AI-Driven Blockchain Framework for Secure Healthcare Data Interchange

Er. Radha Indoriya, Manan Chawla and Nitin Kumar

March 4, 2025

AI-Driven Blockchain Framework for Secure Healthcare Data Interchange

Er. Radha Indoriya
Department of Computer Science and Engineering
Chandigarh University
Mohali, India
indoriya.radha@gmail.com

Manan Chawla
Bachelors of Computer Science and Engineering
Chandigarh University
Mohali, India
chawlamanan25@gmail.com

Nitin Kumar
Bachelor of Computer Science and Engineering
Chandigarh University
Mohali, India
nitinyaduvansh32@gmail.com

***Abstract*—The healthcare industry faces significant challenges in ensuring the secure and efficient interchange of sensitive patient data. Traditional centralised systems are prone to security breaches, unauthorized access, and inefficiencies, making them unsuitable for modern healthcare demands. This paper proposes an AI-driven blockchain framework that combines blockchain's decentralization, immutability, and transparency with AI-powered security mechanisms for real-time threat detection and secure data exchange. The integration of AI enhances anomaly detection, access control, and encryption, ensuring a robust and scalable solution for healthcare data management. The proposed framework improves interoperability, privacy, and regulatory compliance while mitigating security vulnerabilities. By leveraging AI and blockchain, this model aims to establish a trustworthy and efficient ecosystem for healthcare data interchange, fostering innovation in digital healthcare solutions.**

Keywords—AI-driven security, Blockchain in healthcare, Secure data interchange, Healthcare data privacy, Decentralized data management, Smart contracts, AI-based anomaly detection, Interoperability in healthcare, Cybersecurity in healthcare, AI-blockchain integration.

I. Introduction

The healthcare industry creates enormous quantities of sensitive patient information that have to be kept confidentially stored, exchanged interchangeably and have controlled access. Centralised data management in traditional healthcare data systems mostly falls prey to data breaches, inefficiency, and non-interoperability, due to which healthcare organisations start having issues on the fronts of patient privacy, compliance, etc. With escalating cyber threats and sophisticated attacks all around, protecting and safeguarding these data become all the more significant than before [1].

Blockchain technology has been seen as a viable solution because of its decentralised, immutable, and transparent nature, which makes it highly suitable for the security of healthcare records[2]. Blockchain technology alone cannot solve all security issues like real-time threat detection, smart access control, and fraud detection [3]. This is where Artificial Intelligence (AI) comes into the picture. AI-based mechanisms can improve blockchain-based healthcare systems by identifying anomalies, authenticating automatically, and optimising encryption methods, thus providing a very secure and efficient data exchange system [4].

This work suggests an AI-based blockchain model that combines the strengths of the two technologies to provide security, privacy, and interoperability to healthcare data exchange. The model uses blockchain for immutable data storage and AI for real-time threat identification and smart data processing. By overcoming the shortcomings of the conventional data-sharing models, this work intends to transform healthcare data management and build a reliable and efficient digital healthcare ecosystem [5].

II. Literature Review

The convergence of blockchain and artificial intelligence (AI) in healthcare has turned heads with its promise of augmenting data security, privacy, and interoperability. This section looks back on studies undertaken on blockchain healthcare systems, AI-based security mechanisms, and the hurdles to secure healthcare data interchange.

1. Blockchain in Healthcare:
   Blockchain technology represents a decentralised immutable ledger system that promises to play an important part in securing data within healthcare settings. Research in this area involved electronic health records (EHRs) via blockchain-based system systems that keep patients' information safer while accommodating limited access permission to healthcare authorities [6]. Smart contract system within EHR systems through which access regulation happens automatically removes unauthorized alteration on healthcare records risk. Scalability, transaction acceleration, and integration concerns are existing huge hurdles as issues to use them on an extensive basis [7].

2. Security management of AI-enabled healthcare data
   Cybersecurity techniques applied by AI, like machine learning and deep learning, are increasingly being used in cyber analysis for anomaly detection and access control enhancements in healthcare systems [8]. AI-based security models can analyze enormous healthcare data in real time to improve threat detection and response time immensely. Some include fraud detection, unauthorized access, and optimization of encryption protocols for data protection [9]. Scalability and privacy remain challenging issues in their application in the medical field for AI-powered security systems[10].

