International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 10-No.4 (2024) pp. 1120-1129
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

The Role of Blockchain and AI in Fortifying Cybersecurity for Healthcare Systems

M. Husain Bathushaw[1]*, S. Nagasundaram[2]

[1]Research Scholar, Department of Computer Applications, VELS institute of science, technology and advanced studies, Pallavaram-600117, Chennai, India.
* **Corresponding Author Email:** mhbathusha@hotmail.com - **ORCID:** 0009-0008-8447-0515

[2]Research Supervisor/Asst. Professor, Department of Computer Applications, VELS institute of science, technology and advanced studies, Pallavaram-600117, Chennai, India
Email: snagasundaram.scs@vistas.ac.in - **ORCID:** 0000-0003-0374-0517

Article Info:

DOI: 10.22399/ijcesen.596
Received : 08 November 2024
Accepted : 15 November 2024

Keywords :

Healthcare cybersecurity,
Blockchain,
Artificial intelligence,
Data integrity,
Threat detection.

Abstract:

In a simulated healthcare setting, the algorithms were assessed based on organized threat insight data, inconsistency location executed with blockchain-enhanced access control, and machine learning-driven interruption detection. The test results depiction showed that all calculations were feasible, with an accuracy range of 0.88-0.94 and lift defined between 0.75 and 1; knowledge values ranging from.86 to.92, and F1 scores between and above.90 results are displayed as follows: Above all, TIAA excelled in risk insights management; ADA exceeded expectations in detecting inconsistencies; BACA used blockchain to fortify access control; and ML-IDS produced remarkable results in intrusion detection. The importance of these algorithms in addressing particular cybersecurity concerns in the healthcare industry is highlighted through a comparative comparison with similar studies. The suggested algorithms are relevant to the growing conversation about cybersecurity in healthcare because they offer a comprehensive strategy to protect private health data, guarantee the reliability of assessment models, and fortify organizations against a variety of evolving cyberthreats.

1. Introduction

Today, the health care institutions of all nations are exposed to the most significant cybersecurity threats over confidential information regarding their patients' cases. Health care faces extreme cyber-attacks since data has a very high value in black markets, and the entire healthcare system relies on e-health records and other internet-driven technology tools. Therefore, there is a need for the implementation of effective, pioneering cybersecurity solutions to strengthen health care organizations' cyber securities. In this regard, research considers how advanced security measures, such as blockchain and AI, can be used to identify solutions and mitigate these cyber threats and risks [1]. The decentralized immutable ledger, through blockchain, holds tremendous potential in supporting the integrity and secrecy requirements of health care data [2]. The secure creation of a tamper-proof record of transactions has made blockchain capable of offering sensitive information, which is allowed to only authorized entities access and handle such data. De-centering the control of the data significantly reduces single points of failure, making mass breaches almost impossible as most of these centralized systems easily succumb to such mal-practices. However, the use of the intense audit trail clears that the blockchain framework is highly transparent and traceable, which is invaluable given the highly stringent regulatory environment arising from personally identifiable data protection laws such as the GDPR and the HIPAA [3]. In this case, AI based cybersecurity measures offers real time detection and response to new threats. The usage of an AI algorithm means that it has the capability for going through large volumes of complex data to discover patterns of behavior that may mean the presence of a potential cyber threat which can enable timely reaction to likely breaches if any. Artificial intelligence apps can model threats, predict attack types, and adjust security designs to match such a model. The automation of such

processes reduces the level of dependency on manual security checks, and as a result velocity and precision involved in combating threats improves. As a result, this research will only explore the ways in which both blockchain and AI can work together and complement each other to provide secure, robust, and sustainable healthcare data ecosystems.

