Security and Privacy of Technologies in HISs

Subjects: Computer Science, Information Systems

Contributor: Parisasadat Shojaei, Elena Vlahu-Gjorgievska, Yang-Wai Chow

Health information systems (HISs) have immense value for healthcare institutions, as they provide secure storage, efficient retrieval, insightful analysis, seamless exchange, and collaborative sharing of patient health information. HISs are implemented to meet patient needs, as well as to ensure the security and privacy of medical data, including confidentiality, integrity, and availability, which are necessary to achieve high-quality healthcare services.

Keywords: health information systems ; healthcare ; medical data ; security ; privacy

1. Introduction

Described as comprehensive, technology-based systems, health information systems (HISs) are designed to manage and organize health data and information. These systems assist healthcare organizations in storing, retrieving, analyzing, and exchanging patient health information, thereby supporting clinical decision-making and enhancing patient care and outcomes. HISs typically include a range of software applications and tools for electronic health records (EHRs), health information exchange, clinical decision support (CDS), and administrative functions. These systems are versatile, being used in various settings such as hospitals, clinics, long-term care facilities, public health agencies, and even at home. HISs also play a pivotal role in enhancing data security and privacy, supporting compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA) [1].

The increase in digitalization of patient health information through electronic health records and personal health records has created new and serious threats to patient information security and privacy [2]. Medical data containing sensitive information about a patient's health and personal life, including medical history, diagnoses, treatments, and personal identifying information, are vulnerable to breaches. Such breaches can lead to serious consequences, including identity theft, fraud, and medical malpractice [3]. The security of patient data encourages individuals to share their personal health information for current or future care [3]. Furthermore, if healthcare professionals cannot trust an organization to protect records, they may be reluctant to record all information collected from patients [4]. Therefore, it is essential that HISs are designed and implemented with privacy and security as core considerations [4]. This includes using secure technologies for storing and transmitting data, implementing access controls, and providing training to healthcare professionals on best practices for ensuring patient security and privacy. Moreover, ensuring the security and privacy of medical data, including confidentiality, integrity, and availability, is necessary to achieve high-quality healthcare services [3][4].

Table 1 provides an overview of the security and privacy technologies used in various HISs [3].

Table 1. Overview of various health information systems.

Health Information System	Security Technologies	Privacy Technologies	Advantages	Disadvantages
Electronic Health Records (EHRs)	Encryption, Access Control, Auditing	Data Masking, Patient Consent Mechanisms	Improved data integrity, Efficient access control	Complex implementation, High initial setup costs, Privacy concerns, Concerns over data breaches
Health Information Exchange (HIE)	Secure Data Transmission Protocols, Identity Management	Anonymization Techniques, Consent Management Systems	Enhanced interoperability and data sharing	Concerns over data breaches during exchange, Consent management challenges
Clinical Trial Management Systems	Secure Data Storage, Blockchain for Auditing	De-identification Methods, Informed Consent Platforms	Enhanced traceability, Immutable data records	Limited scalability, Ethical concerns related to consent

2. Mobile Health Application

Mobile devices play an important role in the management of medical data in health information science. However, organizations must ensure that appropriate security and privacy measures are in place to protect sensitive information from unauthorized access or theft. These privacy and security measures align with the proposals of Ref. [5], who suggest threat modelling to identify potential threats and possible mitigations. By integrating security policies, defining sensitivity levels of form fields, and corresponding security mechanisms, data security can be catered to as early as the design phase. In addition, articles [6][7][8][9] implement secure models to strengthen the privacy and security of medical data within mHealth applications. These models aim to protect sensitive health information throughout its lifecycle, from collection and transmission to storage and access. For instance, Ref. [7] suggests a lightweight security framework for securing mHealth data collection systems, relying on lightweight and low-cost mechanisms to secure data exchanged with servers. These findings emphasize the importance of implementing strong encryption techniques for both data in transit and data at rest. This includes encrypting communication channels between devices and servers, as well as storing medical data on mobile devices and in the cloud [6]. For example, Ref. [6] proposes a scheme called an Efficient and Provable Secure Certificate-Based Combined Signature, Encryption, and Signcryption (CBCSES) scheme. This scheme not only provides encryption and signcryption but also offers an encryption or signature model when needed.

