patients registration process, the patients queuing process, the healthcare services process, the queuing process at the pharmacy, the drug collection process at the pharmacy, and the payment process at the cashier.

The Internet of Things is a technology that facilitates the control, communication, and collaboration among diverse hardware devices over the internet. It represents a significant advancement in information technology and networking. IoT goes beyond remote control, encompassing data sharing and the transformation of real-world objects into internet-connected entities. In IoT, "things" can include entities such as a person with a heart implant monitor, a farm animal with a biochip transponder, or a car equipped with sensors to alert the driver of low tire pressure.

In telehealth applications, security is an important requirement due to the sensitive nature of the data involved. According to the Indonesian Ministry of Health and Information Data Center in 2014, data from healthcare information systems was reported to be ten times more valuable on the black market than data from credit card and other social security information systems. According to McNally & Newman, the term "identity theft" often describes the theft and the misuse of identity information. Usually, misuse of information follows the theft of information. Legally, these two actions are separate crimes. Identity information includes various "means of identification" such as name, address, credit card number, and social security number (Reynolds, 2023).

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Article 23 of the Government Regulation No. 46 of 2014 on Healthcare Information Systems has deviced the Security and Confidentiality of Information. It states that the security of healthcare information is conducted to ensure that such information remains available, maintains its integrity, and retains confidentiality for confidential healthcare information.

Papers have been written by (Czekster et al., 2023) which stated that security in the implementation of IoT in healthcare systems is a major concern. The main challenges involve cybersecurity and the protection of the patients' data, especially in the context of using smart medical devices and remote healthcare monitoring. It emphasizes that the security of smart medical devices is an important focus to prevent cyberattacks and ensure the accuracy of health data. Additionally, in pandemic situations such as COVID-19, it is explained that IoT can play a role in health data collection, but it needs to ensure the data security and privacy, including in the context of medical triage and medical resource management. In this paper, security is identified as a critical aspect that requires undivided attention when it comes to the application of IoT technology in the healthcare sector (Nižetić et al., 2020).

In another paper by Hutabarat (2022), it is mentioned that there are several laws and regulations governing the privacy of the patients' data in the utilization of IoT in the healthcare services (Hutabarat et al., 2022). The laws include Law No. 8/1999 on Consumer Protection, Law No. 44/2009 on Hospitals, and Law No. 29/2004 on Medical Practice. Additionally, the paper highlights the importance of sensitive data protection and legal certainty related to the use of IoT in healthcare services. In the context of using IoT-based applications, the General Data Protection Regulation (GDPR), which is the data protection regulation enforced in the European Union, likewise regulates the responsibilities between data controllers and data processors. Furthermore, a re-evaluation of the PDP Bill is needed to clarify the supervision and standardization of the use of IoT. Indonesia has a constitution that guarantees the protection of privacy rights; however, there is still a need for socialization and clear regulations to regulate the implementation of IoT in the healthcare sector. Thus, government supervision regarding the use of IoT in the health sector still needs to be tightened, and legislators must enact progressive laws in this regard (Sukmadilaga & Rosadi, 2020).

In the pursuit of enhancing the security of healthcare systems driven by IoT, the primary focus is on the security and privacy challenges associated with increased device connectivity. The integration of IoT in healthcare presents opportunities for more effective patient monitoring and service efficiency, yet it also brings about heightened complexities in terms of security. The elevated risk of cyberattacks and potential privacy breaches underscores the necessity for improved security solutions.

This paper emphasizes the importance of implementing stronger authentication mechanisms, meticulous access controls, and robust data encryption as pivotal

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105

measures to tackle security challenges. Furthermore, it highlights the significance of adopting a comprehensive approach involving all stakeholders, including healthcare providers and regulators, to establish a secure and dependable ecosystem for IoT deployment in healthcare. Thus, the emphasis on security is acknowledged as a critical component in advancing and integrating IoT into healthcare services infrastructure, ensuring that the advantages of this technology can be realized without compromising patient privacy or security (Irshad et al., 2023).

