EHR Security and Privacy Aspects: A Systematic Review

Sourav Banerjee[1(✉)], Sudip Barik[1], Debashis Das[2], and Uttam Ghosh[3]

[1] Computer Science and Engineering, Kalyani Government Engineering College, Kalyani, Nadia, India
mr.sourav.banerjee@ieee.org

[2] Department of Computer Science and Engineering, Narula Institute of Technology, Kolkata, West Bengal, India

[3] Department of CS and DS, Meharry Medical College, Nashville, TN, USA

Abstract. Electronic Health Records (EHRs) have become increasingly popular in recent years, providing a convenient way to store, manage and share relevant information among healthcare providers. However, as EHRs contain sensitive personal information, ensuring their security and privacy is most important. This paper reviews the key aspects of EHR security and privacy, including authentication, access control, data encryption, auditing, and risk management. Additionally, the paper discusses the legal and ethical issues surrounding EHRs, such as patient consent, data ownership, and breaches of confidentiality. Effective implementation of security and privacy measures in EHR systems requires a multi-disciplinary approach involving healthcare providers, IT specialists, and regulatory bodies. Ultimately, the goal is to come upon a balance between protecting patient privacy and ensuring timely access to critical medical information for feature healthcare delivery.

Keywords: Electronic Healthcare · Record (EHR) · Deep Federated learning (DFL) · Deep Learning · Artificial Intelligence · Machine Learning

1 Introduction

Electronic Health Records (EHRs) have become an integral part of modern healthcare, providing a convenient way to store, manage and share patient information among healthcare providers. With the increasing adoption of EHRs, ensuring their security and privacy has become an essential Characteristic of healthcare delivery. This paper provides an overview of the key aspects of EHR privacy and security, including authentication, access control, data encryption, auditing, and risk management. Additionally, the paper discusses the legal and ethical issues surrounding EHRs, such as consent, data ownership, and breaches of confidentiality [33].

Published by Springer Nature Switzerland AG 2023
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 683, pp. 243–260, 2023.
https://doi.org/10.1007/978-3-031-45878-1_17

1.1 Importance of EHR in Modern Healthcare

EHRs contain sensitive personal information, including medical history, diagnoses, and treatments, which cybercriminals can exploit for identity theft or insurance fraud. In addition, unauthorized access to EHRs leads to serious branches of patient confidentiality, resulting in reputational damage to healthcare providers and legal repercussions. Moreover, patients have the right to control their health information, and healthcare providers are responsible for protecting that information. To protect the confidentiality, integrity, and availability of Electronic Health Records (EHRs), it is imperative to establish vigorous security and privacy protocols [39].

1.2 Key Aspects of EHR Security and Privacy

- Access Control: Access control is the process of dealing with the situation who can access EHRs and what actions they can perform. It includes authentication, authorization, and accountability. Authentication verifies the identity of the user, authorization determines what resources the user can access, and accountability ensures that the actions of the user are recorded for auditing purposes [7].
- Data Encryption: Data encryption is the process of converting plaintext data into ciphertext to prevent unauthorized access. Encryption ensures that the data is secure during transmission and storage, making it unreadable to unauthorized users [30].
- Auditing: Auditing is the process of recording and monitoring EHR access and use. Auditing helps to detect and investigate any unauthorized access, modification or disclosure of EHRs, ensuring compliance with regulatory requirements and standards [24].
- Risk Management: Risk management refers to the series of activities aimed at identifying, evaluating, and minimizing risks related to the security and privacy of electronic health records (EHRs). This involves the creation of policies and procedures to manage EHRs, training employees on how to maintain EHR security and privacy, and implementing various technical controls such as firewalls, intrusion detection systems, and prevention mechanisms. Through this process, organizations can effectively safeguard the confidentiality, integrity, and availability of their EHRs, while complying with relevant laws and regulations governing the handling of medical information [31].

1.3 Legal and Ethical Issues

The protection of Electronic Health Records (EHRs) poses significant legal and ethical challenges that demand thoughtful contemplation. Patients are entitled to manage their health information, which encompasses the ability to regulate who can retrieve it and for what reason. Conversely, healthcare providers have a responsibility to secure patients' information from being accessed or revealed

without authorization. Furthermore, healthcare providers must adhere to various regulations such as the Health Insurance Portability and Accountability Act (HIPAA) that establishes nationwide criteria for preserving the privacy and security of patient health information [17,21,31].

1.4 Motivation

EHR security and privacy are critical aspects of modern healthcare, requiring a multi-disciplinary approach that involves healthcare providers, IT specialists, and regulatory bodies. Effective implementation of security and privacy measures in EHR systems is crucial for protecting patient privacy and ensuring timely access to critical medical information for quality healthcare delivery. In conclusion, protecting EHRs requires constant attention and vigilance, and healthcare providers must remain up-to-date with the latest security and privacy measures to protect their patients' sensitive personal information.

