Review of Contemporary Philosophy
ISSN: 1841-5261, e-ISSN: 2471-089X
Vol 23 (2), 2024
Pp 1702 - 1712

Privacy Protection in Big Data Health Analytics: A Comprehensive Review of Challenges and Solutions

[1]-Reem Munawar Awad Al-Rashdi,[2]-Salihah Abdullah Saeed Alghamdi,[3]-Khuluod Ali Mohammed Rezgallah,[4]-Abdulaziz Ali Abdulaziz Alghaythar,,[5]- Faisal Fahad Mohammed Alshammari,[6]- Abdullah Jaber Eissa Faqihi,[7]-Dhaifallah Mohammed Dhaifallah Moraya,[8]- Muath Mohammed Dhaifallah Moraya,[9]- Khloud Masead Dhaif Allah Al-Mutairi.,[10]-Ahlam Abdullah Ibrahim Aqeel,[11]- Nasser Nashi Alshaibani,[12]-Khaled Ibrahim Muhammad Mobaraki,[13]-Mohammed Saleh Abdulkareem Al Juma,[14]-Sarah Ahmed Arif

1. Ksa, Ministry Of Health, The First Health Cluster In Riyadh
2. Ksa, Ministry Of Health, Al Imam Abdul Rahman Al Faisal Hospital
3. Ksa, Ministry Of Health, Al Imam Abdul Rahman Al Faisal Hospital
4. Ksa, Ministry Of Health, Primary Health Care Center In Aldar Albedh2
5. Ksa, Ministry Of Health, Eradah Complex And Mental Health - Hail
6. Ksa, Ministry Of Health, Jazan Eradh And Mental Health Hospital
7. Ksa, Ministry Of Health, Jazan Mental Health Hospital
8. Ksa, Ministry Of Health, Jazan Mental Health Hospital
9. Ksa, Ministry Of Health, Specialized Dental Center In Riyadh.
10. Ksa, Ministry Of Health, Jazan Mental Health Hospital
11. Ksa, Ministry Of Health, Diriyah Hospital
12. Ksa, Ministry Of Health, Samtah General Hospital
13. Ksa, Ministry Of Health, National Guard Health Affairs
14. Ksa, Ministry Of Health, Mohammed Bin Abdulaziz Hospital

Abstract

Background: The emergence of big data and Health Information Systems (HISs) has revolutionized healthcare delivery by improving data management and supporting clinical decision-making processes. However, this transition to digital platforms has introduced significant concerns surrounding the privacy and security of patient health data.

Methods: This systematic literature review investigates various technological solutions utilized in HISs, focusing on their effectiveness in protecting patient data. The review examines studies from several databases, including Scopus and PubMed, highlighting key privacy-preserving technologies such as blockchain, mobile health applications, the Internet of Things (IoT), and cloud computing.

Results: Findings reveal that while these technologies enhance data accessibility and operational

efficiency, they also introduce distinct security risks, including unauthorized access and data breaches. The results underscore the importance of developing comprehensive frameworks that prioritize patient privacy and security, in alignment with regulations such as HIPAA in the U.S. and GDPR in Europe.

Conclusion: The review concludes that the implementation of advanced security protocols, ongoing staff education, and adherence to regulatory standards are critical to fostering patient trust and safeguarding the confidentiality of health data in the context of big data.

Keywords: Privacy, Big Data, Health Information Systems, Data Security, Blockchain

Received: 13 October 2024 **Revised:** 27 November 2024 **Accepted:** 08 December 2024

Introduction

Characterized as extensive, technology-driven systems, health information systems (HISs) are intended to administer and structure health data and information. These systems aid healthcare organizations in the storage, retrieval, analysis, and exchange of patient health information, therefore facilitating clinical decision-making and improving patient care and results. Health Information Systems (HISs) generally include various software programs and tools for electronic health records (EHRs), health information interchange, clinical decision support (CDS), and administrative operations. These systems are adaptable, used in many environments including hospitals, clinics, long-term care institutions, public health organizations, and residential settings. Health Information Systems (HISs) are crucial for improving data security and privacy, facilitating adherence to requirements such as the Health Insurance Portability and Accountability Act (HIPAA) [1].