Moreover, mHealth applications can be designed using a secure framework for data collection, minimizing the risk of unauthorized access or theft of information. This contributes to securing the data exchanged with the server and includes key features such as tolerance to delays and lack of connectivity [5][7]. A previous study identified the need to use secure cloud storage for storing data, which can provide additional backup and security measures [8]. The system proposed in [8] offers salient features including efficient key management, privacy-preserving data storage and retrieval—particularly effective in emergency situations—and auditability to prevent misuse of health data. Furthermore, an approach presented in [9] utilized privacy-aware anomaly detection methods. These prioritize the security of health data by identifying abnormal patterns and ensuring the privacy of individual users, thus helping to maintain the confidentiality and integrity of sensitive health information [9].

3. IoT

The Internet of Things (IoT) has the potential to transform healthcare by enabling data collection and exchange from various devices and sensors. IoT devices feature built-in security measures, including encryption and authentication, to protect data in transit and storage while ensuring access is restricted to authorized parties [10].

IoT devices can store and organize medical data, simplifying access and analysis for healthcare professionals [11]. A new shared, agnostic, and permissioned decentralized data layer enhances data availability. This architecture has been implemented in a real-world Internet of Medical Things (IoMT) application [11], effectively handling sensitive data by preserving privacy and ensuring data availability without third-party reliance. Additionally, the IoT enhances data security and privacy through encryption, robust authentication, and access control, ensuring that sensitive health data are accessible only to authorized parties, thereby making unauthorized access more challenging [12][13][14][15][16].

It is important to note that IoT applications in healthcare offer cost reduction and efficiency benefits. These applications streamline operations, minimize errors and waste, and reduce system costs [13]. The focus in [13] was on avoiding the key escrow problem and establishing a new session key between servers and personal digital assistants (PDAs) for future communication, enhancing cost-effectiveness, and security against various attacks. Remote monitoring contributes to shorter hospital stays and fewer readmissions, improving treatment outcomes and reducing healthcare costs [13][17]. Furthermore, Ref. [17] discusses using an edge server to compute data authenticators to verify data integrity, significantly reducing computational costs and the management burden on third-party verifiers.

4. Blockchain

Extensive research has established that blockchain technology offers a secure, transparent, and tamper-proof method for storing and sharing medical data, which is crucial for maintaining patient privacy and security within HISs. Operating on a decentralized network, blockchain technology lacks a central authority controlling the data. This approach mitigates the risk of a single point of failure or a single entity accessing sensitive information, addressing potential security issues inherent in centralized storage systems [10]. Additionally, Ref. [10] discovered that blockchain technology can overcome challenges related to interoperability, security, confidentiality, privacy protection, and secure storage. Similarly, Ref. [18] integrated two decentralized technologies, the Solid ecosystem and blockchain, using solidity-based smart contracts to resolve security issues, thereby providing a secure, patient-centric design for complex, developing electronic health record (EHR) data exchange.

Blockchain technology can also create secure private networks for sharing sensitive medical data (transferred and distributed) exclusively among authorized parties [19][20]. For example, Ref. [19] proposes a permissioned blockchain-based system for EHR data sharing and integration, employing public key infrastructure-based asymmetric encryption and digital signatures to secure EHR data. This system ensures patient privacy protection and adheres to healthcare data management requirements, including the access control policy specified by the patient. Similarly, Ref. [21] introduced a privacy-preserving medical data-sharing scheme that balances the need for privacy with the necessity of data sharing. This perspective aligns with Ref. [20], who utilized a blockchain-based secure data sharing mechanism for the safe uploading and sharing of health data. The study by Ref. [22] developed a blockchain-based system with a secure data storage architecture to tackle cybersecurity storage challenges, employing private data collection to ensure privacy and decentralizing nodes in the network to prevent storage complications. This method also addresses other security challenges typically associated with centralized systems. Furthermore, blockchain technology enables the creation of smart contracts that automate data sharing under predefined conditions, ensuring that data are only shared with authorized parties. In line with this, Ref. [23] developed an access control framework based on smart contracts, which is built on a distributed ledger (blockchain), to secure the sharing of electronic medical records among various entities in the smart healthcare system.