This work is structured into several sections for clarity and organization. In Sect. 2, we will explore the role of digitalization in the healthcare sector. Section 3 will delve into the importance of ensuring the security and privacy of Electronic Health Records (EHRs) in the context of federated learning. Major challenges in this area will be analyzed in Sect. 4, followed by an examination of the current state of the art in Sect. 5. Section 6 will analyze the limitations of some existing approaches. In Sect. 7, we will propose federated learning-based solutions for ensuring security and privacy in the healthcare sector. Finally, in Sect. 8, we will discuss possible directions for future work.

2 Digital Advancements in Healthcare

Digital technology has become more and more important in healthcare innovation and has introduced several tools and methods for improving healthcare services. These measures consist of maintaining secure storage of patient information in a centralized location and implementing software that enhances the availability of health-related data for patients. However, the digitization of healthcare is still in its early stages, and several multidimensional problems need to be addressed.

Healthcare organizations are adopting digital technologies to improve performance and efficiency, save costs, and increase efficacy. This trend is fueled by the availability of cost-effective and energy-efficient equipment and software, as well as the success of high-profile projects in many countries. Digital health systems can be especially beneficial in low-income countries, helping organizations achieve cost savings and improve healthcare delivery, which is critical in the time-reactive nature of healthcare.

A periodic survey is carried out by the World Health Organization (WHO) to gather information on the scope and structure of healthcare digitization across different countries. However, a recent report on digital healthcare innovation

in France indicates that the integration of innovation is still lacking, which is preventing the expansion of healthcare digitization in the country.

Expanding the scope of National Health Service (NHS) mobile health services is of paramount importance, given that a significant number of such services are currently restricted to limited pilot studies and have yet to achieve widespread adoption. The integration of technology in healthcare has both advantages and disadvantages. On one hand, it promotes innovation in health services and administrative processes, leading to reduced healthcare costs and improved efficiency in both internal and inter-hospital services [23]. On the other hand, there are multidimensional challenges that must be addressed, such as cybersecurity risks, inadequate integration of innovation, and infrastructure issues. Some factors influencing Digital Health are shown below in Fig. 1.

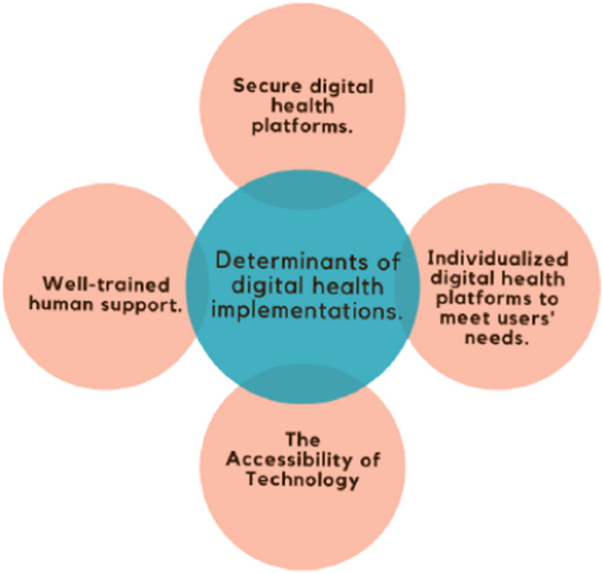

Fig. 1. The Key Factors Influencing Digital Health.

According to researchers, the integration of technologies in healthcare has both positive and negative sides. On the positive side, it promotes novel health services and streamlined administrative processes, leading to decreased healthcare costs and increased efficiency of both internal and inter-hospital services [3]. However, some challenges must be addressed, such as understanding the social barriers that may arise, including conflicts with hospital strategies and medical staff's behaviour. In addition, there is a significant of technical risk associated with information security.

Table 1 outlines the security goals that are paramount in the healthcare sector, which primarily revolve around protecting patient data, guaranteeing the

privacy and confidentiality of sensitive information, and upholding the availability and integrity of healthcare systems [16].

Table 1. Some solutions to enhance privacy and security in the healthcare sector.

Security objective	Description	Techniques
Availability	Authorized users can always access healthcare systems, even in situations where failures or attacks occur	For modern computing architecture, distributed storage, virtualization, and data backup/recovery are essential
Confidentiality	Only authorised healthcare personnel have access to patient information	Virtual private networks and encryption
Privacy	Ensure that only authorized individuals have access and safeguard against any breaches of personal data	The processes of rendering data anonymous, using pseudonyms, and encrypting it
Integrity	Ensuring that patient information is not altered without authorization	Digital signatures, hash functions, data checksums, version control, audit trails
Authentication	The authentication of users and their access to healthcare is crucial matter in preventing unauthorized entry to patients' confidential information	Passwords, two-factor authentication, biometrics, smart cards, tokens, certificates, and PKI are examples of popular authentication techniques
Authorization	Regulating the availability of patient data by considering a user's position and duties within the healthcare institution	Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Access Control Lists (ACL), OAuth
Nonrepudiation	The prohibition of denial of participation in acts such as changing patient information and accessing private data supports healthcare accountability	Blockchain and Digital signatures

3 The Need for EHR Security and Privacy in Federated Learning

Federated Learning (FL) is a technique for machine learning that enables multiple organizations to collaborate on a model without compromising the privacy of their sensitive data. This approach is decentralized and allows the participants to train the model locally while sharing only the necessary information with the central server. However, Electronic Health Records (EHRs) contain sensitive personal information that can be exploited by malicious actors if not adequately protected. Therefore, ensuring the security and privacy of EHRs in FL is critical to protect patient privacy and maintaining public trust.