The proliferation of digitalization of patient health information via electronic health records and personal health records has engendered significant concerns to the security and privacy of patient information. Medical data including sensitive information on a patient's health and personal life, including medical history, diagnosis, treatments, and personally identifiable information, is susceptible to breaches. Such breaches may result in severe repercussions, including identity theft, fraud, and medical malpractice [2,3]. The protection of patient data incentivizes people to provide their personal health information for present or future medical treatment [3]. Moreover, if healthcare personnel lack confidence in an organization's ability to safeguard data, they may hesitate to document all information obtained from patients [4]. Consequently, it is imperative that Health Information Systems (HISs) be developed and executed with privacy and security as fundamental priorities [4]. This includes using secure technology for data storage and transmission, instituting access restrictions, and delivering training to healthcare personnel on optimal practices for safeguarding patient confidentiality and privacy. Furthermore, safeguarding the security and privacy of medical data—encompassing confidentiality, integrity, and availability—is essential for delivering high-quality healthcare services [3,4].

Prior literature evaluations have mostly focused on specific technologies, like blockchain and the Internet of Things (IoT) [5,6]. To yet, the majority of these research have not thoroughly elucidated and assessed the many methods for safeguarding the privacy and security of medical data. This literature review aims to comprehensively assess the security and privacy dimensions of various technologies used in health information systems, while analyzing their benefits, drawbacks, and prospective developments.

This literature review encompasses research using many technologies to augment the security and privacy of healthcare information. These technologies may be examined via three security dimensions: secure access management, safe data exchange, and secure data storage. To mitigate data security and privacy concerns, these technologies provide several safe methods, including secure frameworks, authentication protocols, privacy-preserving infrastructures, data storage solutions, and access control models [7,8].

This literature study assesses four contemporary technologies: mobile health apps, the Internet of Things (IoT), blockchain, and cloud computing, as well as additional approaches that integrate several technologies. Mobile applications and the Internet of Things (IoT) are distinct entities, as they fulfill different objectives and possess various attributes, including unique

features and functionalities, disparate access points, diverse operating systems, and differing threats, encompassing distinct security and privacy risks along with requisite security countermeasures. Mobile devices may need enhanced encryption or multi-factor authentication to access sensitive health information, whilst IoT devices may demand supplementary restrictions to safeguard the privacy and security of the data they gather and communicate.

Security of medical data and health information pertains to safeguarding sensitive patient information from illegal access, use, or disclosure. It includes many strategies to protect the confidentiality, integrity, and availability of health data [9]. Privacy is a distinct facet of security that emphasizes the regulation of the storage and dissemination of private information. The privacy of medical data is crucial since it gives people authority over the accessibility and use of their health information. This ensures the preservation of confidentiality and mitigates the illegal use or revelation of medical information, which may result in identity theft, discrimination, and other adverse outcomes [9].

Consequently, several governments have created rules and regulations. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 comprises federal legislation that safeguards the privacy and security of health information in the United States. These regulations guarantee people's rights to their health information and provide certain precautions for the safeguarding of electronic health data [10]. All entities functioning within the U.S. healthcare sector are required to adhere to HIPAA requirements. This includes healthcare providers, health plans, healthcare clearinghouses, and their commercial connections. The HIPAA establishes an extensive framework for safeguarding the privacy and security of health information. The principal principles include a security rule, a privacy rule, a breach reporting rule, and an enforcement rule. The security rule delineates the rules for safeguarding electronic protected health information (ePHI). It encompasses administrative, physical, and technological measures to guarantee the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI). Privacy regulation sets national standards for safeguarding people' medical records and personal health information. It regulates the use and dissemination of PHI and confers upon patients their rights over their health information. In the occurrence of a breach involving unsecured PHI, HIPAA-compliant businesses must inform impacted people, the Secretary of Health and Human Services, and, in some instances, the media. The enforcement rules describe the methods for investigating complaints and the consequences for non-compliance with HIPAA standards [3,11].