A paper by Cirne (2022) discusses several key challenges in using IoT with a focus on security aspects (Cirne et al., 2022). One of the main highlights are the increased connectivity and data exchange between IoT devices, which brings several security challenges that need to be addressed. A critical weakness discussed involves the lack of regulation in the IoT industry, particularly on the implementation of security mechanisms by manufacturers, creating an opening for potential security threats to the infrastructure. As a solution to this problem, the concept of IoT certification is discussed as a key step to improve security. Some existing certifications in the market are also outlined as examples. In terms of regulation, the role of the European Union (EU) is recognized in the paper for passing the Cybersecurity Act, a move to unify and regulate security certification in member states. A key point emphasized is the importance of IoT system certification as the most effective solution to improve security mechanisms and build buyer confidence in IoT devices.

Research utilizing the literature review method by Neto (2024) explains that IoT has been widely adopted in healthcare systems, offering various benefits, such as increasing the accuracy of medical procedures, improving decision-making processes, and creating new healthcare solution models (Neto et al., 2024). The study also emphasizes that IoT-based healthcare systems are vulnerable to security attacks and highlights the importance of deep learning-based intrusion detection to enhance IoT security in healthcare. This paper identifies Machine Learning techniques as a solution for securing IoT applications in healthcare services. Through a review of several studies, it is observed that various Machine Learning methods, such as Deep Learning (DL), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM), are employed to address security challenges in healthcare IoT.

In another paper by Agrawal (2023) discussing the integration of 5G technology in the medical field, 5G data transfer capabilities support real-time monitoring, diagnostics, and real-time genomic analysis, enabling personalized care (Agrawal et al., 2023). IoT in the 5G era increases security risks, so patients' privacy is a major concern in this regard. It is mentioned that the Health Insurance Portability and Accountability Act (HIPAA) regulations applicable in the United States are not only a legal requirement but also an important aspect in maintaining patients' trust and safety. This paper emphasizes the need for a balanced approach by prioritizing patients' privacy, data security, and regulatory compliance for the development of safe and effective health technology.

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Implementing cybersecurity standards for IoT is important to maintain security measures and standards that are appropriate to the IoT market and domain. There are policies from the European Telecommunications Standards Institute (ETSI) and NIST Interagency or Internal Reports (NISTIR) that can be used for cybersecurity on IoT devices (Yaacoub et al., 2023), namely:

1. ETSI EN 303 645 v2.1.1 as the global standard for cybersecurity of consumer IoT devices. It consists of 13 high-level recommendations and 35 recommendations, 68 provisions, and 33 mandatory requirements. ETSI TS 103 701 as an IoT security testing guide.
2. NISTIR 8259 which provides guidance to manufacturers and third parties in designing, testing and supporting IoT devices. It consists of three final documents and one draft document, including NISTIR 8259A and NISTIR 8259B.

The protection of personal data related to the use of digital platforms in Indonesia, among others, are regulated in the 1945 Constitution (UUD 1945) which is derived from its mandate into several regulations, namely 1. Law Number 8 of 1999 on Consumer Protection, 2. Law Number 23 of 2006 as amended by Law Number 24 of 2013 on Population Administration of the Republic of Indonesia (AKRI), 3. Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Electronic Information and Transactions (ITE Law), 4. Law Number 27 of 2022 on Personal Data Protection, 5. Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions (PP IEST), 6. Regulation of the Minister of Communication and Information Technology Number 20 of 2016 on the Protection of Personal Data in Electronic Systems.

The anticipation of the use of information technology in various aspects of life in Indonesia has been addressed through the preparation of the ITE Law. This law aims to provide legal certainty for both organizers and the public, who are users of information technology. Serving as the foundation for regulations in the Information Technology sector, the ITE Law significantly influences the implementation of various activities on electronic media. Article 15 Paragraphs (1) and (2) of the ITE Law mandate that every electronic system operator must ensure the reliable and secure operation of the electronic system, with the electronic system organizer bearing responsibility for its operation (Arfah & Puspitosari, 2023).