EHRs typically contain sensitive information, such as patient names, addresses, social security numbers, medical histories, and other personal health information. This information is highly valuable and can be used by malicious

actors for identity theft, insurance fraud, and other criminal activities. Moreover, the unauthorized disclosure or misuse of EHRs can harm patients' reputations, cause emotional distress, and lead to physical harm.

In FL, multiple institutions collaborate on a machine learning model without sharing their sensitive data. This collaborative approach can provide significant benefits, such as improved accuracy, reduced bias, and faster model training. However, it also introduces new security and privacy risks, such as data breaches, data poisoning attacks, and model inversion attacks.

Therefore, it is critical to ensure the security and privacy of EHRs in FL to protect patients' sensitive personal information. This requires implementing robust security and privacy measures, such as access control, data encryption, auditing, and risk management. Additionally, participants in FL must comply with various regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), which sets national standards for protecting the privacy and security of patient's health information.

In summary, protecting EHRs in FL is essential to maintain public trust, protect patient privacy, and comply with regulatory requirements. Healthcare providers, data scientists, and regulatory bodies must work together to implement effective security and privacy measures to protect patient's sensitive personal information [8,35].

3.1 Federated Learning

Federated learning provides a secure and privacy-focused approach for distributed machine learning models among different devices in the context of the Internet of Medical Things (IoMT). To leverage the benefits of federated learning in the IoMT, it is essential to establish a connection between the devices with sensors and other data-generating components and a central server. After collecting data from the devices, the server uses it to train a machine-learning model. This model is then sent back to each device for further use. The local storage of data ensures its safety against potential data breaches, while predictions can be made using the trained model. The general architecture of FL is illustrated in Fig. 2. This allows medical professionals to benefit from IoMT insights without compromising patient privacy. The utilization of federated learning to combine data from various devices can have a substantial impact on enhancing prediction accuracy and yielding better outcomes in the healthcare domain.

The healthcare industry has been slow to adapt to the digital advancements seen in other fields, but various digital developments are now causing significant changes. Figure 3 demonstrates the practical application of a Federated Learning architecture within a healthcare context. The trend towards digitization and real value in healthcare is being propelled by various factors, including the proliferation of digital firms, the cost management initiatives of payers, and the growing demand for improved care among elderly patients. By adopting digital transformation, healthcare providers can improve their services and reduce costs, leading to macroeconomic disruption and improved business models. Furthermore, established companies can team up with newer firms to minimize investment

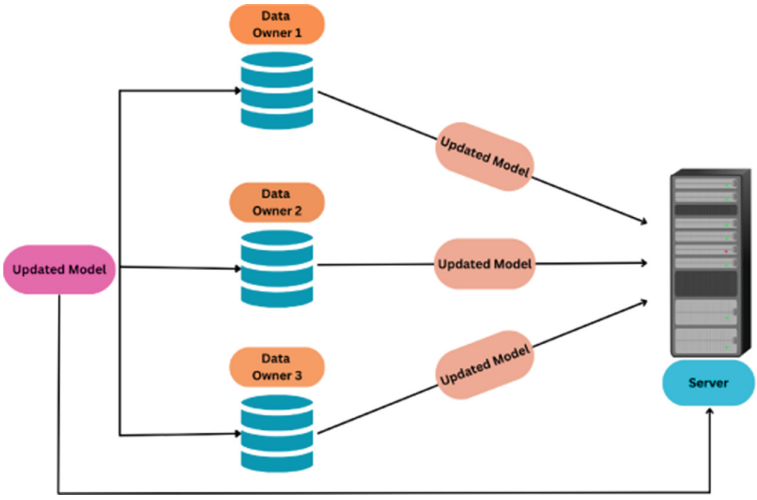

Fig. 2. General Architecture of Federated Learning

expenses. According to the authors referenced in [5], established organizations' expertise, when combined with proper regulations, can assist startups in digitally disrupting the healthcare industry.

Digitalization has the potential to enhance healthcare outcomes while also reducing costs. The capacity to process large amounts of varied data quickly and with flexibility is a key advantage of digital technologies. However, to fully leverage these benefits, data warehouses, and cloud-based data management technologies must be employed. Although data warehouses are still prevalent in health IT, they may not be sufficient for utilizing big data. To utilize big data efficiently, it is essential to have appropriate IT infrastructure, visualization techniques, workflows, user interfaces, and tools. Moreover, big data must be employed in a manner that balances societal benefits with patient privacy, in order to create value for healthcare. In order to make optimal use of big data in healthcare, institutions need to be ready to elaborate modifications in their database utilization, accessibility, sharing, privacy measures, sustainability practices, and compliance requirements [26,37].