In the context of blockchain applications in HISs, patient autonomy is a central theme, allowing individuals to have ownership and control over their personal health data. This empowerment is crucial, yet it poses challenges, particularly when patients are cognitively impaired or unable to manage their data. In such cases, the use of advanced directives or legally authorized representatives could be integrated into blockchain systems to ensure responsible data management [24]. Moreover, blockchain's decentralized nature and cryptographic techniques provide robust security for health data [18]. However, challenges arise in maintaining consistent permissions, especially in emergency situations where swift access to patient data is crucial. Smart contracts and cryptographic keys within blockchain networks can be employed to manage permissions seamlessly, ensuring healthcare professionals have necessary access while maintaining patient privacy and data integrity [23].

Furthermore, the legal implications of using blockchain in HISs under different jurisdictions, such as the potential access by the U.S. government to cloud-stored data under U.S. law, raise significant privacy concerns. While blockchain offers many benefits for healthcare data security, its integration into existing healthcare systems must be approached with caution, ensuring adherence to regulations like the HIPAA and addressing potential privacy issues related to decentralized data storage. This necessitates a careful balance between technological innovation and compliance with legal and regulatory standards.

5. Cloud Computing

Cloud computing offers multiple advantages for ensuring the security and privacy of medical data in HISs. By adopting cloud-based solutions, healthcare organizations benefit from strong security controls, encryption, access controls, redundancy, and compliance certifications, all aimed at safeguarding patient data. These include multi-factor authentication and role-based access control, ensuring that only authorized personnel can access sensitive medical data, thereby enhancing security measures [25][26].

Moreover, cloud computing can be more cost-effective compared to maintaining an on-premises IT infrastructure. This efficiency comes from eliminating the need for expensive hardware and software, allowing healthcare organizations to reduce costs and improve their overall financial performance [25]. Cloud computing also guarantees data recovery following a disaster, further bolstering data security and privacy [8][27]. For instance, a study by Ref. [27] describes a secure encryption algorithm (SE) combined with fragmentation and dispersion for storage. This method is designed to protect data even if both the key and the public fragment of EHR data on clouds are compromised. This aligns with other research demonstrating that storing EHR in the cloud significantly enhances security and protects patient information from unauthorized access [28].

6. Other Technologies

In addition to the technologies mentioned earlier, several studies have examined methods that employ a variety of technologies to enhance the security and privacy of medical data. **Table 2** presents an overview of these technologies.

Table 2. Overview of other technologies used in HISs.

Reference	Technology Name	Security and Privacy Features	Primary Functions	Advantages
[29]	Multi-agent-based systems (user interface agent, authentication agent, connection establishment agent, and connection management agent)	Security Privacy	These intelligent agents make ease of use and effective communication between patients/users and the e-service providers.	Simple and efficient access control mechanism based on the agents' functionalities, Provides effective and secure e-health security services
[30]	Log of round value-based elliptic curve cryptography (LR-ECC) Herding genetic algorithm-based deep learning neural network (EHGA-DLNN)	Security Privacy	Enhance the security level during data transfer after the initial authentication phase	High security and accuracy
[31]	Hash-based BBS (HBBS)	Security	For integrity purposes, the hash value is generated using secure hash algorithm SHA-256 and is hidden in the least significant bit (LSB) of the extracted pseudo-random bits for the purpose of generating multiple keystreams.	Has high security and good efficiency
[32]	Decentralized federated learning-based convolutional neural network	Security Privacy	Presents a privacy-friendly and secure EHR scheme for medical cyber-physical systems.	Securing valuable hospital biomedical data useful for clinical research organizations, Suitable for promoting a secure and privacy-friendly environment for sharing data with clinical research centers for biomedical research
[33]	Ordered binary decision diagram (OBDD)	Security	Achieves immediate attribute/user revocation, collusion resistance, forward security, backward security, efficiency, and expressiveness	The efficiency of the scheme can be attributed to the use of prime-order groups, minimized hashing operations, and reduced amount of exponentiation operations.
[34]	Elliptic curve cryptography (ECC) operations Physically unclonable function (PUF)	Security	Improve security and efficiency at the same time, Strict formal security proof is provided to demonstrate the proposed scheme meets the security and reliability requirements	Meets more security and usability requirements and takes less computational and communication costs than related protocols proposed recently
[35]	Lightweight encryption scheme Message authentication code (MAC) generation scheme	Security Privacy	Secures the communication between medical sensors and data servers	Achieves data confidentiality, authenticity, and integrity between each medical sensor and each data server
[36]	Subprotocols as building blocks, such as PPC, PPCC, PPSS, and PPSU protocols	Privacy	It first designs secure and privacy-preserving several subprotocols to ensure privacy in the e-healthcare system, then it adopts the greedy algorithm in a secure manner to perform the query and the min-heap technology to improve efficiency.	Practical and efficient in terms of computational cost and communication overhead
[37]	Near-field communication (NFC) authentication mechanism	Privacy	To generate a trustworthy source of visit records, the article uses a system that supplies concrete evidence that healthcare personnel visited a patient's residence.	Using the NFC tag enhances the workflow of users and integrates it into a seamless access control process. It helps improve user interaction by eliminating user input tasks.