The implementation of IoT-based telemedicine itself is intrinsically linked to the trilogy of medicine as a crucial aspect in medical practice, namely informed consent, medical records, and medical secrets (Mangesti, 2021). After the repeal of the Law on Medical Practice, the medical trilogy is regulated in Health Law Number 17 of 2023 Paragraphs 5,6,7, namely on Approval of Health Service Actions, Medical Records and Patient Health Secrets.

Efforts to anticipate the potential leakage of health application data, especially IoT-based telemedicine applications, is one of the backgrounds for the Government of

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105

Indonesia to finally formalize the Personal Data Protection Law Number 27 of 2022. The Personal Data Protection Law is expected to provide the legal protection needed in the security of personal data of telemedicine patients (Arfah & Puspitosari, 2023).

During the Covid-19 pandemic, the Minister of Health Regulation Number 20 of 2019 on the Implementation of Telemedicine Services Between Health Care Facilities only regulates Telemedicine between Health Facilities, not on doctor-patient telemedicine and has not regulated the implementation of telemedicine specifically, especially legal protection for patients and their personal data and medical records (Mangesti, 2021).

The implementation of telemedicine uses on cyber networks as a tool that mediates between the consultant and the requestor, thus requiring a guarantee of personal data protection as a manifestation of medical confidentiality, especially regarding personal data and medical records of patients as requestors of consultations (Andrianto & Fajrina, 2021).

Article 4 Paragraph (1) of the Personal Data Protection Law states that personal data regulated and protected in this law is specific and general personal data. Specific personal data as referred to in paragraph (1) letter a of the Personal Data Protection Law includes: a. health data and information; b. biometric data; c. genetic data; d. crime records; e. child data; f. personal financial data; and/or g. other data in accordance with the provisions of laws and regulations.

Legal protection regarding personal data related to health services can be seen in Articles 35 through 39 of the Personal Data Protection Law.

1. Article 35 stipulates that the controller of personal data, or in this case, the electronic system organizer, is obliged to protect and ensure the security of personal data under its system. Data controllers in the implementation of telemedicine are healthcare facilities that provide telemedicine health service applications or websites.
2. Article 36 states that the controller of personal data is required to maintain the confidentiality of personal data when processing it. If the patient, as the requester of consultation, has agreed to receive medical services by providing informed consent to the doctor, who is the consulting party, then the patient is given a medical record in electronic form. This electronic medical record must be kept confidential by the healthcare facility, which acts as the data controller.
3. Article 37 regulates the obligation of the data controller to supervise the personal data of each party involved in the electronic system process.
4. Article 38 requires the controller of personal data to protect personal data from any form of unauthorized processing.
5. Article 39 reiterates in Paragraph 1 that the data controller has an obligation to prevent personal data from being accessed unlawfully. The prevention mentioned in Paragraph 2 must be carried out by using a reliable, secure, and responsible security system in accordance with the provisions of laws and regulations.

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105
P-ISSN: 1412-6834
E-ISSN: 2550-0090

In line with the concept of Cyber Security is the CIA Triad, which ensures confidentiality, integrity, and availability of systems or information.

Health Law No. 17 of 2023 is like a dipper with the Personal Data Protection Law to fill the legal vacuum for the protection of patient personal data that has not been regulated through article 351 which contains, among others, in:

1. Paragraph (1) that the Health Information System Operator shall ensure the protection of Health data and information of each individual.
2. Paragraph (2) Processing of Health data and information that uses individual Health data must obtain the consent of the data owner and/or fulfil other conditions that are the basis for processing personal data in accordance with the provisions of laws and regulations in the field of personal data protection.
3. Paragraph (3) The data owner as referred to in paragraph (2) is entitled to: a. obtain information regarding the purpose of collecting individual health data; b. access and make improvements to data and information through the Health Information System organizer; c. request the Health Information System organizer to the organizer of other Health Information Systems d. request the Health Information System organizer to delete incorrect data with the consent of the data owner; and e. obtain other personal data subject rights in accordance with the provisions of laws and regulations in the field of personal data protection.
4. Paragraph (4) The rights of data owners as referred to in paragraph (3) shall be exempted for certain purposes as stipulated in laws and regulations in the field of personal data protection.
5. Paragraph (5) The Health Information System Operator shall inform the data owner if there is a failure to protect individual Health data and information in accordance with the provisions of laws and regulations in the field of personal data protection.
6. Paragraph (6) The protection of individual health data and information shall be carried out in accordance with the provisions of laws and regulations.

Healthcare facilities as organizers of electronic systems as well as controllers of personal data have the responsibility to protect patients' personal data. In the practice of telemedicine health services, it is the responsibility of healthcare facilities to provide protection of personal data and patient medical records by referring to the Law Number 20 of 2022 on Personal Data Protection which regulates the responsibility of health care facilities for telemedicine patient data, among others, at:

1. Article 67 of the Personal Data Protection Law states that every person who intentionally and unlawfully:
    a. obtaining or collecting Personal Data that does not belong to him/her with the intention to benefit himself/herself or others which may result in harm to the Personal Data Subject as referred to in Article 65 paragraph (1) shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp 5,000,000,000.00 (five billion rupiah).

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105

b. disclose Personal Data that does not belong to him as referred to in Article 65 paragraph (2) shall be punished with a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp 4,000,000,000.00 (four billion rupiah).
c. using Personal Data that does not belong to him as intended in Article 65 paragraph (3) is punishable by imprisonment for a maximum of 5 (five) years and/or a fine of a maximum of IDR 5,000,000,000.00 (five billion rupiah).

2. Article 68 of the Personal Data Protection Law which states that any person who intentionally falsifies personal data for the purpose of benefiting themselves or others will be punished with imprisonment for a maximum of 6 (six) years or may be subject to a maximum fine of Rp 5,000,000,000.00 (five billion rupiah).
3. Furthermore, Article 70 Paragraph (1) of the Personal Data Protection Law also stipulates that if the criminal offense as mentioned in Article 67 and Article 68 is committed by a corporation or in this case a health service facility, then the punishment can be imposed on the management, controllers, commanders, beneficial owners, and/or responsible corporate parties. Article 70 Paragraph (2) of the Personal Data Protection Law explains that health service facilities as absolute corporations as a whole can only be subject to fines. Healthcare facilities can be subject to additional punishment in the form of confiscation of profits from criminal acts, freezing of all or part of the health service facility, permanent prohibition to continue to carry out business, closure of all functions of the healthcare facility, implementation of obligations resulting from criminal acts, payment of compensation, revocation of licenses, and dissolution of health service facilities.

The challenges and obstacles in implementing telemedicine services can hinder its adoption, particularly due to its reliance on an electronic system accessible to anyone, anywhere. Laws No. 27 of 2022 on Personal Data Protection and No. 17 of 2023 on Health impose strict regulations on electronic system providers, including healthcare facilities, to ensure full protection of patient data, including personal and medical records.

Blockchain Technology in Healthcare and Data Protection

This study has shown that blockchain technology is a critical component in resolving privacy and data security issues in IoT applications for the healthcare sector. The decentralized and unchangeable ledger system of blockchain technology guarantees the confidentiality and integrity of patient data by thwarting illegal access and data manipulation. Blockchain technology has the potential to greatly reduce hazards associated with IoT environments, including ransomware attacks and data breaches. Smart contracts, which automate tasks like processing medical claims and save administrative expenses while increasing efficiency, are another application of blockchain technology that is supported. Additionally, the combination of blockchain technology and IoT can offer strong security protocols for data transmission and storage, guaranteeing that patient data is safeguarded at every stage of its existence. As a result, implementing blockchain technology is not only a game-changing move

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024

JURNAL HUKUM
NOVELTY
Volume 15, Issue 1, 2024, pp. 87-105
P-ISSN: 1412-6834
E-ISSN: 2550-0090

for bettering healthcare services but also a vital step in securing patient data in the digital age.