4 Major Challenges

Healthcare organizations worldwide are embracing Electronic Health Records (EHRs), which are digital versions of a patient's medical history. However, EHRs also pose significant security and privacy challenges, some of which are:

Unauthorized access: EHRs contain sensitive patient information, such as medical history, social security number, and insurance details. Unauthorized access to this information by individuals can result in identity theft or fraud.

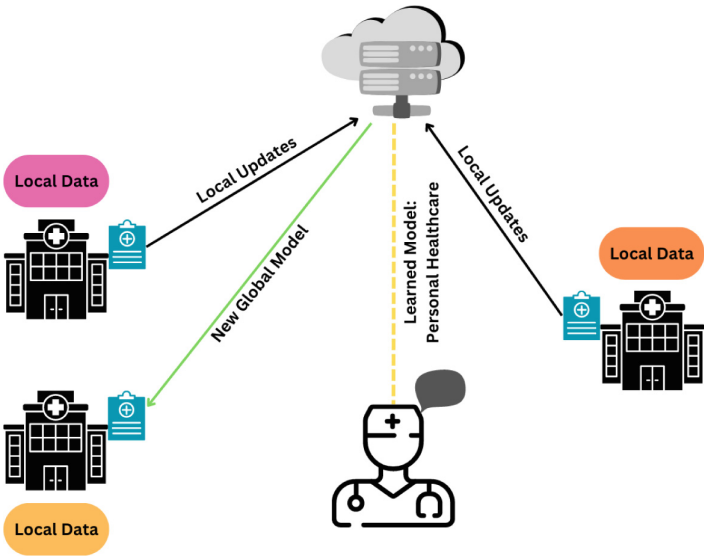

Fig. 3. Federated Learning used in healthcare industry

Cybersecurity threats: Healthcare institutions are a prime target for cybercriminals as they contain sensitive and valuable patient information in electronic health records (EHRs). Cyber threats such as malware, phishing attacks, and ransomware can jeopardize the security of EHRs, potentially resulting in data breaches. Such data breaches can lead to significant harm to patients, including identity theft, fraud, and medical identity theft. Therefore, healthcare organizations must prioritize cybersecurity measures to safeguard patient data and ensure the confidentiality, integrity, and availability of their EHRs.

Human error: EHRs can be misused, intentionally or unintentionally, by authorized users, resulting in the exposure of sensitive information. For example, a healthcare worker may accidentally upload a patient's medical record to a public-facing website.

Interoperability: EHRs may need to be shared between different healthcare providers to facilitate patient care. However, sharing EHRs between organizations can increase the risk of unauthorized access, data breaches, and privacy violations.

Legal compliance: EHRs must comply with numerous regulations and laws, including HIPAA, GDPR, and others. Healthcare organizations must ensure that they are compliant with all applicable regulations, which can be challenging, given the complexity of the regulations and the frequency of updates.

Patient consent and control: Patients must be given control over their health information, including the right to access, modify, and delete their data. Ensuring that patients are fully informed and have given their informed consent to the

use and sharing of their data can be challenging, especially given the complexity of the healthcare system and the varied interests of different stakeholders.

5 State of the Art

Electronic Health Record (EHR) security and privacy are critical aspects that need to be addressed to protect patient health information. Here are some of the state-of-the-art measures that are being implemented to ensure EHR security and privacy:

Access control: EHR systems use access control mechanisms to ensure that only authorized personnel can access patient health information. These mechanisms include password-protected logins, two-factor authentication, and role-based access controls [7].

Encryption: Encryption is used to protect data stored in EHR systems, making it unreadable to unauthorized users. Encryption can be applied to data both in transit and at rest.

Audit trails: EHR systems maintain an audit trail of all access and modifications to patient health information. This allows organizations to track who has accessed the information and when, and to detect any unauthorized access or modifications.

Data backup and recovery: Electronic health record (EHR) systems are crucial in maintaining patient health information, and backups of this data are regularly created to safeguard against system failure or cyberattacks. These backups serve as a failsafe mechanism and are frequently tested to guarantee their efficiency in restoring data. In case of a disaster, EHR backups can be relied upon to restore vital information, ensuring continuity of care and patient safety.

Data minimization: EHR systems implement data minimization principles, meaning that they collect only the minimum amount of information necessary to provide patient care. This helps reduce the risk of data breaches and protects patient privacy.

Regular vulnerability assessments: EHR systems undergo regular vulnerability assessments to identify and address potential security weaknesses. This helps prevent security breaches and ensures that the EHR system remains secure over time.

Employee training and awareness: EHR systems implement training and awareness programs to ensure that employees are aware of the security and privacy policies and procedures. This helps prevent accidental breaches of patient health information.

Compliance with regulations: EHR systems comply with relevant regulations and standards, such as HIPAA and GDPR. This ensures that patient health information is protected and that organizations are not subject to legal or financial penalties.

So EHR security and privacy are essential components of healthcare IT systems, and these state-of-the-art measures are crucial to ensuring that patient health information is protected from unauthorized access, use, and disclosure.

6 Limitations of Some Existing Work

While there has been significant research on EHR security and privacy, there are several limitations to existing research, including:

Limited scope: Much of the existing research has focused on specific aspects of EHR security and privacy, such as access control or data encryption. However, EHR security and privacy are complex issues that require a holistic approach.

