Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Secure e-health framework using artificial intelligence and blockchain technology

Reham Almukhlifi [1], Mahmoud Ahmad Al-Khasawneh [2, 3, *], Amal Abdullah Bukhari [4], Ahmad Ali Ahmad Harasis [5]

[1]*Department of Computer Science, College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia*
[2]*School of Computing, Skyline University College, University City Sharjah, 1797, Sharjah, UAE*
[3]*Applied Science Research Center, Applied Science Private University, Amman, Jordan*
[4]*College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia*
[5]*Business Management Department, Faculty of Business, Middle East University, Amman, Jordan*

ARTICLE INFO

Article history:
Received 17 May 2024
Received in revised form
3 November 2024
Accepted 19 January 2025

Keywords:
Blockchain technology
Artificial intelligence
E-health framework
Healthcare efficiency
Data security

ABSTRACT

This review explores emerging technologies in the healthcare sector, specifically focusing on blockchain and artificial intelligence (AI). Data on healthcare trends were gathered from documents published on the Web of Sciences and various Google surveys conducted by different governing bodies. The review aims to examine the potential of integrating blockchain and AI to enhance healthcare by promoting the use of generalizable analytical technologies that can be integrated into comprehensive risk management strategies. This article discusses how blockchain can be utilized as an open network for sharing and authorizing information, which creates opportunities for developing reliable AI models for e-health. AI, using various algorithms and decision-making capabilities, can help healthcare professionals access patient medical records stored on the blockchain. This integration is expected to improve the efficiency of the medical system, reduce costs, and democratize healthcare delivery by incorporating the latest technological advances. Cryptographic records stored on blockchains are essential for AI to securely manage information. The main goal of this article is to develop a secure e-health framework using AI and blockchain technology, referred to as SEHFUAIBC. The design science methodology (DSM) was used in this study. The SEHFUAIBC framework includes seven components: advanced encryption algorithms, access control, multi-factor authentication, AI-based threat detection, blockchain-based data sharing, privacy protection, and audit trail. The framework was evaluated using real-world scenarios, and the results show that the combination of AI and blockchain in this framework provides hybrid security techniques that are crucial for protecting e-health records from unauthorized access.

1. Introduction

Assert that health informatics techniques are typically based on a sequence of conditional steps that can be visualized as a series of repeated patient-care activities in the context of budgeting, personnel, patients, legal disputes, logistics, supplies, and other procedures and medical workflows (Alotaibi and Federico, 2017). According to Chapuis et al. (2010), hospitals and others that provide healthcare should increase the level of internal controls, improve the level of performance, compliance, and consistency, and reduce the level of risk, job time, and overhead. Based on advanced healthcare blockchain research and a robust approach to healthcare management, this article outlines an advanced healthcare blockchain analysis and a robust approach to healthcare management to simplify complicated medical treatments (Campanella et al., 2016). A blockchain-based solution to healthcare management has been presented based on cutting-edge blockchain research in healthcare and we have analysed cutting-edge blockchain studies in healthcare. Governments and related sectors are becoming more involved in digitizing healthcare systems around the world, as demonstrated by numerous initiatives conducted in various countries and economies. The critical challenge to success is to

* Corresponding Author.
Email Address: mahmoud.alkhasawneh@skylineuniversity.ac.ae (M. A. Al-Khasawneh)
https://doi.org/10.21833/ijaas.2025.02.006
Corresponding author's ORCID profile:
https://orcid.org/0000-0003-1698-0237

integrate technology into the DNA of each company in a manner that utilizes blockchain, artificial intelligence, and other technologies to accomplish this (Wong et al., 2019; Bragazzi et al., 2020). According to Sahoo and Baruah (2018), to advance the field of medical research and achieve patient-centricity, technology will be utilized to facilitate user- and customer-centric interfaces and generate data-driven decisions to generate innovative data processing approaches and better results for improving the welfare of patients. By using artificial intelligence (AI), for instance, it is possible to identify and prioritize individual patients to monitor and grow their drug production. This is extremely important for managing drug production and shortening production timelines (Mak et al., 2023). Agu and Obulose (2024) used numerical drug design methods and artificial intelligence to monitor clinical trial data to repurpose marketed medications, investigate the effectiveness of medication formulations, and measure dosage using data collected in clinical. Due to the rapidly changing climate in which we are currently living, it is increasingly critical that governments identify the most effective methods by which they can leverage resources to drive reforms while ensuring the required consistency, compliance, or data protection (Siyal et al., 2019). Blockchain is an innovative solution that makes it possible to develop and manage content blocks with safe and automated data analysis in an environment where it is constantly evolving. To provide timely updates to medical experts, healthcare providers, and payers regarding the status of health-related data, all health-related data will be securely recorded and analyzed.

Moreover, Artificial Intelligence can also execute complex computations and be capable of rapidly analyzing vast quantities of patient data to help make medical decisions (Priyanka et al., 2024). The use of AI in healthcare, however, remains unpopular with some doctors, particularly when it comes to positions that could have a significant impact on a patient's well-being. I don't think there can be any argument in Favor of the use of artificial intelligence, as it has proven to be capable of executing many profound and sophisticated tasks more rapidly than a person. There is no doubt that the automotive industry can exploit artificial intelligence to deliver driverless vehicles shortly. By utilizing machine learning, other companies are already able to detect fraud or determine financial threats, allowing them to identify threats at an early stage. In terms of AI maturity level, only a few points could be indicators (Akkiraju et al., 2020).

Thus, the study aims to design a framework for a secure e-health system using artificial intelligence and blockchain technologies, which will be called SEHFUAIBC. For this study, we are using the design science methodology (DSM). As a result of SEHFUAIBC's development, seven underlying components have been developed: advanced encryption algorithms, access control, multifactor authentication, AI-based threat detection, data sharing based on blockchain, privacy protection, and audit trail checks. A real-life scenario was used to evaluate the developed SEHFUAIBC.