Reference	Technology Name	Security and Privacy Features	Primary Functions	Advantages
[38]	Spring Framework services for sensitive data (TSD) Hypertext Transfer Protocol (HTTP (H))	Security	Providing secure hosting and operation of application services, collection, storage, processing, and provisioning of data	A key element of Spring is application-level infrastructure support. It effectively protects the application programming interface (API) and personal health data.
[20]	Edge cloud blockchain	Security	The edge cloud performs context-aware health situation identification and utilizes a blockchain-based secure data sharing mechanism to facilitate secure uploading and sharing of health data.	It identifies the health situation based on a similarity measure in the edge cloud. A blockchain-based securing data sharing mechanism is used to achieve secure sharing of health data among patients and health service providers.

The study by Ref. [38] developed a hybrid security solution using the Spring Framework, services for sensitive data (TSD) as a service platform, and Hypertext Transfer Protocol (HTTP) security methods. This solution provides secure hosting and operation of application services, as well as the collection, storage, processing, and provisioning of data. The results demonstrate that the adopted digital solution effectively protects APIs and personal health data. Another study by Ref. [31] presents a new hash-based BBS (HBBS) pseudo-random bit generator to ensure the integrity and security of data, making it suitable for smart health applications and telemedicine. This study also proposes an encryption technique aimed at achieving robust security during the transmission of medical data. Furthermore, Ref. [34] introduces a secure and lightweight approach using fewer elliptic curve cryptography (ECC) operations and a physically unclonable function (PUF), improving security and efficiency with lower computational and communication costs. The study by Ref. [35] proposes a privacy-preserving encryption approach that incorporates an innovative data collection protocol. This method involves dividing patient data into three parts and storing them across three data servers to maintain privacy.

Additionally, Ref. [36] designed several secure and privacy-preserving subprotocols to ensure privacy in an e-healthcare system, adopting a secure greedy algorithm for query performance and min-heap technology to enhance efficiency. The method in [37] offers an architecture that improves the reliability of data exchange between healthcare personnel by providing a security layer that supports accountability through context-aware services, enabling appropriate data access for users. Ref. [30] proposes a secure method for preserving privacy in healthcare data, specifically for disease prediction in modern healthcare systems. This system uses cryptography during data transfer and allows authorized healthcare staff to securely access patient data for disease prediction using a herding genetic algorithm-based deep learning neural network. Ref. [33] suggests a secure, expressive, and efficient access control scheme with immediate attribute/user revocation in collaborative e-health systems, based on the ordered binary decision diagram (OBDD) access structure. It binds user keys to user identities, therefore creating resistance to collusion attacks. Additionally, Ref. [29] highlights a model based on a multi-agent system comprising various intelligent agents such as a user interface agent, authentication agent, connection establishment agent, and connection management agent. This model provides effective and secure e-health security services, facilitating ease of use and effective communication between users and e-service providers.

Various studies have demonstrated the relationship between secure solutions for storing and sharing sensitive health information and ensuring the security and privacy of data in HISs. For instance, Ref. [32] proposed a secure scheme using a decentralized federated learning-based convolutional neural network, private and public interplanetary file systems (IPFS), a consortium blockchain network, and smart contracts. This scheme is ideal for promoting a secure and privacy-friendly environment for data sharing. In a study by Ref. [20], a framework for 5G-secure smart healthcare monitoring (5GSS) was employed for fast and accurate identification of context-aware health situations, along with a blockchain-based secure data sharing mechanism and low-latency services for emergent patients.

References

1. Yusof, M.M.; Papazafeiropoulou, A.; Paul, R.J.; Stergioulas, L.K. Investigating Evaluation Frameworks for Health Information Systems. Int. J. Med. Inform. 2008, 77, 377–385.