Lack of real-world data: Many studies rely on simulated data or hypothetical scenarios, which may not reflect real-world threats and vulnerabilities.

Small sample sizes: Some studies have small sample sizes, making it difficult to generalize findings to larger populations.

Limited diversity: Many studies have focused on healthcare organizations in developed countries, which may not reflect the challenges faced by organizations in developing countries or underserved communities.

Outdated technology: Some research may be based on outdated EHR systems or security protocols, which may not reflect the current state-of-the-art in EHR security and privacy.

Limited longitudinal data: There is a lack of long-term studies on the effectiveness of EHR security and privacy measures. It is essential to evaluate the long-term effectiveness of these measures to ensure that they continue to provide adequate protection against evolving threats.

Lack of standardized evaluation methods: There is a lack of standardized methods for evaluating EHR security and privacy. This makes it difficult to compare findings across studies and to establish best practices for EHR security and privacy.

So, while existing research has provided valuable insights into EHR security and privacy, there is a need for more comprehensive, real-world studies that can help healthcare organizations better understand and address the challenges they face in protecting all patient health information. A few works have been carried out on this EHR security and privacy issues which are mentioned in Table 2.

Table 2. Some solutions to enhance privacy and security in the healthcare sector.

Cite	Network Model	Method	Security Models	Advantage	Limitations
[15] 2020	IOMT	Blockchain-based solution	anonymous and untraceable	Health records are safely kept on a tamper-proof blockchain that is managed by cloud servers	Advanced encryption and decryption techniques are employed as part of the protocol
[25] 2020	Internet of Health Things	Federated Learning	Data privacy	Federated learning and differential privacy address privacy and security concerns	A full decentralisation of FL is impossible due to the federated nodes' limited training capacity
[28] 2022	The network architecture comprises patients, telecare servers, and the registration centre	Elliptic Curve Cryptography	Patient Anonymity	Insiders, privileged individuals, and thieves using stolen equipment cannot attack the protocol	Compared to other protocols, the protocol's cryptography techniques use more energy
[36] 2022	Medical monitoring system based on RFID	The encryption process utilizes a combination of cyclic shifting and XOR operations	RFID security authentication	Medical monitoring systems with RFID technology guarantee the privacy and confidentiality of patient records	Designing an efficient and effective authentication protocol is challenging due to the resource constraint imposed by RFID tags/readers
[18] 2022	IoMT-based cloud-healthcare infrastructure	Elliptic curve cryptography	Patient anonymity	According to the comparative analysis, RAPCHI has shown better effectiveness than other protocols	The absence of practical application
[38] 2022	Wireless Medical Sensor Network	Blockchain-based solution	Anonymity and Untraceability	The utilization of smart contracts and PUF in the suggested approach offers both decentralization and security	There is no indication in the paper regarding the practicality of implementing the proposed approach in an actual real-life situation
[6] 2022	Internet of Health Things	An Authentication Protocol with Minimal Overhead	Mutual authentication	The process includes biometric measures for user anonymity, authentication, key negotiation, privacy, and access control	The procedure requires intricate techniques for encrypting and decrypting data

(*continued*)

Table 2. (*continued*)

Cite	Network Model	Method	Security Models	Advantage	Limitations
[2] 2022	IoT-based healthcare	Homomorphic Encryption	Privacy-preserving	By utilizing data aggregation, the EPPADA scheme aims to decrease energy usage by eliminating unnecessary data	The plan entails utilizing intricate techniques for encrypting and decrypting data
[1] 2022	Utilizing an IoT network for remote patient monitoring	A solution based on Elliptic Curve Cryptography	Privacy-preserving	The suggested RPM system provides secure authentication via RFID, ensures secure communication, and protects privacy	Challenges with dependability, restricted availability, and expensive communication
[34] 2023	Smart healthcare systems	Federated Learning	Privacy-preserving	FRESH uses certificate ring signatures as a source inference attack (SIA) defence	The system being considered is susceptible to attacks through adversarial machine learning techniques
[13] 2023	Smart healthcare utilizing the Internet of Things technology	Cryptographic primitives designed for low computational and memory requirements are commonly referred to as lightweight	Privacy-preserving	The effectiveness of the proposed authentication technique is evaluated through security and performance analysis in comparison to established and widely-used schemes	Challenges of dependability, restricted availability, and expensive communication.
[4] 2023	Internet of Things (IoT) network for healthcare	Data aggregation	Privacy-preserving	Compared to traditional methods, it lowers both the expense of communication and computation	The absence of practical application in actual situations
[29] 2023	A financial system for smart healthcare utilizing the Internet of Things	Blockchain-based solution	Data privacy	The suggested solution protects user data privacy and enables information sharing across devices using blockchain and zero-knowledge evidence	The inherent properties of blockchain technology may impose limitations on the system's ability to scale

7 Federated Learning Based Security and Privacy Solutions for the Healthcare Sector

In their research, Rahman et al. [25] suggested the use of the Internet of Health Things (IoHT) for managing health, while emphasizing the importance of protecting privacy through secure data management. They identified a lack of training capabilities and trust management as key challenges to IoHT adoption and proposed a hybrid federated learning framework that incorporates blockchain smart contracts to manage trust and authentication among federated nodes.