The privacy and security of Health Information Systems (HISs) are essential to safeguard the confidentiality of patient personal information and to avert any security breaches that might undermine data integrity. Moreover, access control mechanisms and comprehensive training are vital for safeguarding patient information and ensuring confidentiality [10]. The structure and execution of security and privacy in Health Information Systems (HISs) might differ markedly based on the nation and the category of provider or user. This diversity principally results from disparities in legislative frameworks, cultural perceptions of privacy, technical infrastructure, and the distinct requirements of healthcare providers and consumers. The European Union's General Data Protection Regulation (GDPR) is among the most extensive and rigorous privacy legislation, influencing global corporate data management of EU residents' information. Conversely, the United States employs a more sector-specific methodology, shown by legislation such as HIPAA for healthcare data and the Children's Online Privacy Protection Act (COPPA) for safeguarding children's data. Conversely, Australia's strategy on health information privacy is delineated in the Privacy Act 1988, which includes the Australian Privacy Principles (APPs) [12]. These principles include a more extensive range of personal information than the U.S. HIPAA and are applicable to a greater array of enterprises, including all private health care providers [12].

In the realm of HISs, the endorsement and regulation of adherence to rules, standards, and guidelines, together with the execution of audits and inspections, are supervised by many regulatory entities and governmental authorities. The HIPAA establishes standards for the storage, sharing, and management of health information, while the Office of the Inspector General enforces compliance via audits and investigations. Moreover, the validation of Health Information Systems increasingly includes security and

privacy considerations. This is crucial due to the delicate nature of health data and the changing environment of cybersecurity threats. Contemporary validation approaches for e-health systems emphasize the effective integration and compliance of security and privacy policies with relevant rules and standards. These methodologies generally encompass a synthesis of technological innovations, compliance with legal standards, and the implementation of optimal practices in data security and privacy management. The objective is to guarantee the confidentiality, integrity, and availability of health data throughout its lifespan, including collection, storage, and processing. The validation process often involves thorough testing and evaluation of security measures, privacy policies, and adherence to regulations such as HIPAA in the U.S. and GDPR in the EU. This method is essential for protecting patient data from illegal access, breaches, and other security problems [13].

In the domain of Health Information Systems (HISs), regulatory authorities like the U.S. The Food and Drug Administration (FDA) and the European Medicines Agency (EMA) provide crucial functions. These organizations are essential in developing and implementing standards that guarantee the safety, effectiveness, and privacy of health technology. The FDA in the United States regulates medical devices, including both software and hardware used in Health Information Systems (HISs). It establishes protocols that govern the development, testing, and implementation of these technologies to safeguard patient data and maintain system integrity. The EMA of the European Union similarly conducts evaluations and supervises medical items, consequently impacting healthcare technology across Europe.

These regulatory entities significantly influence the evolution and use of HIS technology inside healthcare settings. By imposing rigorous compliance standards, they shape the design and performance of HIS technology, emphasizing the confidentiality and privacy of patient data. Adherence to these laws is not just a legal requirement but also an essential element in fostering confidence and acceptability among healthcare practitioners and patients. Although these authorities mainly focus on safeguarding public health, their criteria also stimulate innovation, prompting developers and providers to devise solutions that adhere to these stringent standards while maintaining efficiency and user experience. Consequently, the roles and functions of the FDA, EMA, and other regulatory agencies are essential to the development and implementation of safe and privacy compliant HIS systems [14,15].

1. Methods

This literature study was performed across five databases (Scopus, Web of Science, PubMed, Medline, and IEEE) to gather publications concerning the privacy and security of health information systems. During the querying step, certain keywords were used to locate relevant articles.

2. Mobile Health Application

Mobile devices are crucial in the administration of medical data within health information science. Organizations must implement adequate security and privacy safeguards to safeguard sensitive information from unauthorized access or theft. The privacy and security measures correspond with the recommendations of [7], which advocate for threat modeling to recognize potential risks and corresponding mitigations. Data security may be addressed from the design phase by incorporating security rules, establishing sensitivity levels for form fields, and implementing associated security methods. Furthermore, studies [8,16-18] use secure methods to enhance the privacy and security of medical data in mHealth apps. These approaches seek to safeguard sensitive health information over its entire lifespan, including collection, transmission, storage, and access. Tong et al. [16] proposes a lightweight security framework for safeguarding mHealth data gathering systems, using cost-effective and efficient approaches to protect data sent to servers. These results underscore the need for using robust encryption methods for data both in transit and at rest. This encompasses the encryption of communication routes between devices and servers, along with the storage of medical data on mobile devices and in the cloud [8]. Ullah et al. [8] introduces a technique termed Efficient and Provably Secure Certificate-Based Combined Signature, Encryption, and Signcryption (CBCSES). This approach enables both encryption and signcryption, as well as an encryption or signature model as required.