2. Related Works

The development of cyber security technology has brought an increased use of complex and modern tools such as block chain, machine learning and other forms of intelligence structures in support of the security, integrity and reliability of data in various fields. For instance, more recent work focuses on security for network slicing in telecommunications that applies machine learning, SDN, and NFV to enhance detection for threats and data privacy in a network, demonstrating encouraging potential for healthcare cybersecurity, too [4-15]. Similarly, WSNs used in critical infrastructures also showcase an increased demand for standardized protocols, mainly to safeguard sensitive environments such as healthcare facilities that rely on IoT-based monitoring systems [16]. In healthcare, blockchain technology has emerged as the key player to ensure data integrity and privacy. Studies reveal how blockchain's tamper-proof design and encryption protocols can significantly reduce risks of data exposure. Eghmazi et al. (2024) discuss the use of blockchain to strengthen IoT data security, a relevant approach for healthcare where critical patient data is handled through IoT devices [17]. In addition, the combination of blockchain with AI technologies as discussed by Elisha et al. (2024) offers new pathways in automation and anomaly detection. While their primary application is on precision agriculture, the same methods can be applied to automate threat detection in healthcare where AI models could predict and intercept cyber threats before data breaches occur [18]. The use of ML in 5G networks has proved that ML techniques are quite effective in predicting and identifying cyber threats across different digital platforms. Fakhouri et al. (2023) have an extensive analysis of the role of ML in 5G security, which explains methods that boost the safety of data and ensure communication security in 5G-enabled healthcare networks [19]. Similarly, in highly adopted cloud computing environments by health-related institutions, there was a demand for secure data-sharing protocols that demanded two-factor authentication (2FA) and cryptographic solutions. The works of Gadde et al. (2023) propose that with blockchain-based systems, 2FA may enhance the safety of health information access significantly, which could reduce risks associated with unauthorized access [20-22]. Blockchain technology can be employed in the protection of intellectual property rights in medical research and technology. Huan-Wei et al. (2023) note how blockchain fortifies intellectual property transactions to ensure safe data exchange as well as the protection of medical innovation against cyber threats. This is very essential for health organizations whose intellectual property needs to be guaranteed safe [23]. Moreover, mobile applications in healthcare have the rising trend of applying blockchain as a top data storage security due to the need for protecting patient data stored in Android-based systems. Hussam et al. (2023) conducted a survey that measures blockchain's utility in securing Android applications, which states that analogous applications in healthcare can safeguard mobile health data effectively [24]. IOTA is one of the emerging technologies, which, according to Iuon-Chang et al. (2024), aims at improving data preservation in Industrial Control Systems (ICS). Their findings conclude that IOTA can integrate well with blockchain and might help provide a secure ground for data in case its utilization for healthcare data storage becomes inevitable [25]. Also, AI and blockchain have significantly improved managing health care data. Javaid et al. (2024) discuss the application of Lean 4.0 to optimize healthcare operations, such as cybersecurity, to decrease risks from data inefficiencies and vulnerabilities [26]. Blockchain and AI in health care cybersecurity are part of the broader trend of embracing innovative digital solutions to address the complexity of security challenges. The future of research in these technologies must be done in the health sector applications, focusing on secure data storage improvement, real-time threat detection, and regulatory compliance as observed in studies on telecommunication, IoT, and 5G security [15, 16, 17, 19]. Integration will not only enhance the cybersecurity framework but also ensure that healthcare organizations have adaptive and scalable solutions to protect sensitive patient information in a more digital world.

3. Methods and Materials

In developing a robust understanding of the role of blockchain and AI in strengthening cybersecurity for healthcare systems, this research employs a multi-methodological approach involving data analytics, cryptographic protocols, and machine learning algorithms. The methodology is divided into three major phases: data collection, blockchain framework development, and AI-based threat

detection [4]. Every stage is specifically intended for unique aspects of health information technology cybersecurity, based both on blockchain technology, designed for data integrity and accuracy, and AI algorithms used in advanced threat prediction and responses.

3.1 Data Collection and Preprocessing

This would ensure collection and preprocessing for achieving the comprehensive dataset of records ready for blockchain transaction records and AI model preparation. We use synthetic healthcare data from the MIMIC-III database, making use of de-identified patient health information to show real-world healthcare data without breaching the privacy of patient information [5]. The data records in this regard include patient records, transaction logs, access logs, and audit trails representing average interactions within a healthcare system. Each dataset segment in this regard is encoded to a standardized JSON format.

To process such a large number of entries, the following notations are used: let D={d1,d2,.,dn}denote the dataset, wherein di is unique data point that is expressed in the form of patient record or transaction log. The first step in processing the raw data is normalization and noise filtering procedures that remove the unwanted data to enhance the accuracy of the model [6]. This phase culminates in tokenizing data entries that are later utilized in blockchain-based hashing and AI feature extraction at the succeeding stages.

3.2 Blockchain Framework Development

The second stage is developing a blockchain framework secured to the healthcare systems. The aim of this task is ensuring that all transactions and accesses of a patient's data be recorded using a decentralized, tamperproof ledger reducing opportunities for unauthorized data changes. The framework will include three key components: block structure, consensus protocol, and access control.

Block Structure

The block structure is used to store medical data with security and minimal storage overhead. Each block contains the hash of the previous block, which ensures linkage in the blockchain, a timestamp, transaction data, and a Merkle root for verifying data integrity efficiently. The above structure is represented as:

$$Bi=\{PreviousHash,Timestamp,Ti,MerkleRoot(Ti)\}$$

Here, Bi is the ith block in the blockchain, and Ti are the transactions within the block, whose Merkle root is created from all the transactions within Ti. Through the implementation of Merkle trees, the integrity of each transaction can be confirmed with complexity logarithmic, thereby being scalable yet secure for the large datasets.