The rest of this article is arranged as follows: the related works are discussed in Section 2, and the methodology is presented in Section 3. The problem statement and objectives are discussed in Sections 4 and 5 respectively. The results discussion and limitations are introduced in Sections 6 and 7 separately, whereas the conclusion and future works are offered in Section 8.

2. Related works

There are some research articles and projects proposed in the literature that focus on the E-Health sector from the security perspective using Artificial Intelligence and Blockchain Technology. For example, Tagde et al. (2021) emphasized the importance of integrating generalizable analytics into a comprehensive risk management strategy, as well as how they promote a significant impact on healthcare. They demonstrated how blockchain, an open network for sharing information and authorizing it, can be used to create reliable artificial intelligence models in e-health.

Alabdulatif et al. (2023) proposed an enhanced and more secure way of protecting the learning model's decision-making process by extending the scope and security. In this study, smart contracts were used to implement the decision function of the learning model using the extracted learning parameters by reverse engineering the decision function of the learning model.

Kubendiran et al. (2019) provided a framework for implementing blockchain in e-healthcare systems to verify data integrity efficiently. Furthermore, they presented an innovative concept for ensuring data provenance, which is a crucial aspect of healthcare that needs to be addressed.

Using blockchain's unique properties, Sanjana et al. (2021) proposed a framework for implementing confidentiality, authentication, and data sharing which are all important aspects to consider when handling sensitive information, and the use of the framework has been endorsed by peers. As part of the framework for a secure e-health system, blockchain is utilized as a method of capturing electronic health records (EHR), securely storing them, and integrating IoT and fog computing infrastructure to provide secure storage and analytics.

Quasim et al. (2020) developed a secure system using blockchain technology to ensure the protection of electronic health records (EHRs). Several components have been integrated into the framework, such as sensors, the Internet of Things, databases, and other computer resources. There is a framework for securing electronic health records that will improve the security and privacy of electronic health records as compared to traditional healthcare systems.

Velliyangiri et al. (2022) developed a new approach that applies blockchain technology to health records and provides a decentralized view, improves medical accuracy, mitigates risk factors, and prevents health problems before they occur.

A blockchain-based electronic health record (BEHR) transmission between physicians and patients was introduced by Mallikarjuna et al. (2021) as an integrated approach to blockchain 4.0 technology. This reduced latency in healthcare records transmission using an IoT-based cloud environment. A Blockchain-based solution was proposed by Jennath et al. (2020) to address the security and privacy concerns that have otherwise not been addressed by current eHealth systems, to address the security and privacy concerns that currently exist. Furthermore, this study explores the possibilities of building trusted AI models over blockchain for implementation in e-health, where a platform for the sharing of consent-based data is designed to allow for transparent data collection.

A system for ensuring authentication and protecting medical records' integrity was developed by Gayathri et al. (2020), utilizing the cloud. Through the implementation of the proposed system, a keyless signature infrastructure will ensure the secrecy of digital signatures and authentication of digital signatures. Also, the proposed blockchain technology has the capability of maintaining data integrity.

A secure data dissemination scheme for IoT-based e-health systems based on IoT is proposed by Kumar et al. (2022) in the form of an artificial intelligence-based blockchain framework. An approach based on deep learning was used to detect intrusions at the edge of the network using an intrusion detection system that uses deep learning to detect intrusions. By utilizing deep learning and cryptography technologies, Veeramakali et al. (2021) have created an intelligent IoT and healthcare diagnosis model that combines deep learning with cryptography to provide secure and reliable diagnostics using deep learning. A proposed model consists of three main processes: secure transactions, hash-value encryption, and the diagnosis of medical conditions. A cryptographic framework based on blockchain technology is proposed by Ghazal et al. (2022) to provide security-based solutions that are based on a computational intelligence approach. The proposed approach can provide better results in terms of 0.93 in the training phase and 0.91 in the validation phase when it comes to training. The framework proposed by Chakraborty et al. (2019) set an excellent example for the complete supervision of a cure or a continuous treatment or generic healthcare from the onset right up to the very end of the treatment course. In the case of healthcare data research, trust and authenticity of the data are two of the primary notions that are always observed in the case of analyzing the data. A novel blockchain approach has been developed by Samad (2022) to evaluate different methods of sharing decentralized views of health information and improving medical accuracy, health, and prevention of health disorders through the use of blockchain technology in the field of eHealth. The goal of the work was to discover the benefits of blockchain technology for improving health.

Farhadighalati et al. (2023) presented the SAFE-HEALTH framework that proposes an edge computing-based model for a secure healthcare system. In addition, the author refers to the importance of the importance of security measures for identifying attacks at every level of the healthcare system and presents various potential remedies that could mitigate these vulnerabilities in the future.

Verma (2024) presented a novel blockchain technology that enables the secure storage of health data in the cloud. As a result, medical records can be authenticated in a secure environment and maintain their integrity. An improved blowfish model that guarantees the authentication of the blockchain is deployed here as a method of deploying blockchains with optimal encryption.

Jakhar et al. (2024) proposed a privacy-preserving access control framework that utilizes blockchain technology to ensure that healthcare data integrity, security, accessibility, and privacy are maintained while using consensus-driven decentralized data management through peer-to-peer distributed computing platforms.

Mourya et al. (2024) examined the use of blockchain technology and mobile agents in prediction markets and the healthcare industry. A blockchain-based system with mobile agents provides more security and durability. A resilient structure can be created by aggregating predictive outcomes from different nodes. Furthermore, mobile agents can serve as a storage platform for machine learning results.

In reviewing the existing models and frameworks developed for securing the e-health industry, we found these challenges and issues that need to be addressed which are shown in Fig. 1. Therefore, this study aims to develop a secure framework that can cope with these issues. This is done by combining modern blockchain technology with artificial intelligence.

3. Problem statement

AI and blockchain are used to collect, store, and process sensitive data, including medical records, diagnosis details, and medication history. Consequently, this information is at risk of being accessed or misused by unauthorized parties. A lack of appropriate access controls could lead to potential security and privacy breaches involving sensitive patient data.