Furthermore, mHealth apps may be developed using a secure architecture for data collecting, hence reducing the danger of unwanted access or information theft. This enhances the security of data sent to the server and encompasses essential properties such as delay tolerance and connection absence [7,16]. Prior research recognized the need of using secure cloud storage for data retention, which offers supplementary backup and security protocols [17]. The system delineated in [17] presents notable attributes such as effective key management, privacy-preserving data storage and retrieval—especially advantageous in emergencies—and auditability to avert the abuse of health data. Additionally, a method described in [18] used privacy-conscious anomaly identification techniques. These emphasize the protection of health data by detecting anomalous trends and safeguarding individual privacy, hence preserving the confidentiality and integrity of sensitive health information [18].

3. Internet of Things

The Internet of Things (IoT) has the capacity to revolutionize healthcare via the facilitation of data gathering and transmission from diverse devices and sensors. IoT devices use inherent security mechanisms, such as encryption and authentication, to safeguard data during transmission and storage, while ensuring access is limited to authorized individuals. IoT devices may store and organize medical data, facilitating access and analysis for healthcare professionals [19]. An innovative, neutral, and permissioned decentralized data layer improves data accessibility. This architecture has been used in a practical Internet of Medical Things (IoMT) application [19], adeptly managing sensitive data while safeguarding privacy and maintaining data availability without dependence on third parties. The IoT improves data security and privacy via encryption, strong authentication, and access control, guaranteeing that sensitive health data is available just to authorized individuals, thereby complicating illegal access.

IoT applications in healthcare provide advantages in cost reduction and efficiency. These applications optimize processes, diminish mistakes and waste, and lower system costs [20,21]. The emphasis in [21] was on circumventing the key escrow issue and generating a fresh session key between servers and personal digital assistants (PDAs) for further communication, hence improving cost-efficiency and security against diverse assaults. Remote monitoring facilitates reduced hospital stays and diminished readmissions, enhancing treatment results and lowering healthcare expenses [21-25]. Additionally, Yongjoh et al. [25] examines the use of an edge server to generate data authenticators for the purpose of verifying data integrity, therefore substantially decreasing computing expenses and alleviating the management responsibilities of third-party verifiers.

4. Distributed ledger technology

Comprehensive study has shown that blockchain technology provides a safe, transparent, and immutable means for storing and distributing medical data, essential for preserving patient privacy and security inside Health Information Systems (HISs). Blockchain technology functions on a decentralized network, devoid of a single authority governing the data. This method reduces the possibility of a single point of failure or a sole entity accessing critical information, hence addressing possible security concerns associated with centralized storage systems [26-28]. Furthermore, Khan et al. [28] identified that blockchain technology may address issues pertaining to interoperability, security, secrecy, privacy protection, and safe storage. Arul et al. [27] combined two decentralized technologies, the Solid ecosystem and blockchain, using solidity-based smart contracts to address security concerns, thereby offering a safe, patient-centric framework for the intricate interchange of evolving electronic health record (EHR) data.

Blockchain technology may establish secure private networks for the exclusive transmission and distribution of sensitive medical data among authorized parties [29-33]. Kim et al. [33] offers a permissioned blockchain system for the exchange and integration of electronic health record (EHR) data, using asymmetric encryption based on public key infrastructure and digital signatures to ensure the security of EHR data. This solution guarantees the preservation of patient privacy and complies with healthcare data management standards, including the access control policy set by the patient. Likewise, Dubovitskaya et al. [32] presented a privacy-preserving medical data-sharing framework that reconciles

the need for privacy with the imperative of data sharing. The research in Xu et al. [31] established a blockchain-based system including a safe data storage architecture to address cybersecurity storage issues, using private data collecting to maintain privacy and decentralizing network nodes to avert storage problems. This approach also tackles other security issues often linked to centralized systems. Moreover, blockchain technology facilitates the development of smart contracts that automate data exchange based on predetermined circumstances, guaranteeing that data is only shared with authorized entities. Accordingly, Mnyawi et al. [30] established an access control framework using smart contracts, constructed on a distributed ledger (blockchain), to safeguard the sharing of electronic medical information across diverse actors inside the smart healthcare system.

