ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

Securing Health Data with Blockchain and Artificial Intelligence

S. Sundara Mohan[1], Polani Vighnesh[2], Naru Siva Chandrikaa[3], Abhilash[4], Sameer[5]

[1] Assistant Professor, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

[2,3,4,5] Students, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

Email id: sundaramohans@gmail.com[1], polanivighnesh5@gmail.com[2], chandunaru71@gmail.com[3], prieabhi11@gmail.com[4], sameersameer58267@gmail.com[5]

Abstract:

In the modern cyber world, data is essential for Artificial Intelligence (AI) algorithms to extract insights from historical data for decision-making, such as product recommendations, healthcare services, or educational institutions. However, not all data, such as sensitive Patient Health Data, can be made publicly available due to privacy concerns. Traditional service providers store user data on third-party servers, often selling it for profit, leaving users with no control. To address this, this project introduces Private Data Centres (PDC) with Blockchain and AI techniques to secure user data. PDC ensures ownership-controlled data sharing via blockchain, intelligent access control with AI-driven verification, and a rewards system to encourage data sharing. This contrasts with traditional Blockchain-based healthcare systems, which use Differential Privacy and Federated Learning to protect data privacy while focusing on data utility. The PDC framework promotes data ownership and incentivizes users to participate in data sharing, offering a secure, user-centric approach.

Keywords: Access Control, Artificial Intelligence, Blockchain, Data Privacy, Django Deployment, Patient Health Data, Private Data Centres, Rewards Mechanism.

1.Introduction

The health informatics technique underlying budgeting, personnel, patients, legal disputes, logistics, supplies, and other procedures and medical workflows are often made up of a sequence of conditional steps that can be visualized as a series of repeated patient-care activities (Alotaibi and Federico 2017). Among hospitals and other healthcare service providers, internal controls should be increased; performance, compliance, and consistency should be enhanced; and risk, job time, and overhead should be reduced (Chapuis et al. 2010). This article outlines a healthcare smart contract structure that can handle patient data and simplify complicated medical treatments (Campanella et al. 2016), based on advanced healthcare blockchain analysis and a robust approach to healthcare management. We have looked at cutting-edge blockchain studies in healthcare and presented a blockchain-based solution to healthcare management. As shown by numerous initiatives in various countries and economies, governments and related business sectors are becoming more involved in digitizing healthcare systems. The path to success is to integrate technology into each company's DNA by utilizing blockchain, AI, and other accessible technologies (Wong et al. 2019; Bragazzi et al. 2020). To advance medical research and achieve patient-centricity, the industry would use technology to create user- and customer-centric interfaces and data-driven decisions for innovative data processing approaches and better results (Sahoo and Baruah 2018). For example, artificial intelligence (AI) could help identify and prioritize individual patients for drug monitoring and growth, critical for managed drug production and shorter timelines (Paul et al. 2021). For repurposing marketed medications, researching the effectiveness of medication formulations, and dose measurement, clinical trial data was monitored using numerical drug design methods and AI (Cha et al. 2018). As a consequence of such a rapidly evolving climate, governments must identify the most effective ways to leverage resources and drive reform while ensuring the necessary consistency, compliance, or data protection (Siyal et al. 2019). We have mention in Fig.1 security measures in e-Health by blockchain and AI. Blockchain aids in the creation of a system that develops and manages content blocks known as ledgers, with safe and automated data analysis.

2.Related work

The blockchain is a distributed database using state machine replication, with atomic changes to the database referred to as transactions grouped into blocks, with the integrity and tamper-resistance of the transaction log assured via hash links among blocks. The blockchain concept was introduced for Bitcoin in the context of decentralized electronic currency. The popularity of Bitcoin allows blockchain that can use without depending on any established third party to enable trustworthy and safe transactions through an untrusted network. There have been many reports on basic building blocks in the blockchain (Feng et al. 2019). A sequential series of blocks containing a list of complete and correct transaction records is blockchain. The blocks are connected by a relation (hash value) to the previous block, thereby creating a chain (Lin et al. 2020). The block that precedes a given block is recognized as its block header, and the very first block is recognized as the block of genesis (Ahmad et al. 2019; Zhang et al. 2020). With a growing interest in many applications, spanning from data storage, financial markets, computer protection, IoT, and nutritional science to the healthcare sector and brain studies, blockchain technology has gained tremendous popularity and progress to distribute safe and stable monitoring of healthcare records. It may be a tool in the future that could theoretically assist in customized, credible, and safe healthcare by combining and displaying the whole real-time clinical records of a patient’s wellbeing in an up-to-date, secure healthcare setup (Linn and Koo 2016). Blockchain platform to determine the health care status of patient illnesses, focused on concurrent execution and artificial intelligence healthcare networks and the proposed approach analyses of the patient’s overall state, diagnosis, and recovery system, and investigates the relevant surgical interventions by simultaneous operations and clinical decision-making computational studies to assess the quality of care for patients and the feasibility of diagnosis, the proposed method has been evaluated in actual, as well as simulated, healthcare systems (Bryatov and Borodinov 2019; Hylock and Zeng 2019).