3. Existing Blockchain-AI Solutions and Gaps:
   Several research studies have investigated the integration of AI and blockchain to secure data management, especially in industries like finance and supply chain. Yet, research on AI-based blockchain models for healthcare data exchange is still in its nascent stages. Most solutions available today concentrate on either blockchain or AI alone, without tapping into the synergistic strength of both technologies. Moreover, interoperability between

various healthcare providers is still a significant challenge, with the majority of blockchain implementations not having standardized data-sharing protocols [13].

An intriguing study has hypothesized a safe and trustworthy architecture for cyber-physical health care based on blockchain principles. This is dependent on technologies such as BigchainDB, Tendermint, and Inter-Planetary File System (IPFS) for data security and defence [14]. Patient-centred design provides greater information control to the patients, supported by blockchain for defence and privacy. Despite the aforementioned advancements, issues like system scalability, integration intensity, and matters of regulatory acceptability remain [15].

4. Need for an AI-Driven Blockchain Framework:
As existing healthcare data handling systems are less than ideal, an AI-enabled blockchain system represents a viable remedy with enhanced security, automation, and optimized protocols for data exchanges. By melding blockchain decentralization and immunity with AI threat intelligence and smart decision-making properties, healthcare organizations can get secure, clear, and large-scale data interchanges. In the future, blockchain scalability-amenable light models of AI that enable regulatory checks and smooth, interoperable transitions between heterogeneous networks of healthcare organizations need to be investigated.

In conclusion, although both blockchain and AI have alone considerable advantages in healthcare data security, their combination offers the complete solution to existing issues. The creation of an AI-based blockchain model could transform the management of healthcare data, providing strong security, privacy, and interoperability to the digital healthcare environment[19].

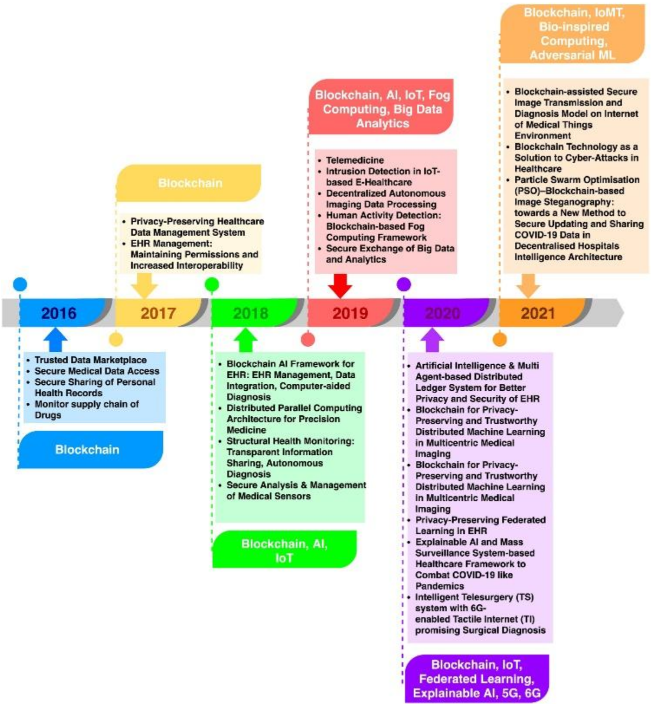
2016
2017
2018
2019
2020
2021
Blockchain
Trusted Data Marketplace
Secure Medical Data Access
Secure Sharing of Personal Health Records
Monitor supply chain of Drugs
Blockchain
Privacy-Preserving Healthcare Data Management System
EHR Management: Maintaining Permissions and Increased Interoperability
Blockchain, AI, IoT
Blockchain AI Framework for EHR: EHR Management, Data Integration, Computer-aided Diagnosis
Distributed Parallel Computing Architecture for Precision Medicine
Structural Health Monitoring: Transparent Information Sharing, Autonomous Diagnosis
Secure Analysis & Management of Medical Sensors
Blockchain, AI, IoT, Fog Computing, Big Data Analytics
Telemedicine
Intrusion Detection in IoT-based E-Healthcare
Decentralized Autonomous Imaging Data Processing
Human Activity Detection: Blockchain-based Fog Computing Framework
Secure Exchange of Big Data and Analytics
Blockchain, IoT, Federated Learning, Explainable AI, 5G, 6G
Artificial Intelligence & Multi Agent-based Distributed Ledger System for Better Privacy and Security of EHR
Blockchain for Privacy-Preserving and Trustworthy Distributed Machine Learning in Multicentric Medical Imaging
Blockchain for Privacy-Preserving and Trustworthy Distributed Machine Learning in Multicentric Medical Imaging
Privacy-Preserving Federated Learning in EHR
Explainable AI and Mass Surveillance System-based Healthcare Framework to Combat COVID-19 like Pandemics
Intelligent Telesurgery (TS) system with 6G-enabled Tactile Internet (TI) promising Surgical Diagnosis
Blockchain, IoMT, Bio-inspired Computing, Adversarial ML
Blockchain-assisted Secure Image Transmission and Diagnosis Model on Internet of Medical Things Environment
Blockchain Technology as a Solution to Cyber-Attacks in Healthcare
Particle Swarm Optimisation (PSO)–Blockchain-based Image Steganography: towards a New Method to Secure Updating and Sharing COVID-19 Data in Decentralised Hospitals Intelligence Architecture