Within the realm of blockchain applications in Health Information Systems, patient autonomy is a crucial concept, enabling people to own and govern their personal health data. This empowerment is essential; nonetheless, it presents difficulties, especially when individuals are cognitively disabled or incapable of managing their data. In certain instances, the incorporation of advanced instructions or legally authorized representatives into blockchain systems might facilitate responsible data management [26]. Furthermore, the decentralized characteristics of blockchain and its cryptographic methods provide substantial protection for health data [27]. Challenges exist in sustaining uniform permissions, particularly during emergencies when rapid access to patient data is essential. Smart contracts and cryptographic keys in blockchain networks may be used to handle permissions efficiently, guaranteeing that healthcare providers have requisite access while preserving patient privacy and data integrity [30].

Moreover, the legal ramifications of using blockchain in Health Information Systems across many countries, including the possible access by the U.S. government to cloud-stored data according to U.S. law, present considerable privacy issues. Although blockchain has several advantages for healthcare data security, its incorporation into current healthcare systems requires careful consideration, ensuring compliance with standards such as HIPAA and resolving possible privacy concerns associated with decentralized data storage. This requires a careful equilibrium between technological advancement and adherence to legal and regulatory norms.

5. Cloud Computing

Cloud computing has several benefits for safeguarding the security and privacy of medical data in Health Information Systems (HISs). Healthcare firms that use cloud-based solutions get robust security measures, including encryption, access restrictions, redundancy, and compliance certifications, all designed to protect patient data [34-36]. This review's results suggest that cloud computing companies may establish effective access control systems. This encompasses multi-factor authentication and role-based access management, guaranteeing that only authorized individuals may access critical medical information, thereby augmenting security protocols [37,38].

Furthermore, cloud computing may be more economical than sustaining an on-premises IT system. This efficiency arises from the removal of costly hardware and software requirements, enabling healthcare companies to decrease expenses and enhance their overall financial performance [36]. Cloud computing enables data recovery post-disaster, hence enhancing data security and privacy. A paper referenced as [37] details a secure encryption method (SE) integrated with fragmentation and dispersion for storage purposes. This strategy aims to safeguard data even if both the key and the public segment of EHR data on the cloud are compromised. This corresponds with several studies indicating that cloud storage of EHR significantly improves security and safeguards patient data from unwanted access [38-42].

6. Alternative Technologies

Moreover, other research has investigated approaches that use diverse technologies to improve the security and privacy of medical data [43-38]. The research referenced in [48] created a hybrid security solution using the Spring Framework, services for sensitive data (TSD) as a service platform, and Hypertext Transfer Protocol (HTTP) security techniques. This solution offers safe hosting and operation of application services,

together with the collection, storage, processing, and provisioning of data. The findings indicate that the implemented digital solution successfully safeguards APIs and personal health information. Further work referenced as [41] introduces a hash-based BBS (HBBS) pseudo-random bit generator designed to guarantee data integrity and security, making it appropriate for smart health applications and telemedicine. This paper presents an encryption mechanism designed to provide strong security in the transmission of medical data. Moreover, Ref. [44] presents a safe and lightweight methodology that employs a reduced number of elliptic curve cryptography (ECC) operations alongside a physically unclonable function (PUF), so enhancing security and efficiency while minimizing computational and communication expenses. Reference [45] presents a privacy-preserving encryption method that integrates a novel data collecting technique. This approach entails partitioning patient data into three segments and distributing it across three data servers to ensure privacy.