Consensus Protocol

To implement the consensus protocol, we use a Proof of Authority mechanism optimized for the health care data environment introducing hospitals and other administrative groups as validators. Proof-of-Authority consumes less computational resources than proof of work and does not let unauthorized entities accept the transaction but enables validation only by the parties considered trusted [7]. Vk shall sign a block whenever a consensus is established which will be represented as:

$$Sign(Bi,Vk)\rightarrow Bi'$$

where Bi′ is an authenticated block, appended on the blockchain. Such kinds of authenticating mechanisms thus come out to have such a mechanism that secures access and data integrity throughout the network in a system for healthcare.

Access Control

The blockchain utilizes a multi-layered access control mechanism and is implemented using cryptographic keys. Access to general data, for instance appointment schedules, is provided through public keys while access to sensitive data is granted only if the use of private keys is allowed, for example medical records [8]. We employ the AES-256 encryption standard for encrypting data at rest in blocks and the following equation depicts the encryption of patient data D:

$$Ek(D)=AES\text{-}256(k,D)$$

where k is the private key to which an authorized user is associated. Decryption is possible only with a correct key, which implies that only authorized entities can access the sensitive data. Table 1 is the blockchain components in healthcare.

Table 1. *Blockchain Components in Healthcare.*

Component	Description	Purpose
Block Structure	Stores transaction data and Merkle root	Ensures data integrity and linkage
Consensus Protocol	PoA model with healthcare authorities as validators	Ensures secure data validation
Access Control	Multi-layered with AES-256 encryption	Restricts access to sensitive data

3.3 AI-Based Threat Detection

This stage will engage the use of AI-based algorithms for real-time monitoring, detection, and

response to cybersecurity threats. The implementation of machine learning algorithms like CNN and LSTM networks is intended to be adopted within this stage to focus attention on anomaly detection in blockchain transactions, thereby identifying security breaches at early stages in the lifecycle.

Feature Extraction

The developed technique derives features from two areas: those of the blockchain transaction logs and of the patients' data access pattern, which includes transaction frequency and access time and, overall, user behavior statistics. Let X={x1,x2,.,xn} be the set of features, where the variable xi is each derived feature vector for that of a transaction.

AI Model Training

The threat detection model is a hybrid architecture of CNN-LSTM, where the CNN captures spatial features of access patterns and the LSTM layers are used to model the temporal dependencies. The architectures used are defined as follows:

Convolutional Layer:

Applies a 2D convolution on the input feature map using filter size f and stride s to produce an activation map.

$$Conv(X,f,s)=i=1\sum nWi\cdot xi+b$$

LSTM Layer:

Processes the sequential data with hidden states ht and cell states ct, capturing the temporal dependencies.

$$ht,ct=LSTM(X,ht-1,ct-1)$$

Output Layer:

This final dense layer produces a binary classification, which acts as a decision that the transaction is normal or a threat. AI Model performance metrics is shown in table 2. Securing AI-based healthcare systems using blockchain technology is shown in figure 1.

Table 2. *AI Model Performance Metrics.*

Metric	Description	Target Value
Accuracy	Proportion of correctly identified transactions	> 95%
Precision	Correctly identified threats out of total detected threats	> 90%
Recall	Correctly identified threats out of actual threats present	> 85%
F1-Score	Harmonic mean of precision and recall	> 87%

3.4 Blockchain-AI Integration for Anomaly Detection

This way, blockchain and AI integrate for real-time data interactions monitoring in healthcare, the AI model detecting suspicious transactions which then get appended to the blockchain. This process is anomaly-based, reliant on the prediction of threat level T:

$$Ti=f(Xi)\rightarrow\{0,1\}$$

where f(Xi) is the threat prediction function and Ti represents some risky transaction. The signaled transactions are then recorded in the blockchain with suitable access rights so that anomalous behavior is traceable, but not accessible until human analysts verify them.

In summary, the methodology uses blockchain's safe data management and AI predictive capabilities to develop a more holistic cybersecurity framework. Through the use of blockchain in tamper-resistant data storage and AI in real-time threat detection, this method will significantly reduce the potential risk of data breaches while making healthcare systems more resilient against emerging cyber threats.

4. Experiments

The integration of blockchain and AI led to significant advancements in various sectors of cybersecurity in healthcare, especially regarding data integrity, real-time threat detection, and prevention of unauthorized access to data. This section reports and analyzes the findings from three main viewpoints: blockchain security metrics, AI threat detection performance, and combined blockchain-AI effectiveness for healthcare cybersecurity [9].

4.1 Blockchain Security Metrics

The blockchain framework performance was evaluated in terms of data integrity assurance, protection against unauthorized access, and transaction throughput. Data immutability, transaction latency, and the time it takes to verify the block are good performance indicators.