Fig. 1 Blockchain Evolution in Healthcare

III. Proposed Framework

This part illustrates our new blockchain platform based on AI designed to secure and simplify the exchange of healthcare data. The platform synergizes the permanent, decentralized nature of blockchain and smart, timely threat detection and access control through AI to support enhanced data security, privacy, and interoperability. The framework is structured into three integrated layers that work together to ensure secure, efficient, and transparent healthcare data interchange. Below is a detailed explanation of the framework and the step-by-step data exchange process [20].

1. Data Transaction Layer: This bottommost layer is founded on a private blockchain network that stores all the transactions about healthcare data management. Its major functions are:

   Immutable Transaction Logging:
   Each healthcare data request, consent event, or access log is recorded as a transaction on the blockchain. These transactions are timestamped and include metadata (e.g., data hash, access permissions, and transaction identifiers).

   Smart Contract Enforcement:
   Two types of smart contracts are deployed in this layer:
   - EHR Manager Smart Contracts: These manage the storage, update, and retrieval of metadata associated with electronic health records (EHRs).
   - User Manager Smart Contracts: These handle user authentication, patient consent, and access permissions.

   The smart contracts will automatically apply pre-defined rules when a transaction is made, and the requests for data access will strictly follow the patient's consent and policies

2. AI Security and Analytics Layer: Placed right above the blockchain layer, this part utilizes artificial intelligence to provide security and guarantee the integrity of data transactions. Its key components are:

   Real-Time Monitoring:
   Machine learning algorithms continuously scan blockchain transaction information. Machine learning models are trained on historical healthcare information to recognize normal patterns of behaviour and to signal any deviations or abnormalities.

   Anomaly Detection:
   If a transaction strays from the normal patterns (e.g., unusual access requests or unusual transaction volumes), the AI system can automatically mark these events for closer examination or initiate automated countermeasures.

   Data Verification:
   The AI layer ensures the integrity of the data by checking the hash values on-chain and comparing them against the actual on-chain data for verification off-chain. This enables a consistent database of data origin and accuracy to be maintained.

3. Interoperability and Application Layer: This top layer provides a bridge between the secure blockchain environment and external healthcare applications. It handles the following functions:

Standardized Data Exchange:
The layer utilizes widely accepted healthcare data standards, such as Fast Healthcare Interoperability Resources (FHIR), to ensure that data exchanged between systems is consistent and compatible.

API-Based Interaction:
A set of secure application programming interfaces (APIs) facilitates communication between healthcare information systems (e.g., hospital EHR systems, clinical trial management systems) and the blockchain network. This allows external applications to send data requests, receive transaction statuses, and interact with smart contracts.

Off-Chain Data Storage Coordination:
Large files (like medical images and long test reports) are kept off-chain in secure storage systems. The blockchain only keeps a reference (like a cryptographic hash and a pointer or link) to this off-chain data, maintaining data integrity without clogging the blockchain.