Impact of IoT Usage in Health

The use of the IoT in the healthcare sector promises various benefits, such as the transformation of healthcare towards a patient-centered model, health system efficiency through responsiveness to big data, and remote patient monitoring through connected wearables. The integration of Machine Learning (ML) and Artificial Intelligence (AI) also helps in early disease detection and more efficient decision-making. However, risks associated with the lack of interoperability standards, security and privacy of health data, limitations of wearable devices, and challenges in ML and AI implementation need to be addressed. In addition, the use of blockchain technology to protect health data also brings error and security risks that need serious attention to ensure patient trust (Shafiq et al., 2023).

The impact of the use of IoT on patients' privacy rights in the context of technology utilization in the healthcare sector is very significant. Research by (Sembiring et al., 2023) highlights that the technological revolution in the IoT era has brought complex impacts on data privacy and security issues. One of the main findings is the misalignment of international and national regulations that can create legal uncertainty and gap in data privacy protection between countries. This shows that the protection of personal data and the authority to collect and use data are important focuses in maintaining the privacy of IoT users. In the context of IoT utilization in the healthcare sector, the protection of patients' personal data is a major issue that needs to be considered. In addition, IoT network security is also a key factor in maintaining privacy and avoiding the risk of data breaches. Therefore, law enforcement in the context of IoT requires cooperation between the authorities and the private sector. Overall, this study emphasizes the importance of addressing the legal challenges that arise with the development of IoT, as well as efforts to balance technological innovation with privacy protection and data security as keys to creating a safe and reliable IoT environment.

Conclusion

The Internet of Things (IoT) offers numerous benefits in healthcare, including enhanced decision-making, real-time patient monitoring, and improved service efficiency. However, it also introduces significant challenges, particularly concerning patient privacy and security of medical data. This includes vulnerabilities in data storage, regulatory compliance issues, and technological constraints. Solutions such as data encryption, strict access controls, and authentication mechanisms are crucial for safeguarding patient information from unauthorized access and breaches. Additionally, integrating blockchain technology can ensure data integrity and prevent tampering, aligning IoT healthcare practices with stringent data security frameworks.

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 1, 2024, pp. 87-105

The transition to smart cities, enabled by Information and Communication Technology (ICT), promises to revolutionize urban services like healthcare, enhancing their effectiveness and efficiency. Yet, it necessitates robust measures to protect the privacy and security of personal data generated and exchanged across interconnected devices. Government regulations play a pivotal role in upholding patient confidentiality and data safety in the evolving landscape of smart city initiatives. As research continues to advance IoT, blockchain, AI, 5G telecommunications, and data analytics in healthcare, addressing existing vulnerabilities and innovating new security solutions remains critical to ensuring robust medical data privacy and security.

Acknowledgement

The authors would like to thank Universitas Harapan Bangsa for supporting this research. Thanks also go to the anonymous reviewers and editors who have provided constructive feedback so that this manuscript is suitable for reading and citation.

Declarations

Author contribution : Author 1 initiated the research idea, developed the instruments, and conducted the analysis. Author 2 handles data collection and drafts the paper. Author 3 revised the research idea. All authors conducted the literature review and contributed to the drafting. Author 4, as an information technology expert, refined the analysis method, especially in the section on IoT and Blockchain technology.