The framework ensures encryption and anonymity of IoHT data using differential privacy (DP) and was evaluated for COVID-19 patient data using deep learning applications, showing potential for widespread adoption.

Wang et al. [34] proposed a smart healthcare framework, known as FRESH, that aims to facilitate the sharing of physiological data while ensuring data privacy. This framework leverages Federated Learning (FL) and ring signature defence to protect against source inference attacks (SIAs).

The data collection process for FRESH involves gathering data from wearable devices and processing it using edge computing devices for local training of machine learning models. The model parameters are subsequently uploaded to the central server for joint training. The authors utilized ring signature technology to hide the source of parameter updates, which significantly reduces the success rate of SIAs. They also introduced a batch verification algorithm to improve the efficiency of signature verification.

According to the authors, FRESH is highly suitable for large-scale smart healthcare systems that cater to multiple users. This framework represents a major milestone in the quest to enhance data privacy and security in the healthcare industry.

8 Future Works

8.1 Advancing Privacy and Security in the Healthcare Industry: The Need for Further Study

The healthcare industry regards the privacy and security of patient data as essential issues, and continuous investigation is imperative to enhance current protocols and confront evolving obstacles. A potential research direction could be to investigate the effectiveness of current privacy and security regulations, such as HIPAA and GDPR, in protecting patient information. This research could examine the gaps and limitations in the existing regulatory framework and propose recommendations for improvements.

Another potential avenue of research is to investigate how emerging technologies like artificial intelligence and blockchain can improve privacy and security within the healthcare industry. For example, blockchain technology offers a decentralized and tamper-proof platform for storing and sharing patient information, which could reduce the risk of data breaches and ensure the accuracy of health records. Similarly, artificial intelligence can be used to detect and prevent potential security breaches and unauthorized access to patient information.

Furthermore, research could be conducted on the impact of privacy and security breaches on patient trust and healthcare outcomes. A breach of patient information can lead to a loss of trust between patients and healthcare providers, which can have long-lasting effects on patient health and well-being. Thus, understanding the effects of privacy and security breaches and developing strategies to restore patient trust could be a valuable research direction.

8.2 Study of the Impacts of Digitization on Health Outcomes

In addition to the benefits mentioned, digitization has also improved patient safety. For example, electronic prescribing (e-prescribing) has reduced medication errors by eliminating the need for handwritten prescriptions, which can be misread or contain errors. EHRs also can flag potential drug interactions or allergies, alerting healthcare providers to potential issues before they occur. The utilization of barcode scanning technology has enhanced medication safety by verifying that the correct medication is administered to the accurate patient at the appropriate time.

Digitization has also enabled better coordination of care among healthcare providers. With EHRs, providers can share patient information more easily and efficiently, ensuring that all members of the care team have access to the same information. This can help to reduce the risk of errors or duplicative testing, leading to improved patient outcomes.

However, despite the many benefits of digitization in healthcare, there are also challenges and potential drawbacks to consider. For example, there may be concerns about the security and privacy of patient information, as well as issues related to data ownership and access. Additionally, there may be concerns about the potential for technology to replace human interaction and the importance of maintaining the human touch in healthcare.

Future research in this area could focus on exploring the benefits and challenges of digitization in healthcare, as well as identifying ways to optimize the use of technology to improve patient outcomes and quality of care. This could include examining the role of patient engagement and education in promoting the adoption and effective use of digital technologies in healthcare, as well as the potential for technology to improve patient-centred care and promote better health results.

8.3 An Evaluation of Artificial Intelligence's Role in Healthcare

AI is transforming healthcare by leveraging natural language processing, virtual assistants, and AI-powered chatbots as well as AI-powered imaging analysis and diagnostic tools, among other technologies, to enhance patient outcomes. AI-powered healthcare solutions have the potential to significantly reduce healthcare costs, increase efficiency, and improve patient outcomes by providing faster and more accurate diagnoses, personalized treatment recommendations, and improved patient communication and engagement. However, it's important to note that while AI has the potential to revolutionize healthcare, it's important to ensure that these systems are developed ethically and that patient privacy is protected.

8.4 The Significance of Patient Engagement in Ensuring Security and Privacy

In the healthcare industry, ensuring privacy and security heavily relies on patient engagement as a crucial factor. When patients are engaged in their healthcare,

they are more likely to be aware of the risks associated with the use of personal health information and are more likely to take steps to protect it. Healthcare providers can encourage patient engagement by providing clear and concise information about privacy and security policies, as well as by offering patient education resources, such as online portals, educational videos, and other materials. Healthcare providers can promote patient privacy and security, as well as enable informed decision-making regarding healthcare, by actively engaging patients in safeguarding their personal information [20,22,32].