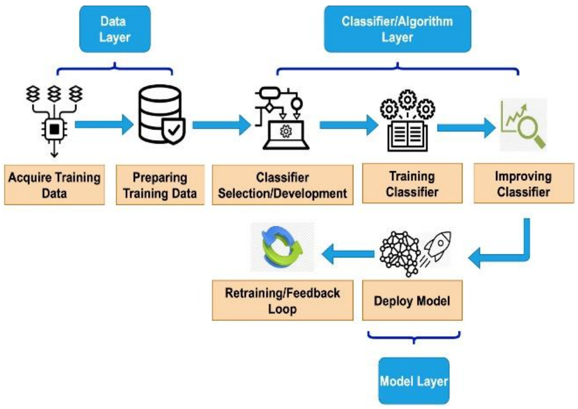

Fig. 2 Phases involved in deploying AI models.

Process Flow: The complete data interchange process within the framework proceeds as follows:

1. Data Preparation and Encryption: Healthcare data is first encrypted and tokenized. A cryptographic hash of the data is generated, and this hash, along with relevant metadata (e.g., patient identifiers, timestamps, and data location), is recorded on the blockchain. The actual data is stored in a secure off-chain storage.

2. Initiation of Data Request: A healthcare provider or application (e.g., a clinical trial system) requests data through the interoperability layer. The request is structured in compliance with standardized procedures and sent over secure APIs to the blockchain network.

3. Smart Contract Execution: The smart contracts on the data transaction layer automatically receive the request. They verify if the request is by patient consent and access policies. If the request is valid, the smart contract logs the transaction and permits the request to proceed.

4. Real-Time Verification and Monitoring: At the same time, the AI security layer tracks the transaction in real time. The AI algorithms verify the transaction's integrity by comparing the on-chain metadata with off-chain data references. Any inconsistencies prompt an alert or automatic response to maintain data security.

5. Data Retrieval and Exchange: Once the transaction is validated and approved, the interoperability layer retrieves the reference to the off-chain data. The requesting application then accesses the required data from the off-chain repository using secure protocols. The entire process is logged on the blockchain for future auditability and traceability.

This multi-layered method guarantees secure, transparent, and efficient healthcare data interchange. Each layer has specialized functions that together ensure data integrity and patient privacy and facilitate seamless interoperability among healthcare systems.

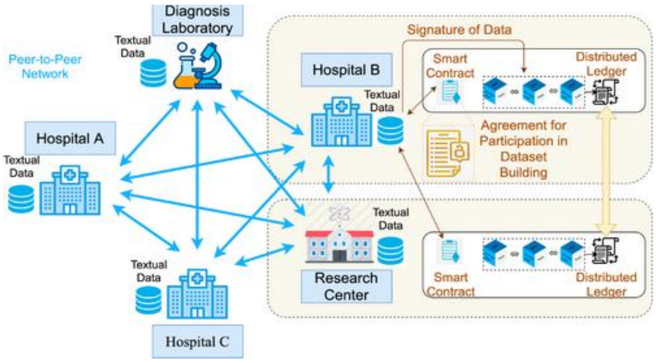

Fig. 3 Dataset building with Blockchain in Healthcare applications

IV. Benefits and Challenges

The integration of blockchain and AI in healthcare data exchange offers benefits like enhanced security and transparency but also presents challenges like complexities, computational overhead, scalability constraints, and regulatory barriers.

Benefits:

1. Enhanced Data Security and Integrity

Immutable Record-Keeping: Immutable Record-Keeping: Blockchain's decentralized ledger ensures that every transaction—ranging from data requests to patient consent events—is recorded in an immutable, tamper-evident manner. That feature avoids unauthorized data modifications and allows for a trustworthy audit trail for compliance and forensic purposes [1],[3],[5].

Real-Time Threat Detection: Real-Time Threat Detection: By continuously monitoring transaction patterns, and the integration of AI models, the security posture is improved. These models are trained to detect anomalies (e.g., unexpected access requests or abnormal transaction frequencies), thereby enabling immediate remediation actions. This dualistic protection, integrating the immutable ledger with predictive AI monitoring, effectively reduces risks like data leakage and/or fraud [2],[6],[12].