Furthermore, Ref. [46] developed many secure and privacy-preserving subprotocols to safeguard privacy in an e-healthcare system, using a secure greedy algorithm for query performance and min-heap technology to improve efficiency. The methodology in [47] presents an architecture that enhances the dependability of data interchange among healthcare professionals by including a security layer that fosters accountability via context-aware services, hence facilitating appropriate data access for users. Reference [40] presents a secure approach for safeguarding privacy in healthcare data, particularly for illness prediction in contemporary healthcare systems. This system employs encryption for data transmission and enables authorized healthcare personnel to safely access patient information for illness prediction with a herding genetic algorithm-based deep learning neural network. Reference [43] proposes a safe, expressive, and efficient access control strategy with rapid attribute/user revocation in collaborative e-health systems, using the ordered binary decision diagram (OBDD) access structure. It associates user keys with user identities, hence establishing resilience against collusion assaults. Furthermore, Ref. [39] emphasizes a model founded on a multi-agent system that includes diverse intelligent agents, such as a user interface agent, authentication agent, connection setup agent, and connection management agent. This paradigm delivers efficient and safe e-health security services, enhancing usability and promoting effective communication between users and e-service providers.

Numerous studies have shown the correlation between safe methods for storing and distributing sensitive health information and the assurance of data security and privacy in Health Information Systems (HISs). Reference [42] introduced a safe framework using a decentralized federated learning-based convolutional neural network, private and public interplanetary file systems (IPFS), a consortium blockchain network, and smart contracts. This approach is optimal for fostering a safe and privacy-conscious atmosphere for data exchange. Research referenced as [49] used a framework for 5G-secure smart healthcare surveillance (5GSS) to provide rapid and precise detection of context-aware health scenarios, including a blockchain-based secure data sharing system and low-latency services for urgent patients.

7. Conclusions

This research examines the literature of health information systems (HISs) with respect to medical data privacy and security. It enhances current research by identifying diverse connected technologies and examining security and privacy considerations. This research underscores the need for a secure Health Information System (HIS) that fulfills corporate goals while safeguarding patient data. Health Information Systems (HISs) provide substantial advantages to healthcare organizations for the storage, retrieval, analysis, exchange, and sharing of patient health information. These systems must fulfill the requirements of patients and healthcare professionals, while ensuring the security and confidentiality of medical information. Consequently, Health Information Systems (HISs) must be developed and deployed with paramount emphasis on privacy and security. This entails using secure technology for data storage and dissemination, implementing access restrictions to limit data visibility or alteration, and instructing healthcare workers on optimal practices for patient data confidentiality and security.

This analysis has examined the notable developments and problems in health information systems (HISs),

emphasizing critical technologies such blockchain, mobile health apps, cloud computing, and secure data exchange and storage. In contemplating the future of Health Information Systems (HISs), it is essential to examine the changing dynamics of health data management systems. In this perspective, openEHR stands out as a significant framework. This assessment does not primarily concentrate on openEHR; nonetheless, its methodology for standardized data models and archetypes for electronic health records may provide possible synergies with the systems examined. Its focus on interoperability, security, and patient-centered data management corresponds with the overarching goals of improving Health Information Systems (HISs). Future study may advantageously investigate the amalgamation of openEHR with contemporary technology to meet the dynamic requirements of healthcare systems, therefore assuring a thorough and secure methodology for handling health information. The ongoing advancement of Health Information Systems necessitates flexible and innovative solutions, with openEHR emerging as a pivotal domain for future investigation and enhancement in this sector.

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. Agbo, C.C.; QMahmoud, H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. Healthcare 2019, 7, 56.
6. Mohamad Jawad, H.H.; Bin Hassan, Z.; Zaidan, B.B.; Mohammed Jawad, F.H.; Mohamed Jawad, D.H.; Alredany, W.H.D. A Systematic Literature Review of Enabling IoT in Healthcare: Motivations, Challenges, and Recommendations. Electronics 2022, 11, 3223.
7. Katarahweire, M.; Bainomugisha, E.; Mughal, K.A.; Ngubiri, J. Form-based security in mobile health data collection systems. Secur. Priv. 2021, 4, e155.
8. 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.
9. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. Egypt. Inform. J. 2021, 22, 177–183.
10. Harman, L.B.; Flite, C.A.; Bond, K. Electronic Health Records: Privacy, Confidentiality, and Security. Am. Med. Assoc. J. Ethics 2012, 14, 712–719.
11. Basil, N.N.; Solomon, A.; Chukwuyem, E.; Ekokobe, F. Health Records Database and Inherent Security Concerns: A Review of the Literature. Cureus 2022, 14, e30168.
12. Fathima Shah, W. Preserving Privacy and Security: A Comparative Study of Health Data Regulations—GDPR vs. HIPAA. Int. J. Res. Appl. Sci. Eng. Technol. 2023, 11.
13. Amato, F.; Casola, V.; Cozzolino, G.; De Benedictis, A.; Mazzocca, N.; Moscato, F. A Security and Privacy Validation Methodology for e-Health Systems. ACM Trans. Multimed. Comput. Commun. Appl. 2021, 17.
14. Joppi, R.; Bertele, V.; Vannini, T.; Garattini, S.; Banzi, R. Food and Drug Administration vs European Medicines Agency: Review times and clinical evidence on novel drugs at the time of approval. Br. J.