3. Research Methodology

The processes or strategies used to locate, select, process, and Analyze information on a topic are referred to as research methodology. In this study, a systematic literature survey using the

PRISMA approach is presented to answer the research questions that investigates the robustness of the healthcare system. This technique is split into the following areas: selection criteria, quality assessment, and selection result

Quality assessment

The following criteria were considered for quality assessment. The articles which meet the criteria are then considered for the systematic review.

- Application area: The article emphasizes healthcare applications or medical domain.
- Objectives: The article discusses the challenges in AI-based healthcare and mitigating those with Blockchain.
- Techniques: Proposed or implemented framework in the article must have Blockchain technology integrated with AI methods.
- Security measures: The article must identify the features of Blockchain and use them to achieve privacy, security, and integrity.

Attack Surface of Artificial Intelligence

Machine learning is a data processing technique that automates the development of analytical models. It is a subfield of AI that is focused on the principle that computers can learn from data, recognize patterns, and make decisions excluding human involvement. These tasks require obtaining the validated data, using which the classifiers are trained. After successful training, the model is deployed. It might proceed with retraining and feedback loops for performance improvement. Figure shows the different phases involved in the successful deployment of the AI model. It starts with the data collection and its preparation for training by looking for bias or labeling the data. Then, based on the requirement of the application that is being studied, the classifier is either developed or selected from existing ones. A classifier is trained for the acquired dataset and can be further improved by adjusting the parameters. The trained model is deployed at the end, and the model will proceed with retraining for performance improvement and enhancement. An attack on a device or an information system is any action to reveal, change, disable, damage, capture, or collect information by exploiting the vulnerabilities available in the system. The basic security requirement for any system is maintaining the privacy of sensitive data or processes, getting untampered data or processes, and allowing data or processes to be available to an intended user at any time. Henceforth this CIA triad applies to the phases mentioned above for securely deploying the ML model. Figure focuses on the attack surface of AI. Data, classifier/algorithm, and learned model are the targeted areas for imposing attacks by any adversary in any AI-based systems.

Blockchain technologies in healthcare

In the context of healthcare and medical data, maintaining the privacy rights of individuals regarding their confidential medical information is paramount. Such sensitive data must be released with meticulous care and attention to ethical and legal considerations. Oversight and regulation are provided by frameworks such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States35 and analogous international data protection laws. These rules aim to safeguard patient privacy while facilitating the authorized and secure sharing of data that is essential to the healthcare system. Understanding these rules is essential to ensuring that people's medical records are not accessed or disclosed without authorization, protecting the privacy of their personal health information. In parallel, emerging concepts outlined in literature, such as reference, offer innovative ways to facilitate convenient and secure user information sharing. These concepts are particularly relevant in healthcare and IoT medical devices. The utilization of IoT medical devices for monitoring a patient's health has witnessed a growing trend, becoming increasingly common in healthcare settings. These devices, characterized by their ability to provide real-time data on physiological parameters, offer a straightforward assessment of an individual's health status. This includes parameters like temperature, oxygen saturation, heart rate, and the capability to assess internal body temperature

Enhancing security

The use of blockchain technology enhances the security and privacy of the data produced by Internet of Tings (IoT) healthcare devices. It guarantees the privacy of sensitive health information while granting authorized parties access to relevant information when needed.