Data Integrity Verification: Data Integrity Verification: As it stores cryptographic hashes on-chain and confidential off-chain storage for the actual data, the architecture allows data integrity to be cross-verified on an ongoing basis. Whenever there is a change in the off-chain data it immediately generates a hash mismatch and alerts to possible tampering[8].

2. Patient-Centric Data Control

Granular Consent Management: Granular Consent Management: Smart contracts are programmed to enforce patient consent dynamically. Patients may define and dynamically change access permissions, allowing access to the patient's data only to certain authorized healthcare providers or applications. This level of control fosters trust and respects patient autonomy, aligning with stringent privacy regulations [7],[15].

Transparent Audit Trails: Transparent Audit Trails: Each access request and data sharing are logged on the blockchain, which routes patients and auditors with full transparency and verifiability regarding who accessed their data and at what point. This transparency is confidence-building for patients about how their confidential health information is being treated [9].

3. Improved Interoperability and Traceability

Standardized Data Exchange: Standardized Data Exchange: The use of healthcare standards such as FHIR within the interoperability layer guarantees that data from diverse systems is standardized so that it can be transferred in an unobstructed and efficient manner between different healthcare providers and institutions [10],[14].

Cross-System Traceability: Cross-System Traceability: Blockchain’s transparent ledger and traceability mechanisms allow for the complete tracking of data provenance. Individual transactions are identifiable, facilitating tracing of the source and history of modification of data, which is essential for both clinical decision-making and regulatory compliance [19].

4. Efficient Data Exchange

Optimized Storage and Retrieval: Optimized Storage and Retrieval: The framework uses a hybrid approach where large data files are stored off-chain, while the blockchain maintains only essential metadata (such as cryptographic hashes and pointers). This architecture reduces blockchain storage costs but guarantees retrieval efficiency and security [13].

Automated Process Execution: Automated Process Execution: Smart contracts enable the automatic realization of data acquisition and data exchange procedures. This automation reduces human error, speeds up transactions, and ensures that all operations adhere to predefined security policies without manual intervention [4].

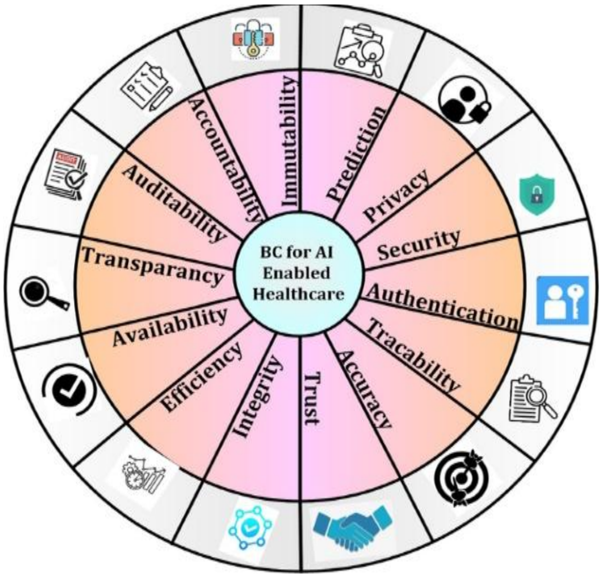

Fig. 4 Blockchain for AI-enabled Healthcare

Challenges

1. Integration Complexity

System Interoperability: Integration of blockchain and AI into current healthcare IT platforms can be tricky because of the variety of legacy systems. Establishing robust interfaces (e.g., through standardized APIs) that allow seamless communication between old and new systems is complex and requires meticulous planning and development.

Multi-Layer Synchronization: Multi-Layer Synchronization: The need for a sophisticated orchestration mechanism that ensures that all three layers, i.e. blockchain ledger, the AI security module and the interoperability platform, operate synchronously without data loss or delays arises. Coordination between these layers, especially at heavy throughput, is an important technical bottleneck [7],[12].

2. Computational Overhead:

Real-Time Analytics Demands: Real-Time Analytics Demands: Continuous running of machine learning analytics on blockchain transaction data is computationally intensive. Real-time analysis of huge volumes of data can lead to an increase in latency and energy consumption, which need to be optimized but with no compromise in security [11].