Funding statement : The authors received no direct funding for this research

Conflict of interest : The authors declare no conflict of interest

Additional information : No additional information is available for this paper

References

A, A., Dahan, F., Alroobaea, R., Alghamdi, Wael. Y., Mustafa Khaja Mohammed, Hajjej, F., Deema mohammed alsekait, & Raahemifar, K. (2023). A smart IoMT based architecture for E-healthcare patient monitoring system using artificial intelligence algorithms. *Frontiers in Physiology*, *14*. https://doi.org/10.3389/fphys.2023.1125952

Agrawal, V., Agrawal, S., Bomanwar, A., Dubey, T., & Jaiswal, A. (2023). Exploring the risks, benefits, advances, and challenges in internet integration in medicine with the advent of 5G technology: A comprehensive review. *Cureus*. https://doi.org/10.7759/cureus.48767

Alam, S., Shuaib, M., Ahmad, S., Jayakody, D. N. K., Muthanna, A., Bharany, S., & Elgendy, I. A. (2022). Blockchain-based solutions supporting reliable healthcare for fog computing and internet of medical things (IoMT) integration. *Sustainability*, *14*(22), 15312. https://doi.org/10.3390/su142215312

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024

P-ISSN: 1412-6834
E-ISSN: 2550-0090

Alekya, R., Boddeti, N. D., Monica, K. S., Prabha, Dr. R., & Venkatesh, Dr. V. (2020). IoT based smart healthcare monitoring systems: A literature review. *European Journal of Molecular & Clinical Medicine*, *7*(11), 2761–2769.

Al-Nbhany, W. A. N. A., Zahary, A. T., & Al-Shargabi, A. A. (2024). Blockchain-IoT healthcare applications and trends: A review. *IEEE Access*, *12*, 4178–4212. https://doi.org/10.1109/ACCESS.2023.3349187

Alruwaill, M. N., Mohanty, S. P., & Kougianos, E. (2023). hChain: Blockchain based healthcare data sharing with enhanced security and privacy location-based-authentication. *Proceedings of the Great Lakes Symposium on VLSI 2023*, 97–102. https://doi.org/10.1145/3583781.3590255

Alshammari, H. H. (2023). The internet of things healthcare monitoring system based on MQTT protocol. *Alexandria Engineering Journal*, *69*, 275–287. https://doi.org/10.1016/j.aej.2023.01.065

Ardiansyah, M. R., & Ardiana, R. (2023). Kewajiban dan tanggung jawab hukum perdata dalam perlindungan privasi data pasien dalam layanan kesehatan digital. *Hakim*, *1*(4), 276–287.

Arfah, N. A., & Puspitosari, H. (2023). Perlindungan hukum terhadap data pasien telemedicine dalam menerima pelayanan medis berbasis online. *Jurnal Syntax Fusion*, *3*(07), 658-668. https://doi.org/https://doi.org/10.54543/fusion.v3i07.339

Arora, A., Kaur, A., Bhushan, B., & Saini, H. (2019). Security concerns and future trends of internet of things. *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, 891–896. https://doi.org/10.1109/ICICICT46008.2019.8993222

Azbeg, K., Ouchetto, O., Andaloussi, S. J., & Fetjah, L. (2022). A taxonomic review of the use of iot and blockchain in healthcare applications. *IRBM*, *43*(5), 511–519. https://doi.org/10.1016/j.irbm.2021.05.003

Chakraborty, C., & Kishor, A. (2022). Real-time cloud-based patient-centric monitoring using computational health systems. *IEEE Transactions on Computational Social Systems*, *9*(6), 1613-1623. https://doi.org/10.1109/TCSS.2022.3170375

Cirne, A., Sousa, P. R., Resende, J. S., & Antunes, L. (2022). IoT security certifications: Challenges and potential approaches. *Computers & Security*, *116*, 102669. https://doi.org/10.1016/j.cose.2022.102669

Czekster, R. M., Grace, P., Marcon, C., Hessel, F., & Cazella, S. C. (2023). Challenges and opportunities for conducting dynamic risk assessments in medical IoT. *Applied Sciences*, *13*(13), 7406. https://doi.org/10.3390/app13137406

Febrianti, F., Wibowo, S. A., & Vendyansyah, N. (2021). Implementasi IoT (internet of things) monitoring kualitas air dan sistem administrasi pada pengelola air bersih skala kecil. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *5*(1), 171–178. https://doi.org/https://doi.org/10.36040/jati.v5i1.3249