4. Objectives of the study

The main aim of this study is to develop a secure e-health framework using artificial intelligence and blockchain technology called (SEHFUAIBC).

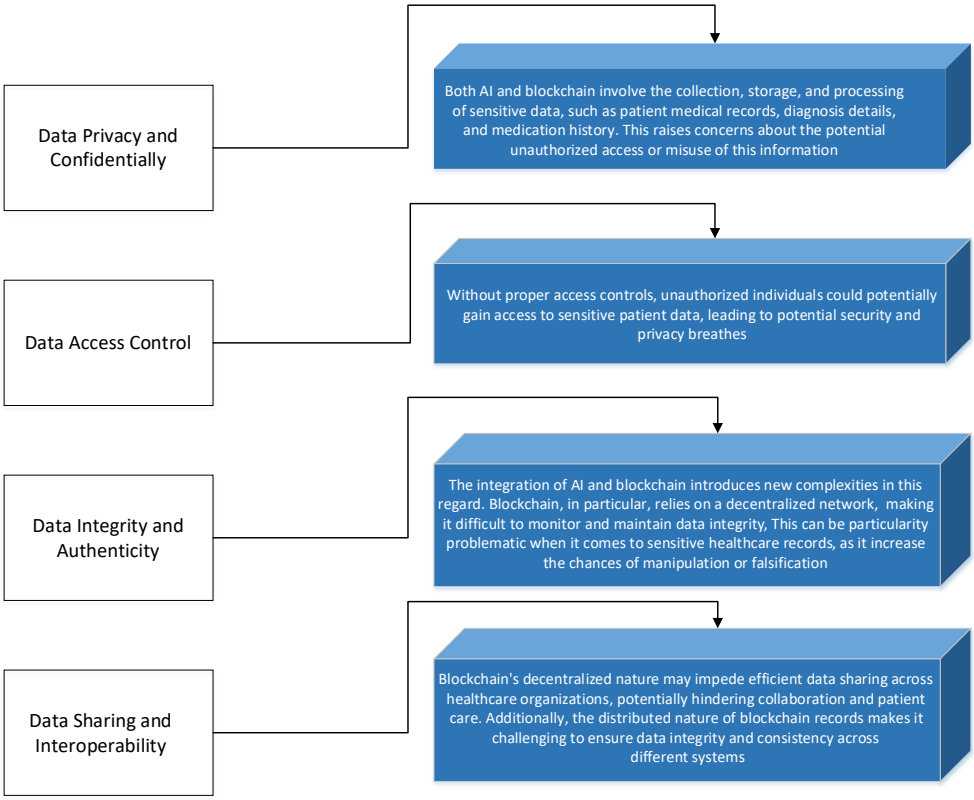

Fig. 1: Discovered challenges and issues for securing the e-health industry

5. Methodology

The DSM is applied in March and Smith (1995). It is a qualitative research approach that combines a design process to learn how an artifact is designed and how the design is constructed, which is what is known as design science research (March and Smith, 1995; Alotaibi et al., 2023; Alotaibe, 2024; Alotibi, 2024). It uses this process to learn how both the design itself and how it is constructed work together. The goal of DSR is to optimize the performance of (designed) artifacts by developing new methods and techniques that will promote their development as well as their performance (Al-Dhaqm et al., 2020). The adapted methodology consists of three stages as shown in Fig. 2.

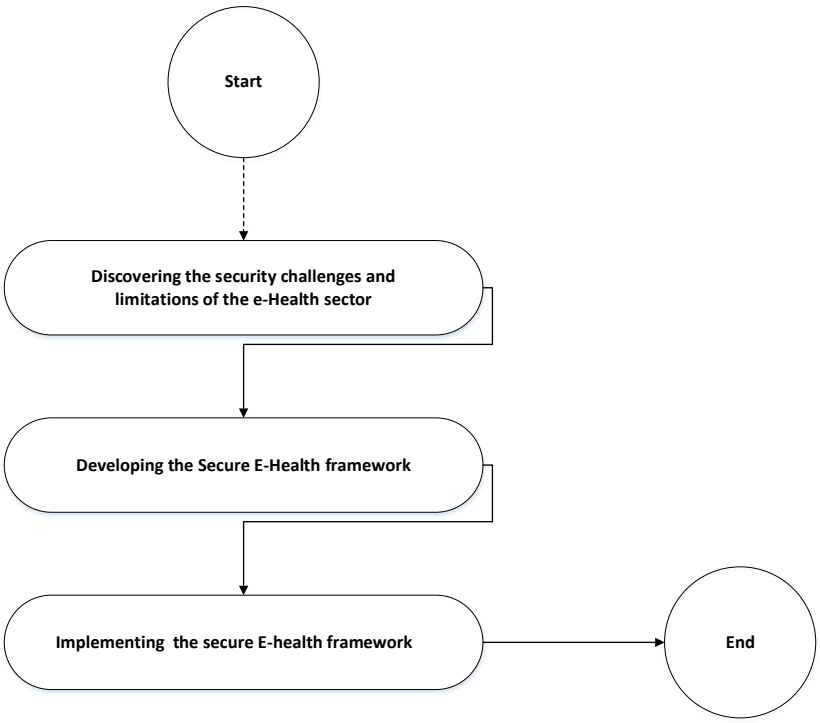

Fig. 2: Adapted methodology (March and Smith, 1995)

Stage 1: Discovering the security challenges and limitations of the e-health sector: The purpose of this step is to examine security challenges and limitations in the e-health sector. Security challenges in the e-health sector have been addressed by several models, frameworks, and approaches. Nevertheless, these models and approaches are specific and developed for different scenarios, according to the literature. Table 1 displays the challenges and contributions of the existing works for the e-Health sector.