Data

The most critical component of AI is data. Any model cannot be trained without data, and all current technological development will be for naught. There is an enormous investment of money only to collect specific data as much figure

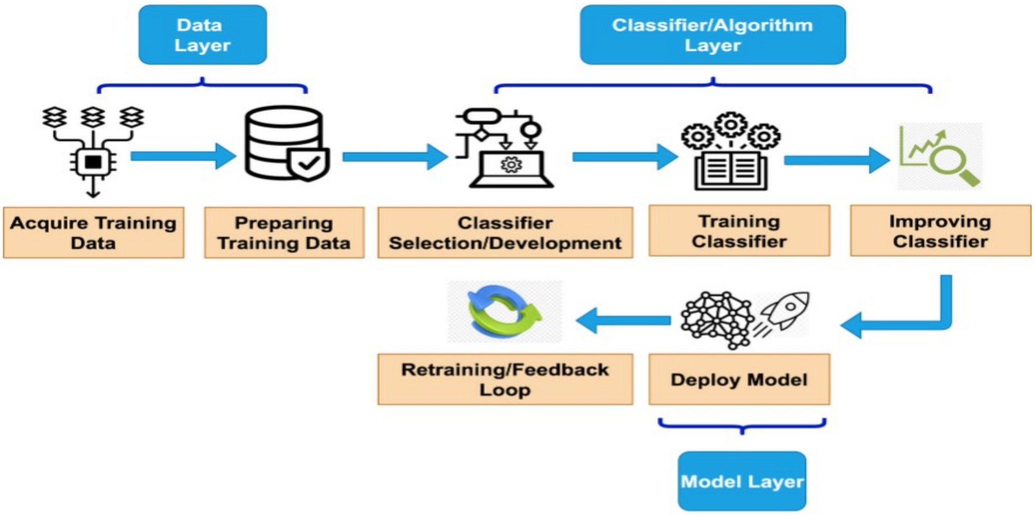

Figure: Phases involved in deploying AI models.

The integrity of data can be undermined during either the training or testing stages by exploiting the AI models' susceptibility to minor input variations, resulting in abnormal model behavior referred to as poisoning and evasion attacks. These attacks can be facilitated by spoofing, which involves deceptive tactics by an adversary to deceive computer networks by posing as a legitimate entity, utilizing computers, devices, or networks. The malicious opponents frequently lack access to the training phase of the model. They create an adversarial input to deceive a classifier or elude detection from a neural network during the testing phase. These can be either physical or digital types of attacks. This study focuses on digital types of attacks. A digital approach directly imparts tiny perturbations in the input. In this scenario, the assailant can manipulate the specific system without triggering any alerts from the intrusion detection mechanism. Eva-sion attacks can also result in a concept drift.57 Potential aggressors might additionally infiltrate the training dataset and introduce malicious samples, referred to as poisoning attacks, thereby contaminating the dataset. Adversarial attacks in AI-based healthcare systems have the potential to harm human beings, as discussed in the subsequent sections.

4. Results

Developing comprehensive interoperability within the healthcare industry poses significant challenges because of the inherent vulnerability of patient privacy. Blockchain technology is rapidly developing as a beautiful solution for preserving functionality in the healthcare system. The highest priority is establishing strategies to enhance communication among care-related information systems203. It is imperative to ensure an adequate level of security during the process of transmitting patient medical records. Various risks linked to the practice give rise to potential consequences that can significantly affect healthcare providers' financial, insurance, and ethical aspects204. Healthcare professionals often examine healthcare from various perspectives daily. One of the options available is utilizing Blockchain technology to operate a Hospital Management System (HMS). The objective is to enhance the safeguarding of information and simplify inter-system communication. In a healthcare environment, protecting user privacy, availability, and integrity is imperative while accessing information consistent with many systems. Achieving an equitable relationship between interoperability and security within the healthcare domain necessitates a careful balance due to the crucial functional basics, non-functional criteria, and business factors involved. Integrating BC technology in healthcare presents advantages and disadvantages, primarily due to a lack of skilled experts in developing effective software designs that ft this unique environment

NLP techniques

Named entity recognition

The most fundamental method in NLP is retrieving entities from the text. It emphasizes the key topics and connections in the text. Named Entity Recognition (NER) extracts entities from the text such as persons, places, organizations, and dates. Grammar rules and supervised models are commonly used.