2. Vora, J.; Italiya, P.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Hsiao, K.F. Ensuring Privacy and Security in E-Health Records. In Proceedings of the International Conference on Computer, Information and Telecommunication Systems (CITS), Colmar, France, 11–13 July 2018.
3. Mbonihankuye, S.; Nkunzimana, A.; Ndagijimana, A. Healthcare Data Security Technology: HIPAA Compliance. Wirel. Commun. Mob. Comput. 2019, 2019, 1927495.
4. Qayyum, A.; Qadir, J.; Bilal, M.; Al-Fuqaha, A. Secure and Robust Machine Learning for Healthcare: A Survey. IEEE Rev. Biomed. Eng. 2020, 14, 156–180.
5. Katarahweire, M.; Bainomugisha, E.; Mughal, K.A.; Ngubiri, J. Form-based security in mobile health data collection systems. Secur. Priv. 2021, 4, e155.
6. Ullah, I.; Amin, N.U.; Khan, M.A.; Khattak, H.; Kumari, S. An Efficient and Provable Secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things (IoT) in Mobile Health (M-Health) System. J. Med. Syst. 2020, 45, 4.
7. Simplicio, M.A.; Iwaya, L.H.; Barros, B.M.; Carvalho, T.C.; Näslund, M. SecourHealth: A Delay-Tolerant Security Framework for Mobile Health Data Collection. IEEE J. Biomed. Health Inform. 2015, 19, 761–772.
8. Tong, Y.; Sun, J.; Chow, S.S.; Li, P. Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability. IEEE J. Biomed. Health Inform. 2014, 18, 419–429.
9. Xie, Y.; Zhang, K.; Kou, H.; Mokarram, M.J. Private anomaly detection of student health conditions based on wearable sensors in mobile cloud computing. J. Cloud Comput. 2022, 11.
10. Arul, R.; Al-Otaibi, Y.D.; Alnumay, W.S.; Tariq, U.; Shoaib, U.; Piran, M.J. Multi-modal secure healthcare data dissemination framework using blockchain in IoMT. Pers. Ubiquitous Comput. 2021.
11. Bigini, G.; Lattanzi, E. Toward the InterPlanetary Health Layer for the Internet of Medical Things With Distributed Ledgers and Storages. IEEE Access 2022, 10, 82883–82895.
12. Kong, F.; Zhou, Y.; Xia, B.; Pan, L.; Zhu, L. A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment. IEEE Access 2019, 7, 161822–161830.
13. Agrahari, A.K.; Varma, S.; Venkatesan, S. Two factor authentication protocol for IoT based healthcare monitoring system. J. Ambient Intell. Humaniz. Comput. 2023, 14, 16081–16098.
14. Ullah, F.; Ullah, I.; Khan, A.; Uddin, M.I.; Alyami, H.; Alosaimi, W. Enabling Clustering for Privacy-Aware Data Dissemination Based on Medical Healthcare-IoTs (MH-IoTs) for Wireless Body Area Network. J. Healthc. Eng. 2020, 2020, 8824907.
15. Shreya, S.; Chatterjee, K.; Singh, A. A smart secure healthcare monitoring system with Internet of Medical Things. Comput. Electr. Eng. 2022, 101, 107969.
16. Bashir, A.; Mir, A.H. Lightweight Secure MQTT for Mobility Enabled e-health Internet of Things. Int. Arab. J. Inf. Technol. 2021, 18, 773–781.
17. Ding, R.; Zhong, H.; Ma, J.; Liu, X.; Ning, J. Lightweight Privacy-Preserving Identity-Based Verifiable IoT-Based Health Storage System. IEEE Internet Things J. 2019, 6, 8393–8405.
18. Ghayvat, H.; Sharma, M.; Gope, P.; Sharma, P.K. SHARIF: Solid Pod-Based Secured Healthcare Information Storage and Exchange Solution in Internet of Things. IEEE Trans. Ind. Inform. 2022, 18, 5609–5618.
19. Dubovitskaya, A.; Baig, F.; Xu, Z.; Shukla, R.; Zambani, P.S.; Swaminathan, A.; Jahangir, M.M.; Chowdhry, K.; Lachhani, R.; Idnani, N.; et al. ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. J. Med. Internet Res. 2020, 22, e13598.
20. Hu, J.; Liang, W.; Hosam, O.; Hsieh, M.Y.; Su, X. 5GSS: A framework for 5G-secure-smart healthcare monitoring. Connect. Sci. 2022, 34, 139–161.
21. Xu, G.; Qi, C.; Dong, W.; Gong, L.; Liu, S.; Chen, S.; Liu, J.; Zheng, X. A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain. IEEE J. Biomed. Health Inform. 2022, 27, 698–709.
22. Mnyawi, R.; Kombe, C.; Sam, A.; Nyambo, D. Blockchain-based Data Storage Security Architecture for e-Health Care Systems: A Case of Government of Tanzania Hospital Management Information System. Int. J. Comput. Sci. Netw. Secur. 2022, 22, 364–374.
23. Saini, A.; Zhu, Q.; Singh, N.; Xiang, Y.; Gao, L.; Zhang, Y. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. IEEE Internet Things J. 2021, 8, 5914–5925.
24. Yongjoh, S.; So-In, C.; Kompunt, P.; Muneesawang, P.; Morien, R.I. Development of an Internet-of-Healthcare System Using Blockchain. IEEE Access 2021, 9, 113017–113031.