Stage 2: Developing the Secure E-heath Framework: The goal of this stage is to develop a secure e-health framework that utilizes the power of AI and blockchain technologies to provide a quality healthcare experience. We developed the framework to provide a robust and secure platform for handling sensitive healthcare information that can manage a wide range of risks. In addition to protecting patient privacy, the secure e-health framework ensures interoperability and accessibility of data. The framework will address data breaches, unauthorized access, and limitations in interoperability caused by traditional healthcare data management systems. The secure e-health framework consists of several key components that work together to ensure the secure management of patient data as shown in Fig. 3. These components include:

- Data encryption: Encrypting health data using advanced encryption algorithms is a fundamental measure to protect patient confidentiality and prevent unauthorized access. Strong encryption ensures that sensitive medical information remains secure, helps healthcare organizations comply with regulatory requirements, and enhances overall data protection. Therefore, healthcare providers should consider data encryption a key component of their security strategy.
- Access control: Effective access control mechanisms are essential for safeguarding health data. By implementing access controls, healthcare organizations can ensure that only authorized individuals or entities can access sensitive data, thereby maintaining privacy, confidentiality, and data integrity.
- Multi-factor authentication: along with biometric authentication, it plays a crucial role in strengthening security measures. By requiring multiple verification factors, such as physiological or behavioral characteristics, MFA significantly reduces the risk of unauthorized access. Biometric authentication enhances security while offering a more user-friendly and efficient authentication process. Healthcare organizations should integrate biometric authentication into their security frameworks to protect sensitive data and maintain user trust.
- AI-Based threat Detection: AI can be utilized to detect anomalies in health data, such as unauthorized access attempts or suspicious activities, triggering immediate alerts. AI-based threat detection provides a proactive security solution by identifying potential threats before they escalate. Given the increasing complexity of cyber threats, healthcare organizations should invest in AI-driven security solutions to safeguard patient data and ensure privacy.
- Blockchain-based data sharing: Blockchain technology enables secure storage and sharing of health data by ensuring data integrity and preventing unauthorized modifications. The decentralized and immutable nature of blockchain enhances data security, facilitates collaboration among healthcare providers, and improves patient care. As blockchain technology continues to evolve, addressing implementation challenges will be essential to maximize its benefits in healthcare.
- Privacy protection: Privacy-enhancing techniques, such as data anonymization and tokenization, help protect patient privacy while allowing secure data sharing. By incorporating these techniques into healthcare data management, organizations can ensure that sensitive information remains protected while enabling authorized access when necessary.
- Audit trail: A blockchain-based audit trail allows users to track the origin and modification history of health data, ensuring transparency and accountability. This feature enhances data security and integrity, helping healthcare organizations maintain trust while improving the quality and reliability of patient care.

Stage 3: Implementing the secure E-heath framework: To implement the developed SEHFUAIBC we used the following scenario: This scenario explains how the developed SEHFUAIBC can secure the medical records of the patients. John is a 45-year-old patient who has just visited his local healthcare provider for a routine checkup. During the checkup, John's doctor accessed his medical history, including his diagnosis and treatment plans, to make informed decisions about his overall health. This data, known as health, records, contains sensitive information that is crucial for John's care and may need to be shared with various healthcare professionals and organizations. Unfortunately, during the appointment, John noticed that his medical record was not being protected adequately. Concerned about his confidentiality, he asked his doctor about the security measures in place to safeguard his data. The doctor assured John that all necessary precautions had been taken, but upon further examination, John realized that his concerns were valid. To address these issues and protect the confidentiality, integrity, privacy, and availability of the medical history of the patient the developed SEHFUAIBC is applied as shown in Fig. 4. Using advanced algorithms for encryption, access control, multifactor authentication, artificial intelligence-based threat detection, blockchain-based data sharing, privacy protection, and the use of audit trails, we can safeguard sensitive medical information and prevent it from being compromised.

Table 1: The challenges and contributions of the existing works

Reference	Security techniques	Challenges	Contributions
Tagde et al. (2021)	Blockchain technology and AI	Discussed the issues of sharing information and authorizing it, as well as how AI and blockchain can be used in the eHealth field to create reliable models of clinical diagnosis and treatment	Integrated generalizable analytics into a comprehensive risk management strategy would have a significant impact on healthcare
Alabdulatif et al. (2023)	Blockchain technology: Smart contracts	They discussed the challenges and issues that are involved in the implementation of the E-Health framework for safer decision-making	1. Incorporate blockchain and machine learning into an AI framework based on trust 2. Create immutable smart contracts that provide effective security for Support Vector Machine (SVMs) and Multi-Layer Perceptron (MLPs)
Kubendiran et al. (2019)	Blockchain technology	They discussed the challenges of maintaining data integrity efficiently in e-health records	1. Establishing an efficient framework for implementing blockchain in e-healthcare systems 2. Provided an innovative approach to ensuring the provenance of health data
Sanjana et al. (2021)	Blockchain technology	Several important issues, such as confidentiality, authentication, and data sharing, were discussed by the authors	Blockchain is used to capture electronic health records (EHR), store them securely, and integrate IoT and fog computing to provide secure storage and analytics
Quasim et al. (2020)	Blockchain technology	Examined ways of improving electronic health records' security and privacy compared to traditional healthcare systems by securing them	The use of blockchain technology as a secure way to ensure the protection of electronic health records (EHRs) has been developed
Velliyangiri et al. (2022)	Blockchain technology	They discussed medical accuracy, reduction of risk factors, and preventing health challenges before they arise, as well as the importance of medical accuracy	1. Using blockchain technology, they developed a decentralized view of health records 2. Preventing health problems before they occur, mitigating risk factors, and improving medical accuracy are all advantages of this
Mallikarjuna et al. (2021)	Blockchain technology	Using an IoT-based cloud environment, they discussed the limitations of reduced latency in the transmission of healthcare records	Provided a blockchain-based system to facilitate the transmission of health records between doctors and patients
Jennath et al. (2020)	Blockchain technology and AI	Current eHealth systems do not address security concerns or privacy concerns adequately	1. Using Blockchain for trusted AI models in e-health involves sharing consent-based data for transparent data collection 2. The use of Blockchain technology in eHealth has been proposed to resolve security and privacy issues that have otherwise not been addressed
Gayathri et al. (2020)	Blockchain technology	Discussed the issues of certifying medical records and ensuring the integrity of the records	1. Provided secrecy and authentication for digital signatures by implementing a keyless signature infrastructure 2. Maintaining data integrity, blockchain technology is capable of securing transactions
Kumar et al. (2022)	Blockchain technology and AI	To detect intrusions at the edge of the network, they discussed using deep learning-based intrusion detection systems	Proposed an artificial intelligence-based blockchain infrastructure for securely disseminating data for IoT-enabled e-health systems based on IoT
Veeramakali et al. (2021)	AI	They discussed the security and reliability issues associated with the use of deep learning to diagnose medical records were discussed	Provided secure and reliable diagnostics using deep learning and cryptography in IoT and healthcare
Ghazal et al. (2022)	AI	The limitations relating to the sharing of medical records and the sharing of data were discussed	1. A cryptographic framework based on blockchain technology is proposed 2. Provided security-related solutions using a computational intelligence approach, a cryptographic framework based on blockchain technology
Chakraborty et al. (2019)	Blockchain technology	They highlighted the limitation of trust and authenticity of the data in healthcare data research as two of the fundamental aspects of data analysis	1. Presented an excellent model for supervising a cure from the beginning to the end of the treatment 2. Providing complete supervision of a cure, continuous treatment, or generic healthcare
Samad (2022)	Blockchain technology and AI	Examining the challenges of sharing decentralized views of health information and improving health, medical accuracy, and prevention of disease through blockchain technology in eHealth	1. Developed a blockchain approach to examine different methods of sharing centralized views of health information 2. Improved medical accuracy, and health, and prevents health disorders
Verma (2024)	Blockchain technology	The challenge of authenticating medical records in a secure environment and maintaining the integrity of medical records were discussed	1. Presented a new blockchain technology that enables the secure storage of health records in the cloud by using a distributed ledger technology 2. Presented a method of deploying blockchains with optimal encryption based on improved blowfish models
Jakhar et al. (2024)	Blockchain technology	They discussed challenges in maintaining integrity, security, accessibility, and privacy in healthcare data through consensus-driven decentralized management through peer-to-peer distributed computing platforms	1. Propose a privacy-preserving access control framework based on blockchain technology 2. To ensure decentralized management of healthcare data, peer-to-peer distributed computing platforms are used to ensure the integrity, security, accessibility, and privacy of healthcare data