Sentiment analysis Sentiment Analysis is the most used approach in NLP. Sentiment analysis is particularly effective when individuals express their thoughts and feedback, such as through customer surveys, reviews, and social media comments. The most basic result of sentiment analysis is a three-point scale: positive/negative/neutral. The result can be a numerical score grouped into as many categories as the user desires in more sophisticated instances

Table: Query results from data sources

Library	Initial	Title and keyword	Abstract	Full text
IEEE Xplore	250	200	90	50
Science Direct	180	110	75	35
ACM Digital Library	400	250	130	80
Springer Link	150	120	70	40
Wiley	100	80	45	16
Result	1080	760	410	221

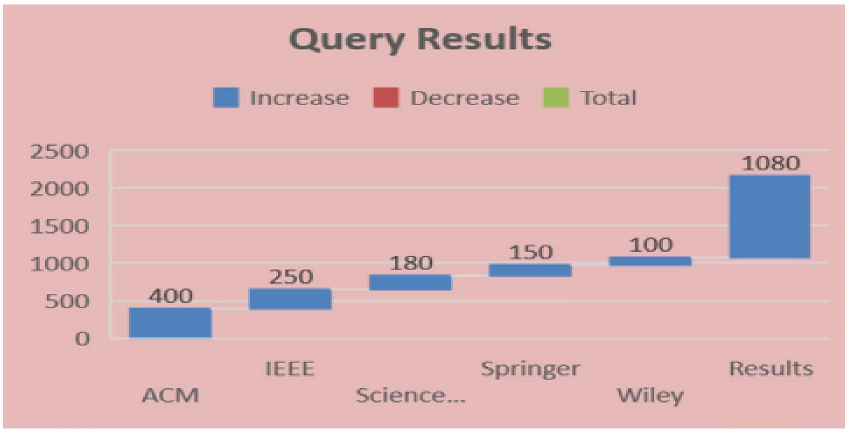

Figure: Query results

Conclusion

In conclusion, this study has comprehensively explored integrating blockchain technology with the IoMT in the healthcare sector. The study has made significant contributions in several key areas through meticulous research and analysis. The study has proposed using zero-knowledge proofs (ZKPs) to address the challenges of scalability and storage requirements. The study offers a viable solution to manage the ever-expanding data generated by IoMT devices by employing encryption techniques and efficient data fragmentation. It highlights the need for adherence to regulations like HIPAA and the role of blockchain in ensuring compliance. It explores the role of blockchain in enhancing communication among healthcare information systems while maintaining patient privacy. This study offers valuable insights into the potential of blockchain technology to revolutionize the healthcare industry by addressing critical challenges and providing secure, interoperable, and compliant solutions. The findings underscore the need for further research and implementation of blockchain-based systems in healthcare to improve patient care, reduce costs, and enhance data security. As the healthcare landscape evolves, blockchain technology is poised to play a pivotal role in shaping its future.

References:

1. Gugueoth, V., Safavat, S., Shetty, S. & Rawat, D. A review of iot security and privacy using decentralized blockchain techniques. Comput. Sci. Rev. 50, 100585 (2023).
2. Peres, R., Schreier, M., Schweidel, D. A., & Sorescu, A. Blockchain meets marketing: Opportunities, threats, and avenues for future research (2023).
3. Khang, A., Rana, G., Tailor, R., & Abdullayev, V. Data-centric ai solutions and emerging technologies in the healthcare ecosystem (2023).

4. Villarreal, E. R. D., Garcia-Alonso, J. & Moguel, E. Blockchain for healthcare management systems: A survey on interoperability and security. IEEE Access 11, 5629–5652 (2023).
5. Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K. & Siddique, A. H. Blockchain application in healthcare systems: A review. Systems 11(1), 38 (2023).
6. Androulaki, E. et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Tirteenth EuroSys Conference; EuroSys '18; Association for Computing Machinery, pp. 30:1–30:15
7. Ahram, T. et al. Blockchain Technology Innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
8. Dagher, G. G., Mohler, J., Milojkovic, M. & Marella, P. B. Ancile: Privacy-preserving frame work for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. 39, 283–297 (2018).
9. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. MedRec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30 (2016).
10. Li, H. et al. Blockchain-based data preservation system for medical data. J. Med Syst. 42, 141 (2018)