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 1, 2024, pp. 87-105

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, *2*, 130–139. https://doi.org/10.1016/j.ijin.2021.09.005

Hutabarat, D. T. H., Zebua, R., Sitorus, R. A., Subakti, F. A., Ramadhani, H., Mangunsong, J., Nduru, F., Alfah, G. S., Pasaribu, J. C. D., Malau, R. M., Anhar, I., & Sahdan, P. (2022). The urgency of legal protection against the implementation of electronic information technology-based medical records in regulation of the minister of health of the republic of indonesia number 269 of 2008. *Journal of Humanities Social Sciences and Business (JHSSB)*, *1*(4), 59-68. https://doi.org/10.55047/jhssb.v1i4.234

Irshad, R. R., Sohail, S. S., Hussain, S., Madsen, D. Ø., Zamani, A. S., Ahmed, A. A. A., Alattab, A. A., Badr, M. M., & Alwayle, I. M. (2023). Towards enhancing security of IoT-Enabled healthcare system. *Heliyon*, *9*(11), e22336. https://doi.org/10.1016/j.heliyon.2023.e22336

Islam, Md. R., Kabir, Md. M., Mridha, M. F., Alfarhood, S., Safran, M., & Che, D. (2023). Deep learning-based iot system for remote monitoring and early detection of health issues in real-time. *Sensors*, *23*(11), 5204. https://doi.org/10.3390/s23115204

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, *24*(2), 393–414. https://doi.org/10.1007/s10796-020-10044-1

Karale, A. (2021). The challenges of IoT addressing security, Ethics, Privacy, and Laws. *Internet of Things*, *15*, 100420. https://doi.org/10.1016/j.iot.2021.100420

Khan, M. A., Din, I. U., Kim, B.-S., & Almogren, A. (2023). Visualization of remote patient monitoring system based on internet of medical things. *Sustainability*, *15*(10), 8120. https://doi.org/10.3390/su15108120

Kumar, A., Nanthaamornphong, A., Selvi, R., Venkatesh, J., Alsharif, M. H., Uthansakul, P., & Uthansakul, M. (2023). Evaluation of 5G techniques affecting the deployment of smart hospital infrastructure: Understanding 5G, AI and IoT role in smart hospital. *Alexandria Engineering Journal*, *83*, 335–354. https://doi.org/10.1016/j.aej.2023.10.065

Lu, Y., & Xu, L. Da. (2019). Internet of things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103–2115. https://doi.org/10.1109/JIOT.2018.2869847

Mangesti, Y. A. (2021, April 21). *Perlindungan hukum data pribadi pasien telemedicine*. Kompasiana. https://www.kompasiana.com/yovitamangesti3767/60780cf2d541df6d7b325dc2/perlindungan-hukum-data-pribadi-pasien-telemedicine#google_vignette

Mishra, P., & Singh, G. (2023). Internet of medical things healthcare for sustainable smart cities: current status and future prospects. *Applied Sciences*, *13*(15), 8869. https://doi.org/10.3390/app13158869

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024

P-ISSN: 1412-6834
E-ISSN: 2550-0090

Mohan, P. (2023). IoT preserving patient-centric models for privacy preserving based personal health records sharing in cloud. *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, 1–6. https://doi.org/10.1109/ICICACS57338.2023.10100155

Nahari, R. V., Alfita, R., Astuti, E. D., Pramudia, M., & Rahmawati, D. (2023). *Fundamental internet of things (IoT) : Teori dan aplikasi* . Eureka Media Aksara.