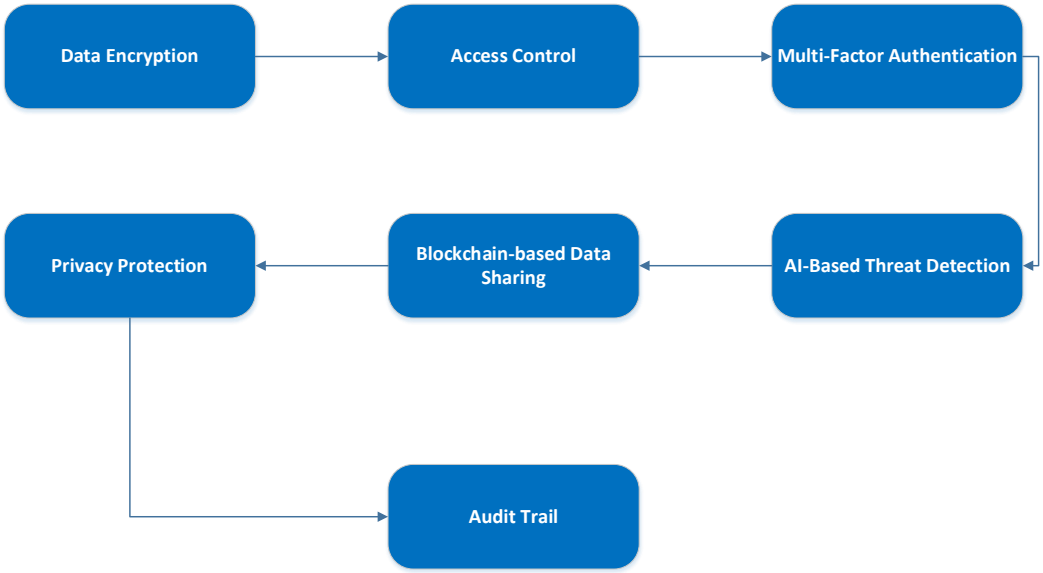

Fig. 3: Secure e-health framework using artificial intelligence and blockchain technology (SEHFUAIBC)

Modern encryption algorithms, such as RSA and AES, employ complex mathematical algorithms to encrypt data, making it unreadable without the necessary decryption keys. These algorithms ensure that even if unauthorized individuals gain access to encrypted health records, they will not be able to decipher or misuse the information. By encrypting all health data, healthcare organizations can safeguard patient information and ensure their safety. By protecting patient data from unauthorized access, healthcare organizations can prevent data breaches, identity theft, and privacy violations. This not only protects the patients' well-being but also helps maintain the integrity of the healthcare system.