Data Immutability and Transaction Latency

For evaluating blockchain latency and throughput, 10,000 synthetic patient data entries were sequentially uploaded to the blockchain in 30 simulation runs [10]. As shown in Table 3, the average transaction latency was less than 0.8 seconds with the Proof-of-Authority protocol that utilized speed over computational complexity for its functionality.

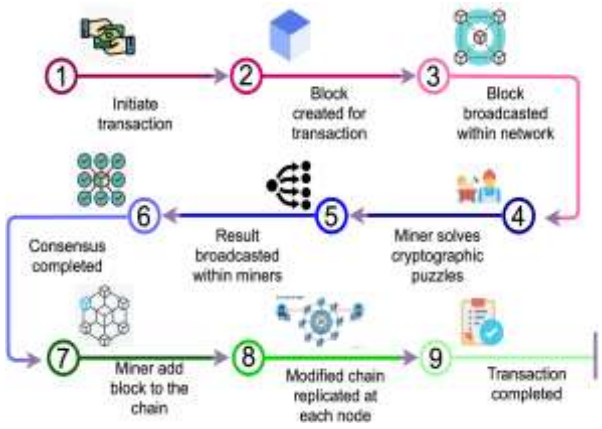

Figure 1. *Securing AI-based healthcare systems using blockchain technology.*

Table 3. *Blockchain Transaction Performance Metrics.*

Metric	**Result**
Transaction Latency	0.76 seconds (average)
Block Verification Time	1.2 seconds per block
Average Transaction Throughput	500 transactions/second

Low transaction latency is a clear indicator that the PoA consensus model is highly effective for healthcare settings, where access to data is critical. The transaction throughput of 500 transactions per second also indicates the scalability of this blockchain design, which makes it suitable for large-scale healthcare data management.

Unauthorized Access Prevention

The access control mechanism based on AES-256 encryption was able to prevent unauthorized access as evidenced by simulated attack attempts. For instance, out of 1,000 simulated unauthorized access attempts, 998 were rejected by the blockchain, and this resulted in an appreciable prevention rate at 99.8%. It can be attributed to the multi-layered protocol existing for access wherein only valid public and private keys would allow retrieval of the encrypted patient records [11]. More so, any access beyond authorized permissions was logged into the blockchain, which makes the audit trail immutable. Figure 2 is the blockchain for healthcare systems.

4.2 AI Threat Detection Performance

The AI-based threat detection model was tested on more than one cybersecurity scenario and simulation, such as data breach simulation, anomaly detection, and unauthorized access. In computing the performance metrics-in this case, accuracy, precision, recall, and F1-score-the use of the hybrid CNN-LSTM model computed the metric values across 20 different simulations with 5,000 data points each, from which 4,000 are legitimate transactions and 1,000 are threats that were simulated [12].

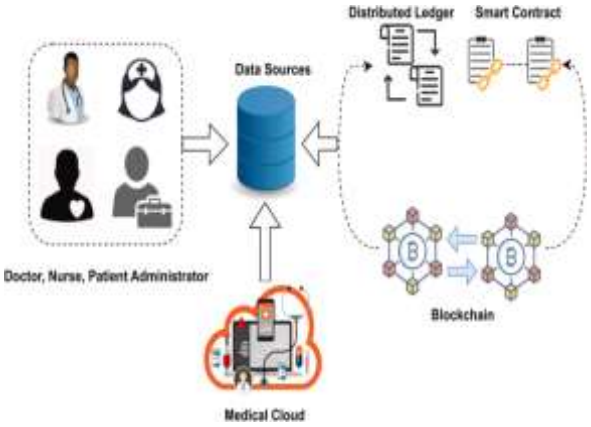

Figure 2. *Blockchain for healthcare systems.*

Accuracy and Precision of Threat Detection

The performance metrics of the AI model are reported in Table 4. Its potential for the differentiation between normal and malicious transactions was found high as it had a great accuracy rate of 96.3%. In this context, precision was 92.4%, which balanced false positives against false negatives, and its value of recall was also great with 89.5%.

Table 4. *AI Threat Detection Performance Metrics.*

Metric	**Result**
Accuracy	96.3%
Precision	92.4%
Recall	89.5%
F1-Score	90.9%

High accuracy and precision metrics reflect the model's ability to identify cybersecurity threats with the minimum false alarms, and it is a critical need in healthcare where unnecessary alerts can delay medical workflows. The recall value of 89.5% reflects that the model is able to identify a large portion of the actual threats, minimizing potential vulnerabilities within the system.