8.5 Exploring the Potential of Blockchain Technology in Healthcare

The healthcare sector has the prospect of a significant transformation through the adoption of blockchain technology, as it offers secure and transparent means for storing and exchanging patient information. Blockchain's distributed ledger technology can ensure that patient data is protected from unauthorized access, while also allowing for the efficient sharing of that data among healthcare providers. The use of blockchain technology for electronic medical records can also reduce errors, streamline workflows, and increase the accuracy of medical data [14,19].

By utilizing blockchain technology, smart contracts can automate and simplify the procedure of insurance claims and reimbursements for both patients and insurance companies. By reducing the time and costs associated with traditional payment processing systems, blockchain-based smart contracts can help to reduce healthcare costs and improve patient outcomes [12,27].

Blockchain technology can leverage the healthcare industry to facilitate supply chain management via vehicular communication [9] securely, enabling the verification and traceability of medical devices and drugs to ensure their genuineness. This can improve patient safety by reducing the risk of counterfeit products, and can also help to improve supply chain efficiency and transparency [10,11].

9 Future Scope and Advancements

Digitalization, including IoMT (Internet of Medical Things) and blockchain technology, offers significant opportunities and advantages to the healthcare sector. However, successful implementation requires careful consideration of social, organizational, and collaborative aspects. Fostering a positive attitude and providing necessary support enable healthcare organizations to adopt digital technologies, improving patient care and cost savings while addressing potential difficulties and constraints. Future work aims to enhance Electronic Health Record (EHR) security through novel approaches, leveraging IoMT and blockchain technology for concise and secure record-keeping in electronic mode.

10 Conclusion

In conclusion, digitalization offers significant opportunities and advantages to the healthcare sector, but its implementation requires careful consideration of the social, organizational, and collaborative aspects of the workplace. Even if digitization can enhance healthcare performance and accomplish strategic goals, it is crucial to be aware of potential difficulties and constraints. By focusing on a positive attitude and providing necessary support, healthcare organizations can successfully adopt digital technologies and streamline their procedures, resulting in improved patient care and cost savings.

Acknowledgement. This work was supported by the National Science Foundation, under award number 2219741.

References

1. Ahmed, M.I., Kannan, G.: Secure and lightweight privacy preserving internet of things integration for remote patient monitoring. J. King Saud Univ.-Comput. Inform. Sci. **34**(9), 6895–6908 (2022)
2. Alam, M.A., Al Riyami, K.: Shear strengthening of reinforced concrete beam using natural fibre reinforced polymer laminates. Constr. Build. Mater. **162**, 683–696 (2018)
3. Alloghani, M., Al-Jumeily, D., Hussain, A., Aljaaf, A.J., Mustafina, J., Petrov, E.: Healthcare services innovations based on the state of the art technology trend industry 4.0. In: 2018 11th International Conference on Developments in eSystems Engineering (DeSE), pp. 64–70. IEEE (2018)
4. Bhowmik, T., Banerjee, I.: Eeppda-edge-enabled efficient privacy-preserving data aggregation in smart healthcare internet of things network. Inter. J. Network Manag. e2216 (2023)
5. Chae, B.: Mapping the evolution of digital business research: a bibliometric review. Sustainability **14**(12), 6990 (2022)
6. Chen, C.M., Chen, Z., Kumari, S., Lin, M.C.: Lap-ioht: a lightweight authentication protocol for the internet of health things. Sensors **22**(14), 5401 (2022)
7. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Urban Areas **39**, 283–297 (2018)
8. Dang, T.K., Lan, X., Weng, J., Feng, M.: Federated learning for electronic health records. ACM Trans. Intell. Syst. Technol. (TIST) **13**(5), 1–17 (2022)
9. Das, D., Banerjee, S., Chatterjee, P., Ghosh, U., Biswas, U.: A secure blockchain enabled v2v communication system using smart contracts. IEEE Trans. Intell. Trans. Syst. (2022)
10. Das, D., Banerjee, S., Chatterjee, P., Ghosh, U., Mansoor, W., Biswas, U.: Design of a blockchain enabled secure vehicle-to-vehicle communication system. In: 2021 4th International Conference on Signal Processing and Information Security (ICSPIS), pp. 29–32. IEEE (2021)
11. Das, D., Banerjee, S., Chatterjee, P., Ghosh, U., Mansoor, W., Biswas, U.: Design of an automated blockchain-enabled vehicle data management system. In: 2022 5th International Conference on Signal Processing and Information Security (ICSPIS), pp. 22–25. IEEE (2022)