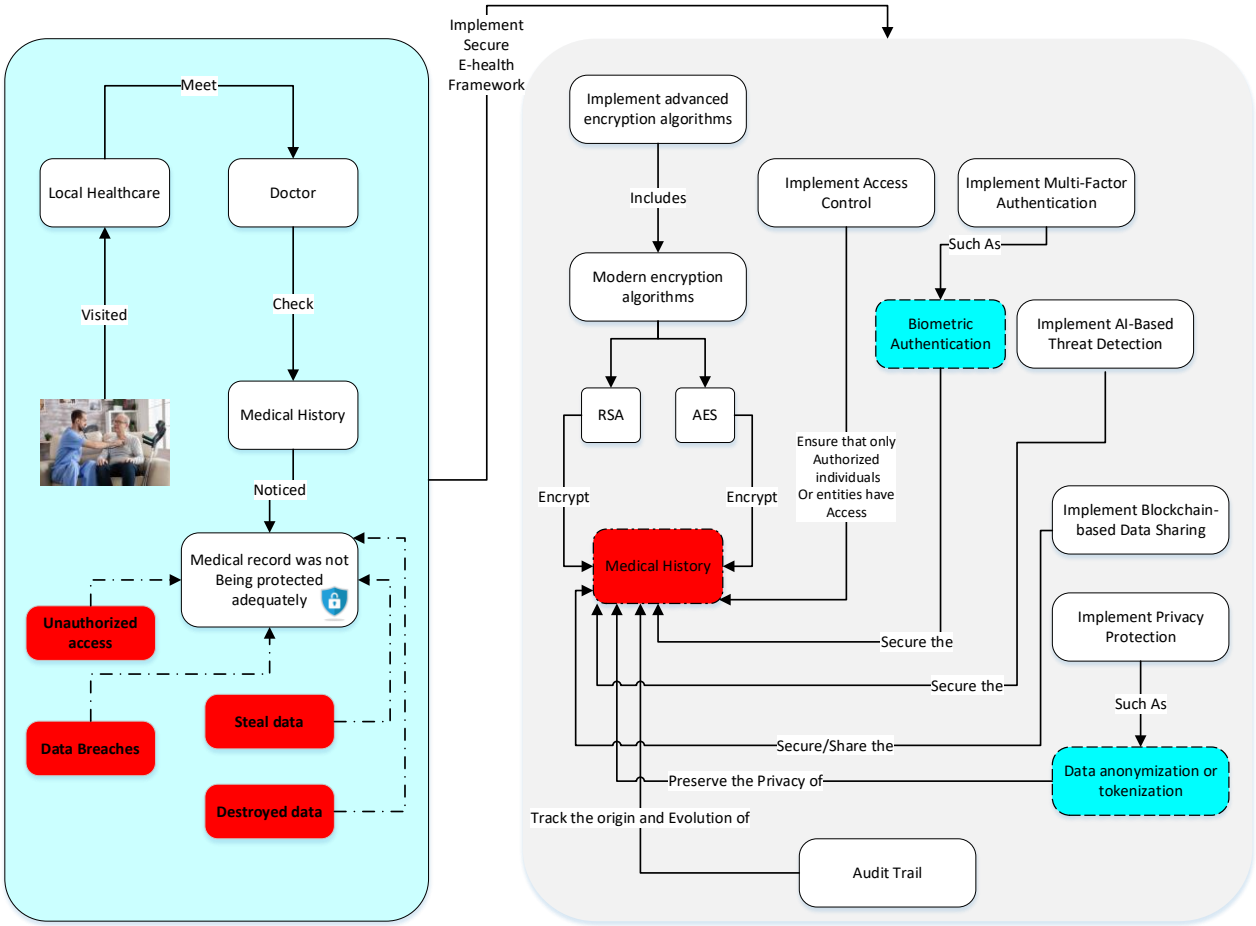

Fig. 4: Real scenario of implementing the secure e-health framework for protecting the medical history of patients

6. Results and discussions

The purpose of this study was to highlight the security challenges that are associated with the e-health sector, as well as the contributions that were provided by existing studies in this area. Based on research on the security challenges and issues of the e-health sector, SEHFUAIBC is developed based on blockchain and AI mechanisms.

The existing works focused on the four main security challenges of the e-Heath records which are: authorization, sharing data, integrity, and privacy. One of the key challenges in the e-Heath sector is ensuring appropriate access controls to medical records. For example, a healthcare provider responsible for treating a patient should be able to access only specific information related to that patient, while an administrator responsible for system maintenance should have limited access to patient data. The second challenge is that sharing medical data among healthcare providers is essential for efficient collaboration and continuity of care. However, sharing medical data securely can be a challenge due to concerns about confidentiality and the potential for unauthorized access. For example, a hospital can share a patient's medical records with another healthcare facility through a secure messaging system, ensuring that only the intended recipient can view the data. The third challenge is the integrity of medical data. Thus, healthcare organizations need to ensure that electronic medical data is accurate, complete, and unaltered. To address this challenge, healthcare organizations can implement robust data integrity measures. This can include the use of digital signatures to verify the authenticity of medical data, as well as regular data backups and disaster recovery plans. Healthcare organizations should also establish policies and procedures for data validation and verification, ensuring that any changes made to medical records are properly recorded and justified. For example, a hospital can implement a system that automatically checks and verifies the integrity of medical data, such as patient demographic information or medication records, to prevent unauthorized changes. The last challenge is the privacy of medical data. Healthcare organizations need to implement robust security measures to protect patient's personal information from unauthorized access or use. This includes implementing a comprehensive data privacy and security framework, including policies, procedures, and technologies to protect patient information from unauthorized access, disclosure, or alteration. Healthcare organizations should also educate their staff about the importance of privacy and ensure their compliance with privacy guidelines. For example, a hospital can store patient information in secure data centers, protected by physical and technical security measures, to prevent unauthorized access. Additionally, the hospital can implement strict access controls, such as role-based access controls, to limit who can access and view patient data. To address the challenges mentioned above, the SEHFUAIBC was developed in the present study. It utilizes a combination of blockchain technology and artificial intelligence technologies to make sure that e-health records are confidential, secure, private, and accessible. A real-world scenario is used to test the applicability of the developed SEHFUAIBC. The implementation of SEHFUAIBC has proven that the framework that has been developed is robust and can secure medical records and protect them from unauthorized users, data theft, and unauthorized destruction by providing a robust framework.

7. Limitations and open directions

As a result of the use of artificial intelligence and blockchain technology, sensitive data such as patient medical records, diagnosis details, and medication history are collected, stored, and processed. There is a danger that this information could be accessed by unauthorized individuals or misused. There is a potential for significant security and privacy breaches if there are no proper access controls in place to prevent unauthorized individuals from gaining access to sensitive patient data. AI and blockchain are now being integrated into this aspect of the project, which introduces several new challenges. Since a blockchain is based on a decentralized network of nodes, it is very difficult to monitor and maintain the integrity of the data since it relies on a decentralized network. There is a particular problem when it comes to sensitive healthcare records since there is a high likelihood that they could be manipulated or falsified as a result. The dispersed nature of blockchain technology may make it difficult for healthcare organizations to share data efficiently across organizations. This could harm patient care and collaboration. Moreover, because blockchain records are distributed, it can be challenging for data integrity and consistency to be maintained across multiple systems due to the distributed nature of blockchain records.