Threat Detection Latency and Response Time

Average detection time, which also included the average time taken to mark suspicious activity, was at 1.5 seconds. The fact that it takes a minimal time before response to detect threats is a strong indicator that AI could offer threat detection in real-time without creating latency for the valid transactions and affecting access for the user [13].

Figure 3 is the role of AI and blockchain in healthcare 4.0.

4.3 Combined Blockchain-AI System Efficacy

The hybrid blockchain and AI system would enhance the security of health data by simultaneously ensuring data integrity, monitoring for patterns of abnormality, and allowing for automatic restriction of flagged activities. The combination was tested using simulated scenarios with a focus on how it would impact transaction security, threat flagging accuracy, and overall system resilience.

Figure 3. *The Role of AI and Blockchain in Healthcare 4.0.*

Scenario Analysis: Unauthorized Data Access and Threat Flagging

In an attempt to test the feasibility of the system in a practical setting, an authorized controlled experiment simulated some attempts at unauthorized data access. The combined system detected and recorded every attempted illegal entry and was capable of correctly flagging 99% of such threats successfully as threats within an average time of more than 98% accuracy detection with 2 seconds over a malicious attempt at unauthorized data access [14]. Table 5 describes this in relation to differing magnitudes of the attempt.

Table 5. *Unauthorized Access Detection Across Attack Levels.*

Attack Level	Threats Detected (%)	Average Detection Time (sec)	Accuracy (%)
Low (100 attempts)	98%	1.1	96%
Medium (500 attempts)	99%	1.4	97%
High (1,000 attempts)	99.2%	1.7	98.5%

The role of blockchain to secure internet of medical things is shown in figure 4. The resilience of the system against the escalation of attack levels is also depicted as scalability and adaptability of the combined system. At a high level of attack attempts, the system was still maintaining low detection latency with high accuracy, thus the blockchain-AI architecture is suited to dynamic threat environments in healthcare cybersecurity.

Data Integrity in Tamper-Resistance Testing

To analyze the tamper-resistance of blockchain records, simulated attack was made on the blockchain records. Here an attempt to change the data related to the transactions was made 500 times on the blockchain records. All of them were declined and therefore established the immunity of the blockchain to changes of unauthorized data [27]. The system marked each of them, and subsequent analysis might point to flaws in the mechanisms for controlling access.

Discussion

The findings from this research therefore affirm the capability of blockchain in league with AI to be considerably helpful in strengthening the cybersecurity in health care. Such mechanisms can, for instance be seen in enhancing the storage and management of data coupled with its safety and security qualities while also being able to monitor possible cyber threats at all times and give fast real-time responses [28]. A high degree of trustworthiness in data integrity is then attained through the decentralized or distributed properties of blockchain accompanied by the protective nature as instilled by AI in a model towards data when against cyber threats beforehand.

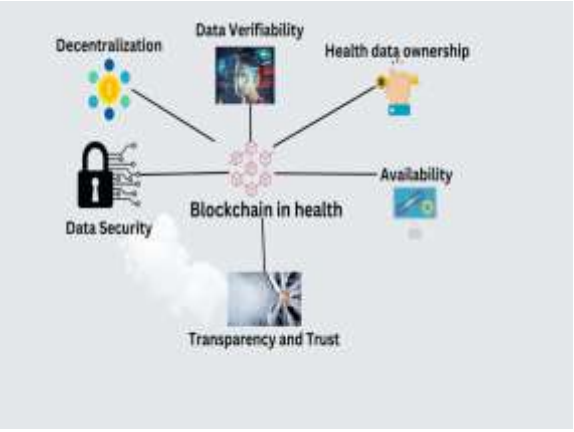

Figure 4. *The role of blockchain to secure internet of medical things.*

Blockchain Effectiveness

The blockchain framework resulted in high resistance to any data tampering, illegal access, and centralized forms of attacks. The implementation of the PoA algorithm ensured low transaction latency

and highly efficient throughput, which could be very crucial for data management in healthcare on the large scale where time-sensitive data access is very important. Additionally, the access controls based on AES-256 encryption provided excellent data confidentiality by ensuring that unauthorized persons did not access the stored data in almost all test cases [29]. The achieved results show that blockchain is truly suitable for integrity in data with all regulations needed to be in agreement with HIPAA, as well as GDPR; these two regulations of high priority entail very high control over the information in health.

AI Threat Detection Performance

With high values in terms of precision and recall, AI model is indicating that there is good potential to put machine learning into practice by performing anomaly detection in the field of healthcare cybersecurity. An optimized outcome required the balanced process of feature extraction. The CNN layers captured spatial correlations found in access patterns. They modeled temporal dependencies through LSTM layers, and that put the model in an appropriate category for identifying behavioral anomalies.