Neto, E. C. P., Dadkhah, S., Sadeghi, S., Molyneaux, H., & Ghorbani, A. A. (2024). A review of Machine Learning (ML)-based IoT security in healthcare: A dataset perspective. *Computer Communications*, *213*, 61-77. https://doi.org/10.1016/j.comcom.2023.11.002

Nižetić, S., Solic, P., Lopez-de-Ipina González-de-Artaza, D., & Patrono, L. (2020). Internet of things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*, 122877. https://doi.org/10.1016/j.jclepro.2020.122877

Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehia, A., & Popoola, J. (2023). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, Challenges and Solutions. *Blockchain: Research and Applications*, 100178. https://doi.org/10.1016/j.bcra.2023.100178

Pratiwi, D. N., Budiman, J., & Syarifuddin, T. I. (2021). Prospek pembangunan area percontohan smart city polder Sangatta Utara Kabupaten Kutai Timur. *Jurnal Ilmiah Administrasi Publik Dan Pembangunan*, *12*(1), 45–58.

Qose, S., Rajnai, Z., & Fregan, B. (2023). Blockchain technology in healthcare industry: Benefits and issues. *2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 171-176. https://doi.org/10.1109/SACI58269.2023.10158669

Reynolds, D. (2023). Decisions, decisions: An analysis of identity theft victims' reporting to police, Financial Institutions, and Credit Bureaus. *Victims & Offenders*, *18*(7), 1373-1400. https://doi.org/10.1080/15564886.2022.2128129

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

Sembiring, T. B., Muhammad, Z., Hafizi, R., Febryani, E., Marsal, I., Gunung, U., & Cirebon, J. (2023). Revolusi teknologi dan tantangan hukum: Perspektif Privasi dan Keamanan Data dalam Era Internet of Things (IoT). *Jurnal Cahaya Mandalika*, *3*(2), 1217-1222. https://doi.org/https://doi.org/10.36312/jcm.v3i2.2202

Sereda, B., & Jaskolka, J. (2022). An evaluation of IoT security guidance documents: a shared responsibility perspective. *Procedia Computer Science*, *201*, 281–288. https://doi.org/10.1016/j.procs.2022.03.038

Shafiq, M., Choi, J.-G., Cheikhrouhou, O., & Hamam, H. (2023). Advances in IoMT for healthcare systems. *Sensors*, *24*(1), 10. https://doi.org/10.3390/s24010010

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 15, Issue 1, 2024, pp. 87-105

Singh, A. K., Garg, A., & Nayyar, A. (2023). Blockchain for security and privacy in healthcare informatics. In *Innovations in Healthcare Informatics: From interoperability to data analysis* (pp. 157–184). Institution of Engineering and Technology. https://doi.org/10.1049/PBHE041E_ch5

Sivasankari, B., & Varalakshmi, P. (2022). Blockchain and IoT technology in healthcare: a review. *Studies in Health Technology and Informatics*, 277–278. https://doi.org/10.3233/SHTI220455

Sukmadilaga, A., & Rosadi, S. D. (2020). Upaya hukum terhadap pelanggaran implementasi internet of things (Iot) di bidang pelayanan kesehatan menurut ketentuan perlindungan data pribadi. *Suara Keadilan*, *21*(2), 205–221.

Syaefuddina, M. A. S. M. A., Saifuddin, A. S. A., & Purwanti, W. P. W. (2022). Konsep AMO dalam penerapan GHRM mewujudkan digitalisasi kesehatan di lingkungan smart city. *CAKRAWALA*, *29*(2), 40-49. https://download.garuda.kemdikbud.go.id/article.php?article=3588505&val=31151&title=Konsep%20AMO%20Dalam%20Penerapan%20Ghrm%20Mewujudkan%20Digitalisasi%20Kesehatan%20Di%20Lingkungan%20Smart%20City

Wu, J.-Y., Wang, Y., Ching, C. T. S., Wang, H.-M. D., & Liao, L.-D. (2023). IoT-based wearable health monitoring device and its validation for potential critical and emergency applications. *Frontiers in Public Health*, *11*. https://doi.org/10.3389/fpubh.2023.1188304

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems*, *3*, 280-308. https://doi.org/10.1016/j.iotcps.2023.04.002

Article History
Submitted 22 February 2024 - Revision Required 8 June 2024 - Accepted 28 June 2024