8. Conclusions

Blockchain and AI are emerging technologies in healthcare. To collect information on healthcare indices, documents published on the Web of Sciences and other Google surveys conducted by a range of governing bodies are used to collect the information. The purpose of this review is to examine a wide range of aspects of blockchain and artificial intelligence, along with how these two technologies can be integrated to make a significant contribution to healthcare. In addition, it is recommended to implement generalizable analytical technologies that can be incorporated into a more comprehensive risk management strategy to make a significant contribution to healthcare. This article discusses the various ways that blockchain technology can be used as an open network for sharing information as well as allowing it to be authorized, which opens up

several opportunities for building reliable artificial intelligence models for e-health applications. The AI will be able to access the medical records of patients on the blockchain by using a variety of algorithms and decision-making capabilities, as well as a large amount of data, to assist healthcare professionals in accessing the medical records of patients on the blockchain. This will lead to a generalized improvement in the efficiency of the medical system, a reduction in costs, as well as a degree of democratization in the healthcare delivery system, since it will incorporate the latest advancements in these technologies, resulting in an improvement of efficiency in everything related to healthcare. Some blockchains are used to store cryptographic records, which is a requirement for AI to store cryptographic records. Hence, the objective of this article is to propose a secure e-health framework using artificial intelligence and blockchain technology that is referred to as SEHFUAIBC. In this study, the DSM is used to conduct the research. As a result of the development of the SEHFUAIBC, the system consists of seven elements: advanced encryption algorithms, access control, multi-factor authentication, AI-powered threat detection, blockchain-based data sharing, privacy protection, and audit trail. A real-world scenario was used to evaluate the SEHFUAIBC developed. Based on the results of this study, it is evident that a combination of AI and blockchain in the framework produced by this study results in hybrid security techniques which hold the keys to protecting e-health records against unauthorized access.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Agu PC and Obulose CN (2024). Piquing artificial intelligence towards drug discovery: Tools, techniques, and applications. Drug Development Research, 85(2): e22159. https://doi.org/10.1002/ddr.22159 **PMid:38375772**

Akkiraju R, Sinha V, Xu A, Mahmud J, Gundecha P, Liu Z, Liu X, and Schumacher J (2020). Characterizing machine learning processes: A maturity framework. In the Business Process Management: 18th International Conference, Springer International Publishing, Seville, Spain: 17-31. https://doi.org/10.1007/978-3-030-58666-9_2

Alabdulatif A, Al Asqah M, Moulahi T, and Zidi S (2023). Leveraging artificial intelligence in blockchain-based e-health for safer decision making framework. Applied Sciences, 13(2): 1035. https://doi.org/10.3390/app13021035

Al-Dhaqm A, Abd Razak S, Dampier DA, Choo KK, Siddique K, Ikuesan RA, Alqarni A, and Kebande VR (2020). Categorization and organization of database forensic investigation processes. IEEE Access, 8: 112846-112858. https://doi.org/10.1109/ACCESS.2020.3000747

Alotaibe DZ (2024). IoT security model for smart cities based on a metamodeling approach. Engineering, Technology and Applied Science Research, 14(3): 14109-14118. https://doi.org/10.48084/etasr.7132

Alotaibi F, Al-Dhaqm A, and Al-Otaibi YD (2023). A conceptual digital forensic investigation model applicable to the drone forensics field. Engineering, Technology and Applied Science Research, 13(5): 11608-11615. https://doi.org/10.48084/etasr.6195

Alotaibi YK and Federico F (2017). The impact of health information technology on patient safety. Saudi Medical Journal, 38(12): 1173-1180. https://doi.org/10.15537/smj.2017.12.20631 **PMid:29209664 PMCid:PMC5787626**

Alotibi G (2024). A cybersecurity awareness model for the protection of Saudi students from social media attacks. Engineering, Technology and Applied Science Research, 14(2): 13787-13795. https://doi.org/10.48084/etasr.7123

Bragazzi NL, Dai H, Damiani G, Behzadifar M, Martini M, and Wu J (2020). How big data and artificial intelligence can help better manage the COVID-19 pandemic. International Journal of Environmental Research and Public Health, 17(9): 3176. https://doi.org/10.3390/ijerph17093176 **PMid:32370204 PMCid:PMC7246824**

Campanella P, Lovato E, Marone C, Fallacara L, Mancuso A, Ricciardi W, and Specchia ML (2016). The impact of electronic health records on healthcare quality: A systematic review and meta-analysis. The European Journal of Public Health, 26(1): 60-64. https://doi.org/10.1093/eurpub/ckv122 **PMid:26136462**

Chakraborty S, Aich S, and Kim HC (2019). A secure healthcare system design framework using blockchain technology. In the 21st International Conference on Advanced Communication Technology, IEEE, PyeongChang, Korea: 260-264. https://doi.org/10.23919/ICACT.2019.8701983

Chapuis C, Roustit M, Bal G, Schwebel C, Pansu P, David-Tchouda S, Foroni L, Calop J, Timsit JF, Allenet B, and Bosson JL et al. (2010). Automated drug dispensing system reduces medication errors in an intensive care setting. Critical Care Medicine, 38(12): 2275-2281. https://doi.org/10.1097/CCM.0b013e3181f8569b **PMid:20838333**

Farhadighalati N, Ghalaty NF, Nikghadam-Hojjati S, Marchetti E, and Barata J (2023). SAFE-HEALTH: A secure framework for advancing edge-based health 5.0. In the IEEE 9th World Forum on Internet of Things, IEEE, Aveiro, Portugal: 1-6. https://doi.org/10.1109/WF-IoT58464.2023.10539418