12. Das, D., Banerjee, S., Dasgupta, K., Chatterjee, P., Ghosh, U., Biswas, U.: Blockchain enabled sdn framework for security management in 5g applications. In: 24th International Conference on Distributed Computing and Networking, pp. 414–419 (2023)
13. Das, S., Namasudra, S.: Lightweight and efficient scpprivacy-preserving/scp mutual authentication scheme to secure scpinternet of things/scp-based smart healthcare. Trans. Emerging Telecommun. Technol. (2023)
14. Dutta, K., Guin, R.B., Chakrabarti, S., Banerjee, S., Biswas, U.: A smart job scheduling system for cloud computing service providers and users: modeling and simulation. In: 2012 1st international conference on recent advances in information technology (rait), pp. 346–351. IEEE (2012)
15. Garg, N., Wazid, M., Das, A.K., Singh, D.P., Rodrigues, J.J., Park, Y.: Bakmp-iomt: design of blockchain enabled authenticated key management protocol for internet of medical things deployment. IEEE Access **8**, 95956–95977 (2020)
16. Herrmann, M., Boehme, P., Mondritzki, T., Ehlers, J.P., Kavadias, S., Truebel, H.: Digital transformation and disruption of the health care sector: Internet-based observational study. J. Med. Internet Res. **20**(3), e104 (2018)
17. Kigera, J., Kipkorir, V.: Electronic health records-the ethical and legal issues. Annals African Surgery **20**(1), 1–2 (2023)
18. Kumar, V., Mahmoud, M.S., Alkhayyat, A., Srinivas, J., Ahmad, M., Kumari, A.: Rapchi: robust authentication protocol for iomt-based cloud-healthcare infrastructure. J. Supercomput. **78**(14), 16167–16196 (2022)
19. Lahiri, P.K., Das, D., Mansoor, W., Banerjee, S., Chatterjee, P.: A trustworthy blockchain based framework for impregnable iov in edge computing. In: 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pp. 26–31. IEEE (2020)
20. Lahiri, P.K., Mandal, R., Banerjee, S., Biswas, U.: An approach towards developments of smart covid-19 patient's management and triaging using blockchain framework (2020)
21. Li, H., et al.: Review on security of federated learning and its application in healthcare. Futur. Gener. Comput. Syst. **144**, 271–290 (2023)
22. Mandal, R., Banerjee, S., Islam, M.B., Chatterjee, P., Biswas, U.: Qos and energy efficiency using green cloud computing. In: Intelligent Internet of Things for Healthcare and Industry, pp. 287–305. Springer (2022). https://doi.org/10.1007/978-3-030-81473-1_14
23. Manogaran, G., Thota, C., Lopez, D., Sundarasekar, R.: Big data security intelligence for healthcare industry 4.0. Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing, pp. 103–126 (2017)
24. Parker, M.: Managing threats to health data and information: toward security. In: Health Information Exchange, pp. 149–196. Elsevier (2023)
25. Rahman, M.A., Hossain, M.S., Islam, M.S., Alrajeh, N.A., Muhammad, G.: Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. IEEE Access **8**, 205071–205087 (2020)
26. Roski, J., Bo-Linn, G.W., Andrews, T.A.: Creating value in health care through big data: opportunities and policy implications. Health Aff. **33**(7), 1115–1122 (2014)
27. Roy, R., Haldar, P., Das, D., Banerjee, S., Biswas, U.: A blockchain enabled trusted public distribution management system using smart contract. In: International Conference on Electronic Governance with Emerging Technologies, pp. 25–35. Springer (2022). https://doi.org/10.1007/978-3-031-22950-3_3
28. Ryu, J., et al.: Secure ecc-based three-factor mutual authentication protocol for telecare medical information system. IEEE Access **10**, 11511–11526 (2022)

29. Singh, R., Dwivedi, A.D., Srivastava, G., Chatterjee, P., Lin, J.C.W.: A privacy preserving internet of things smart healthcare financial system. IEEE Internet of Things J. (2023)
30. Sonkamble, R.G., Bongale, A.M., Phansalkar, S., Sharma, A., Rajput, S.: Secure data transmission of electronic health records using blockchain technology. Electronics **12**(4), 1015 (2023)
31. Tertulino, R., Antunes, N., Morais, H.: Privacy in electronic health records: a systematic mapping study. J. Public Health, 1–20 (2023)
32. Tiwari, S., et al.: Applications of machine learning approaches to combat covid-19: a survey. In: Lessons from COVID-19, pp. 263–287 (2022)
33. Wang, S., Kirillova, K., Lehto, X.: Travelers' food experience sharing on social network sites. J. Travel Tourism Market. **34**(5), 680–693 (2017)
34. Wang, W., Li, X., Qiu, X., Zhang, X., Zhao, J., Brusic, V.: A privacy preserving framework for federated learning in smart healthcare systems. Inform. Proc. Manag. **60**(1), 103167 (2023)
35. Xu, J., Glicksberg, B.S., Su, C., Walker, P., Bian, J., Wang, F.: Federated learning for healthcare informatics. J. Healthcare Inform. Res. **5**, 1–19 (2021)
36. Yang, C., Everitt, J.H., Murden, D.: Evaluating high resolution spot 5 satellite imagery for crop identification. Comput. Electron. Agric. **75**(2), 347–354 (2011)
37. Yin, X., Zhu, Y., Hu, J.: A comprehensive survey of privacy-preserving federated learning: a taxonomy, review, and future directions. ACM Comput. Surv. (CSUR) **54**(6), 1–36 (2021)
38. Yu, S., Park, Y.: A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions. IEEE Internet Things J. **9**(20), 20214–20228 (2022). https://doi.org/10.1109/JIOT.2022.3171791
39. Zhao, Y., et al.: Growth traits and sperm proteomics analyses of myostatin gene-edited Chinese yellow cattle. Life **12**(5), 627 (2022)