25. Shakil, K.A.; Zareen, F.J.; Alam, M.; Jabin, S. BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. J. King Saud Univ.-Comput. Inf. Sci. 2020, 32, 57–64.

26. Son, J.; Kim, J.D.; Na, H.S.; Baik, D.K. Dynamic access control model for privacy preserving personalized healthcare in cloud environment. Technol. Health Care 2015, 24 (Suppl. S1), S123–S129.

27. Qiu, H.; Qiu, M.; Liu, M.; Memmi, G. Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0. IEEE J. Biomed. Health Inform. 2020, 24, 2499–2505.

28. Roehrs, A.; Da Costa, C.A.; da Rosa Righi, R.; De Oliveira, K.S.F. Personal Health Records: A Systematic Literature Review. J. Med. Internet Res. 2017, 19, e5876.

29. Khan, F.; Reyad, O. Application of intelligent multi agent based systems for E-healthcare security. Inf. Sci. Lett. 2019, 8, 67–72.

30. Padinjappurathu Gopalan, S.; Chowdhary, C.L.; Iwendi, C.; Farid, M.A.; Ramasamy, L.K. An Efficient and Privacy-Preserving Scheme for Disease Prediction in Modern Healthcare Systems. Sensors 2022, 22, 5574.

31. Reyad, O.; Karar, M.E. Secure CT-Image Encryption for COVID-19 Infections Using HBBS-Based Multiple Key-Streams. Arab. J. Sci. Eng. 2021, 46, 3581–3593.

32. Salim, M.M.; Park, J.H. Federated Learning-based secure Electronic Health Record sharing scheme in Medical Informatics. IEEE J. Biomed. Health Inform. 2022, 27, 617–624.

33. Edemacu, K.; Jang, B.; Kim, J.W. Collaborative Ehealth Privacy and Security: An Access Control With Attribute Revocation Based on OBDD Access Structure. IEEE J. Biomed. Health Inform. 2020, 24, 2960–2972.

34. Jiang, Z.; Liu, W.; Ma, R.; Shirazi, S.H.; Xie, Y. Lightweight Healthcare Wireless Body Area Network Scheme With Amplified Security. IEEE Access 2021, 9, 125739–125752.

35. Yi, X.; Bouguettaya, A.; Georgakopoulos, D.; Song, A.; Willemson, J. Privacy Protection for Wireless Medical Sensor Data. IEEE Trans. Dependable Secur. Comput. 2016, 13, 369–380.

36. Zhang, M.; Chen, Y.; Susilo, W. PPO-CPQ: A Privacy-Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems. IEEE Internet Things J. 2020, 7, 10660–10672.

37. Dzissah, D.A.; Lee, J.S.; Suzuki, H.; Nakamura, M.; Obi, T. Privacy Enhanced Healthcare Information Sharing System for Home-Based Care Environments. Healthc. Inform. Res. 2019, 25, 106–114.

38. Chatterjee, A.; Gerdes, M.W.; Khatiwada, P.; Prinz, A. SFTSDH: Applying Spring Security Framework With TSD-Based OAuth2 to Protect Microservice Architecture APIs. IEEE Access 2022, 10, 41914–41934.

Retrieved from https://encyclopedia.pub/entry/history/show/124358