Gayathri N, Sakthivel RK, Rizwan P, Gandomi AH, Muthuramalingam S, and Balamurugan B (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing and Applications, 32(3): 639-647. https://doi.org/10.1007/s00521-018-3915-1

Ghazal TM, Hasan MK, Abdullah SNHS, Bakar KAA, and Al Hamadi H (2022). Private blockchain-based encryption framework using computational intelligence approach. Egyptian Informatics Journal, 23(4): 69-75. https://doi.org/10.1016/j.eij.2022.06.007

Jakhar AK, Singh M, Sharma R, Viriyasitavat W, Dhiman G, and Goel S (2024). A blockchain-based privacy-preserving and access-control framework for electronic health records management. Multimedia Tools and Applications, 83: 84195–84229. https://doi.org/10.1007/s11042-024-18827-3

Jennath HS, Anoop VS, and Asharaf S (2020). Blockchain for healthcare: Securing patient data and enabling trusted artificial intelligence. International Journal of Interactive Multimedia and Artificial Intelligence, 6(3): 15-23. https://doi.org/10.9781/ijimai.2020.07.002

Kubendiran M, Singh S, and Sangaiah AK (2019). Enhanced security framework for e-health systems using blockchain. Journal of Information Processing Systems, 15(2): 239-250.

Kumar P, Kumar R, Garg S, Kaur K, Zhang Y, and Guizani M (2022). A secure data dissemination scheme for IoT-based e-health systems using AI and blockchain. In the GLOBECOM 2022-2022 IEEE Global Communications Conference, IEEE, Rio de Janeiro, Brazil: 1397-1403. https://doi.org/10.1109/GLOBECOM48099.2022.10000801

Mak KK, Wong YH, and Pichika MR (2023). Artificial intelligence in drug discovery and development. In: Hock FJ and Pugsley MK (Eds.), Drug discovery and evaluation: Safety and pharmacokinetic assays: 1-38. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-030-73317-9_92-1

Mallikarjuna B, Kiranmayee D, Saritha V, and Krishna PV (2021). Development of efficient e-health records using IoT and blockchain technology. In the ICC 2021-IEEE International Conference on Communications, IEEE, Montreal, Canada: 1-7. https://doi.org/10.1109/ICC42927.2021.9500390

March ST and Smith GF (1995). Design and natural science research on information technology. Decision support systems, 15(4): 251-266. https://doi.org/10.1016/0167-9236(94)00041-2

Mourya AK, Kapil G, and Idrees SM (2024). Modernizing healthcare data management: A fusion of mobile agents and blockchain technology. In: Idrees SM and Nowostawski M (Eds.), Blockchain transformations: Navigating the decentralized protocols era: 93-106. Springer Nature, Cham, Switzerland. https://doi.org/10.1007/978-3-031-49593-9_6

Priyanka EB, Thangavel S, Mohanasundaram R, and Subramaniam S (2024). Artificial intelligence approaches in healthcare informatics toward advanced computation and analysis. The Open Biomedical Engineering Journal, 18: e18741207281491. https://doi.org/10.2174/0118741207281491240118060019

Quasim MT, Radwan AAE, Alshmrani GMM, and Meraj M (2020). A blockchain framework for secure electronic health records in healthcare industry. In the International Conference on Smart Technologies in Computing, Electrical and Electronics, IEEE, Bengaluru, India: 605-609. https://doi.org/10.1109/ICSTCEE49637.2020.9277193

Sahoo MS and Baruah PK (2018). HbasechainDB–A scalable blockchain framework on hadoop ecosystem. In: Yokota R and Wu W (Eds.), Supercomputing Frontiers. SCFA 2018. Lecture Notes in Computer Science, Volume 10776. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-319-69953-0_2

Samad A. (2022). Internet of Things integrated with blockchain and artificial intelligence in healthcare system. Research Journal of Computer Systems and Engineering, 3(1): 1-6.

Sanjana T, Sowmya BJ, Kumar DP, and Srinivasa KG (2021). A framework for a secure e-health care system using IoT-based Blockchain technology. In: Sharma SK, Bhushan B, Khamparia A, Astya PN, and Debnath NC (Eds.), Blockchain technology for data privacy management: 253-273. CRC Press, Boca Raton, USA. https://doi.org/10.1201/9781003133391-12

Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, and Soursou G (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1): 3. https://doi.org/10.3390/cryptography3010003

Tagde P, Tagde S, Bhattacharya T, Tagde P, Chopra H, Akter R, Kaushik D, and Rahman MH (2021). Blockchain and artificial intelligence technology in e-health. Environmental Science and Pollution Research, 28: 52810-52831. https://doi.org/10.1007/s11356-021-16223-0 **PMid:34476701 PMCid:PMC8412875**

Veeramakali T, Siva R, Sivakumar B, Senthil Mahesh PC, and Krishnaraj N (2021). An intelligent Internet of Things-based secure healthcare framework using blockchain technology with an optimal deep learning model. The Journal of Supercomputing, 77(9): 9576-9596. https://doi.org/10.1007/s11227-021-03637-3

Velliyangiri G, Krishnamoorthy V, Inbaraj C, Venkatachalam A, Rahim R, and Ramachandran M (2022). Blockchain and artificial intelligent for Internet of Things in e-health. In: Goundar S, Suseendran G, and Anandan R (Eds.), The convergence of artificial intelligence and blockchain technologies: Challenges and opportunities: 23-42. World Scientific Publishing Company, Singapore, Singapore. https://doi.org/10.1142/9789811225079_0002

Verma G (2024). Blockchain-based privacy preservation framework for healthcare data in cloud environment. Journal of Experimental and Theoretical Artificial Intelligence, 36(1): 147-160. https://doi.org/10.1080/0952813X.2022.2135611

Wong ZS, Zhou J, and Zhang Q (2019). Artificial intelligence for infectious disease big data analytics. Infection, Disease and Health, 24(1): 44-48. https://doi.org/10.1016/j.idh.2018.10.002 **PMid:30541697**