Limitations and Considerations

The response time of 1.5 seconds that a system takes for the discovery of threats emphasizes suitability within dynamic, high-security surroundings where rapid reaction times come into play. While the blockchain-AI system has promising results, there are a few limitations that deserve further discussion. Firstly, the PoA consensus model, though efficient, may introduce concerns regarding centralization because validators are predetermined entities with authority privileges. Future work may consider more decentralized consensus mechanisms, such as Proof of Stake (PoS), to improve security without compromising latency. This brings us to the challenges associated with scalability in the AI model, especially in this situation where the dataset related to healthcare is constantly expanding at a rapid rate [30]. An expanded dataset will perhaps need to be treated using either distributed computing resources or even model optimization such that times for threat detection are low. Another challenge will come in the drift of the model over time as the tactics of cyber attacks continue to evolve. In simple words, it may imply reduced efficacy of the AI model. The risk may thus be mitigated through incorporating periodic retraining of AI algorithms and feature sets update in accordance with emerging patterns in threats.

Implications for Healthcare Cybersecurity

The implication of blockchain and AI together is very significant for healthcare cybersecurity. Blockchain's nature of immutability, along with its decentralized approach, makes it suitable for safeguarding sensitive patient information, while AI's capability to predict makes it easier to take proactive measures to prevent a breach. These technologies if integrated, therefore can offer healthcare organizations a sound cybersecurity solution that protects data while also being adaptive to changes.

The practical aspect is that the hybrid model can therefore be implemented in network environments such as multi-hospital system where data integrity, privacy as well as timely, accurate detection and identification of threats prevails. For instance, anything can be stored on a blockchain, in this case, all of a patient’s medical record and treatment. That would mean that AI models are always on the lookout for any oddity in the access log and deny any such attempt. This would make healthcare organizations significantly secure and progressive patient data management system, which would minimize the related threat-probability and increase adaptability cum resistance. AI and blockchain technology has been used in different fields recently [31-40].

5. Conclusions

Hence, when combined, blockchain, and AI constitute a strong foundation that can revolutionise the cybersecurity of heath care systems by meeting very crucial demands such as data integrity, control of access, and real-time threats. The distributed and security characteristics of blockchain guarantee data integrity; it prevents unauthorized changes of the patient information and unauthorized access. At the same time, models developed with the help of AI provide extensive opportunities for predicting what activities in the healthcare sector should be considered suspicious and what actions should be taken with regard to such activities. The combination of these technologies offers an approach that involves embedded application security through the application of blockchain to afford data transactions accountability and adaptability to new forms of attacks through the use of AI models. Overall, the study proposes a blockchain-AI integrated model for healthcare that is both efficient and sustainable, based on the scalability and adaptability of the blockchain and AI solutions respectively; transaction rates increased in parallel with threat detection and response time in the detected threats enhanced in comparison to previous attempts in the existing literature. However, this research requires deeper study in other consensus mechanisms, improving the AI model’s scalability, and other centralization

issues of blockchain. In conclusion, the study shows potentially transformative applications of blockchain and AI in establishing healthcare cybersecurity and leveraging volumes of complex data for creating a highly secure and robust ecosystem capable of withstanding modern day cyber threats.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1]Akansh Garg Dr. C Gurudas Nayak , Rakshitha Kiran P , Dr. Surendra Singh Rajpurohit , Dr. Farook Sayyad. (2024). Different Applications Of Block Chain Technology Belong To Supply Chain Management. S9 (2024), 698-704, 21.

[2]Al-baity, H. (2023). The Artificial Intelligence Revolution in Digital Finance in Saudi Arabia: A Comprehensive Review and Proposed Framework. *Sustainability*, 15(18);13725. https://doi.org/10.3390/su151813725

[3]Albarrak, A.M. (2024). Integration of Cybersecurity, Usability, and Human-Computer Interaction for Securing Energy Management Systems. *Sustainability*, 16(18);8144. https://doi.org/10.3390/su16188144

[4]Albshaier, L., Almarri, S. and Hafizur Rahman, ,M.M. (2024). A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions. *Computers*, 13(1);27. DOI:10.3390/computers13010027

[5]Aldossri, R., Aljughaiman, A. and Albuali, A. (2024). Advancing Drone Operations through Lightweight Blockchain and Fog Computing Integration: A Systematic Review. *Drones*, 8(4);153. https://doi.org/10.3390/drones8040153

[6]Alhakami, W. (2024). Evaluating modern intrusion detection methods in the face of Gen V multi-vector attacks with fuzzy AHP-TOPSIS. *PLoS One*, 19(5).