Clin. Pharmacol. 2020, 86, 170–174.

15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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
21. 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.
22. Shreya, S.; Chatterjee, K.; Singh, A. A smart secure healthcare monitoring system with Internet of Medical Things. Comput. Electr. Eng. 2022, 101, 107969.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. Khan, A.A.; Wagan, A.A.; Laghari, A.A.; Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. IEEE Access 2022, 10, 78887–78898.
29. 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.
30. 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.
31. 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.
32. 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.

33. Kim, H.J.; Kim, H.H.; Ku, H.; Yoo, K.D.; Lee, S.; Park, J.I.; Kim, H.J.; Kim, K.; Chung, M.K.; Lee, K.H.; et al. Smart Decentralization of Personal Health Records with Physician Apps and Helper Agents on Blockchain: Platform Design and Implementation Study. JMIR Med. Inform. 2021, 9, e26230.
34. Son, S.; Lee, J.; Kim, M.; Yu, S.; Das, A.K.; Park, Y. Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain. IEEE Access 2020, 8, 192177–192191.
35. 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.
36. 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.
37. 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.
38. Khan, F.; Reyad, O. Application of intelligent multi agent based systems for E-healthcare security. Inf. Sci. Lett. 2019, 8, 67–72.
39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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.
45. 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.
46. 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.
47. 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.
48. 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.
49. 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.

الملخص

الخلفية :إن ظهور البيانات الضخمة وأنظمة معلومات الصحة (HISs) قد أحدث ثورة في تقديم الرعاية الصحية من خلال تحسين إدارة البيانات ودعم عمليات اتخاذ القرارات السريرية. ومع ذلك، فقد قدم هذا الانتقال إلى المنصات الرقمية مخاوف كبيرة بشأن خصوصية وأمان بيانات صحة المرضى.

الطرق :يستعرض هذا البحث المنهجي الأدبي الحلول التكنولوجية المختلفة المستخدمة في أنظمة معلومات الصحة، مع التركيز على فعاليتها في حماية بيانات المرضى. يفحص الاستعراض دراسات من عدة قواعد بيانات، بما في ذلك سكوبس وبوبميد، مع تسليط الضوء على تقنيات حماية الخصوصية مثل البلوك تشين، وتطبيقات الصحة المحمولة، وإنترنت الأشياء(IoT) ، والحوسبة السحابية.

النتائج :تكشف النتائج أن هذه التقنيات تحسن الوصول إلى البيانات وكفاءة العمليات، لكنها تقدم أيضًا مخاطر أمنية مميزة، بما في ذلك الوصول غير المصرح به وخرق البيانات. وتؤكد النتائج على أهمية تطوير أطر شاملة تعطي الأولوية لخصوصية وأمان المرضى، بما يتماشى مع اللوائح مثل قانون "HIPAA" في الولايات المتحدة و "GDPR" في أوروبا.

الخاتمة :يخلص الاستعراض إلى أن تنفيذ بروتوكولات أمان متقدمة، وتدريب مستمر للموظفين، والالتزام بالمعايير التنظيمية أمر بالغ الأهمية لتعزيز ثقة المرضى وضمان سرية بيانات الصحة في عصر البيانات الضخمة.

الكلمات المفتاحية :الخصوصية، البيانات الضخمة، أنظمة معلومات الصحة، أمان البيانات، البلوك تشين