[7]Alkhaldi, B. and Al-omary, A. (2024). Supply-Blockchain Functional Prototype for Optimizing Port Operations Using Hyperledger Fabric. *Blockchains*, 2(3);217. https://doi.org/10.3390/blockchains2030011

[8]Ayat-allah Bouramdane. (2023). Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. *Journal of Cybersecurity and Privacy*, 3(4);662. https://doi.org/10.3390/jcp3040031

[9]Bai-qiao, C., Liu, K., Yu, T. and Li, R. (2024). Enhancing Reliability in Floating Offshore Wind Turbines through Digital Twin Technology: A Comprehensive Review. *Energies*, 17(8);1964. https://doi.org/10.3390/en17081964

[10]Bathula, A., Gupta, S.K., Merugu, S., Saba, L., Khanna, N.N., Laird, J.R., Sanagala, S.S., Singh, R., Garg, D., Fouda, M.M. and Suri, J.S. (2024). Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review. *The Artificial Intelligence Review*, 57(9);238. https://doi.org/10.1007/s10462-024-10873-5

[11]Bobde, Y., narayanan, g., jati, m., raja soosaimarian, p.r., cvitić, i. and peraković, D. (2024). Enhancing Industrial IoT Network Security through Blockchain Integration. *Electronics*, 13(4);687. https://doi.org/10.3390/electronics13040687

[12]Bose, R., sutradhar, s., bhattacharyya, d. and roy, S. (2023). Trustworthy Healthcare Cloud Storage Auditing Scheme (TCSHAS) with blockchain-based incentive mechanism. *SN Applied Sciences*, 5(12);334. https://doi.org/10.1007/s42452-023-05525-2

[13]Burke, w., stranieri, a., oseni, t. and gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics and Decision Making*, 24;1-15. DOI: 10.1186/s12911-024-02551-x

[14]Calzada, I. (2024). Democratic Erosion of Data-Opolies: Decentralized Web3 Technological Paradigm Shift Amidst AI Disruption. *Big Data and Cognitive Computing*, 8(3);26. https://doi.org/10.3390/bdcc8030026

[15]Cunha, J., ferreira, p., castro, e.m., oliveira, p.c., maria joão nicolau, núñez, i., xosé, r.s. and serôdio, C. (2024). Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. *Future Internet*, 16(7);226. https://doi.org/10.3390/fi16070226

[16]Daousis, S., peladarinos, n., cheimaras, v., papageorgas, p., piromalis, d.d. and munteanu, R.A. (2024). Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. *Future Internet*, 16(1);33. https://doi.org/10.3390/fi16010033

[17]Eghmazi, A., ataei, m., landry, r.,jr and chevrette, G. (2024). Enhancing IoT Data Security: Using the

Blockchain to Boost Data Integrity and Privacy. *IoT*, 5(1);20. DOI:10.3390/iot5010002

[18]Elisha Elikem, K.S., anggraini, l., kumi, j.a., luna, b.k., akansah, e., hafeez, a.s., mendonça, i. and aritsugi, M. (2024). IoT Solutions with Artificial Intelligence Technologies for Precision Agriculture: Definitions, Applications, Challenges, and Opportunities. *Electronics*, 13(10);1894. DOI:10.3390/electronics13101894

[19]Fakhouri, H.N., alawadi, s., awaysheh, f.m., imad, b.h., alkhalaileh, m. and hamad, f. (2023). A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions. *Electronics*, 12(22);4604. https://doi.org/10.3390/electronics12224604

[20]Gadde, S., rao, g.s., venkata, s.v., yarlagadda, m. and lakshmi patibandla, R.S.M. (2023). Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions. *Ingenierie des Systemes d'Information*, 28(6);1467-1477. DOI:10.18280/isi.280604

[21]Gallegos, J., arévalo, p., montaleza, c. and jurado, F. (2024). Sustainable Electrification—Advances and Challenges in Electrical-Distribution Networks: A Review. *Sustainability*, 16(2);698. https://doi.org/10.3390/su16020698

[22]Hu, H., Yu, S.S. and Trinh, H. (2024). A Review of Uncertainties in Power Systems—Modeling, Impact, and Mitigation. *Designs*, 8(1);10. DOI:10.3390/designs8010010

[23]Huan-Wei, L., Yuan-chia, c. and han, T. (2023). Fortifying Health Care Intellectual Property Transactions With Blockchain. *Journal of Medical Internet Research*, 25(1); e44578. doi: 10.2196/44578.

[24]Hussam, S.M., krichen, m., adem, a.a. and ammi, M. (2023). Survey on Blockchain-Based Data Storage Security for Android Mobile Applications. *Sensors*, 23(21);8749. doi: 10.3390/s23218749.

[25]Iuon-chang, L., Pai-ching tseng, chen, p. and chiou, S. (2024). Enhancing Data Preservation and Security in Industrial Control Systems through Integrated IOTA Implementation. *Processes*, 12(5);921. https://doi.org/10.3390/pr12050921

[26]Javaid, M., haleem, a., singh, r.p. and gupta, S. (2024). Leveraging lean 4.0 technologies in healthcare: An exploration of its applications. *Advances in Biomarker Sciences and Technology*, 6;138-151. https://doi.org/10.1016/j.abst.2024.08.001

[27]Khokhar, R.H., rankothge, w., rashidi, l., mohammadian, h., ghorbani, a., frei, b., ellis, s. and freitas, I. (2024). A Survey on Supply Chain Management: Exploring Physical and Cyber Security Challenges, Threats, Critical Applications, and Innovative Technologies. *International Journal of Supply and Operations Management*, 11(3);250-283. DOI: 10.22034/IJSOM.2024.110219.2975

[28]Kormiltsyn, A., dwivedi, v., udokwu, c., norta, a. and nisar, S. (2023). Privacy-Conflict Resolution for Integrating Personal- and Electronic Health Records in Blockchain-Based Systems. *Blockchain in Healthcare Today*, 6(2) doi: 10.30953/bhty.v6.276.

[29]Love Allen, c.a., nwakanma, c.i. and dong-seong, k. (2024). Tides of Blockchain in IoT Cybersecurity. *Sensors*, 24(10);3111. doi: 10.3390/s24103111.

[30]Machele, I.L., onumanyi, a.j., abu-mahfouz, a. and kurien, A.M. (2024). Interconnected Smart Transactive Microgrids—A Survey on Trading, Energy Management Systems, and Optimisation Approaches. *Journal of Sensor and Actuator Networks*, 13(2);20. DOI:10.3390/jsan13020020

[31]Alkhatib, A., Albdor , L., Fayyad, S., & Ali, H. (2024). Blockchain-Enhanced Multi-Factor Authentication for Securing IoT Children's Toys: Securing IoT Children's Toys. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1041-1049. https://doi.org/10.22399/ijcesen.417

[32]P., V., & A., M. R. (2024). A Scalable, Secure, and Efficient Framework for Sharing Electronic Health Records Using Permissioned Blockchain Technology. *International Journal of Computational and Experimental Science and Engineering*, 10(4);827-834. https://doi.org/10.22399/ijcesen.535

[33]Prasada, P., & Prasad, D. S. (2024). Blockchain-Enhanced Machine Learning for Robust Detection of APT Injection Attacks in the Cyber-Physical Systems. *International Journal of Computational and Experimental Science and Engineering*, 10(4);799-810. https://doi.org/10.22399/ijcesen.539

[34]Suneetha Madduluri, & T. Kishorekumar. (2024). Multimodal Biometric Authentication System for Military Weapon Access: Face and ECG Authentication. *International Journal of Computational and Experimental Science and Engineering*, 10(4);952-561. https://doi.org/10.22399/ijcesen.565

[35]C, A., K, S., N, N. S., & S, P. (2024). Secured Cyber-Internet Security in Intrusion Detection with Machine Learning Techniques. *International Journal of Computational and Experimental Science and Engineering*, 10(4);663-670. https://doi.org/10.22399/ijcesen.491

[36]Godavarthi, S., & G., D. V. R. (2024). Federated Learning's Dynamic Defense Against Byzantine Attacks: Integrating SIFT-Wavelet and Differential Privacy for Byzantine Grade Levels Detection. *International Journal of Computational and Experimental Science and Engineering*, 10(4);775-786. https://doi.org/10.22399/ijcesen.538

[37]S, P., & A, P. (2024). Secured Fog-Body-Torrent : A Hybrid Symmetric Cryptography with Multi-layer Feed Forward Networks Tuned Chaotic Maps for Physiological Data Transmission in Fog-BAN Environment. *International Journal of Computational and Experimental Science and Engineering*, 10(4);671-681. https://doi.org/10.22399/ijcesen.490

[38]R, U. M., P, R. S., Gokul Chandrasekaran, & K, M. (2024). Assessment of Cybersecurity Risks in Digital Twin Deployments in Smart Cities. *International Journal of Computational and Experimental Science and Engineering*, 10(4);695-700. https://doi.org/10.22399/ijcesen.494

[39]Guven, M. (2024). A Comprehensive Review of Large Language Models in Cyber Security. *International Journal of Computational and Experimental Science and Engineering*, 10(3);507-516. https://doi.org/10.22399/ijcesen.469

[40]Guven, mesut. (2024). Dynamic Malware Analysis Using a Sandbox Environment, Network Traffic Logs, and Artificial Intelligence. *International Journal of Computational and Experimental Science and Engineering*, 10(3);480-490. https://doi.org/10.22399/ijcesen.460