Consensus Algorithm Complexity: Consensus Algorithm Complexity: Despite a more performant consensus protocol (e.g., proof of stake or PBFT), the distributed model of blockchain already includes redundancies in computations over all nodes. Balancing the need for robust consensus with computational efficiency is a persistent challenge, particularly as the network scales [1].

3. Scalability Issues

Transaction Throughput: Transaction Throughput: As healthcare data volumes increase, ensuring that the blockchain network can handle a high number of concurrent transactions without significant delays is crucial. The limitations of many blockchain protocols, as they relate to transaction throughput, may make separate scalability options like sharding or off-chain processing more desirable, which adds to the complexity of the problem.

Storage Demands: Storage Demands: While the framework alleviates such problems by offloading the huge data files off-chain, the blockchain needs to deal with the incremental data arrival of metadata and transaction records. With the increase in number of transactions, it is possible to increase the amount of storage and the number of duplications that are required by the blockchain network, which might be detrimental to the performance [9].

4. Regulatory and Standardization Barriers

Compliance with Privacy Regulations: Information in healthcare is subject to strict laws, like the HIPAA law, the GDPR and others. Applying a decentralized system such as blockchain to meet such regulatory standards while preserving the benefits of transparency and immutability carries complex legal and technical implications.

Interoperability Standards: Interoperability Standards: The difficulty of interoperability standards to be accepted on a global scale for blockchain-incorporated health systems adds to the complexity of the integration process. Differences in the types of data and protocols in different areas and institutions can make it difficult to exchange information without effort and to continue with the standardization of practice [20].

5. Adoption and Usability Challenges

User Training and Change Management: User Training and Change Management: Healthcare professionals, patients, and administrative personnel may have a lack of familiarity with blockchain and artificial intelligence technologies. The complexity of such systems requires a large amount of training and change management approaches to guarantee successful adoption and proper use.

User Interface Design: User Interface Design: Creating intuitive and easy-to-use interfaces that hide the underlying technological nuances and deliver reliable functionality is a key factor in their ultimate deployment. Maintaining an accessible platform to nontechnical users without impacting security or feature performance is a design challenge that continues [17].

This detailed benefits and challenges section outlines the multifaceted advantages of integrating AI and blockchain in healthcare data interchange, while also addressing the significant technical, regulatory, and operational hurdles that must be navigated for successful deployment.

V. FUTURE SCOPE AND EMERGING TRENDS

The integration of AI-driven blockchain frameworks in healthcare data exchange is still in its early stages, but it holds significant promise for future improvements. As technology advances, we can expect several developments that will enhance security, interoperability, and efficiency in managing healthcare data. This section looks at potential future advancements and emerging trends that could transform the secure sharing of healthcare information:

1. Improvements in AI-Driven Security Mechanisms Future versions of AI algorithms are expected to become more adept at identifying cyber threats, unauthorized access, and irregularities in blockchain transactions. Enhanced machine learning models will improve real-time fraud detection, allowing for a proactive stance on healthcare data security. Moreover, AI-driven predictive analytics will enable healthcare providers to foresee and address risks before they become serious issues.

2. Integration with Decentralized Identity Management Decentralized identity (DID) solutions based on blockchain technology have the potential to transform how patients are identified and how they manage their data. By removing the need for centralized authorities, patients can maintain self-sovereign identities, granting them secure and verifiable access to their health records across various healthcare providers without the need for intermediaries. This method will bolster privacy, minimize identity fraud, and streamline access control.

3. Interoperability with Global Healthcare Systems Future blockchain networks are likely to enhance interoperability among healthcare institutions around the globe. Emerging standards, such as Fast Healthcare Interoperability Resources (FHIR) and HL7, will continue to develop, facilitating seamless data exchange between different electronic health record (EHR) systems. This will simplify cross-border healthcare data sharing, leading to better international patient care and collaborative medical research.

4. Scalability Solutions for Blockchain Networks
   To tackle the existing challenges in transaction speed and storage, future advancements will introduce sophisticated blockchain scalability solutions, including:
   Sharding: This involves splitting blockchain networks into smaller segments to enhance transaction processing speed.
   Layer-2 Solutions: Certain transactions will be handled on secondary layers (like sidechains or state channels) to alleviate congestion on the primary blockchain.
   Hybrid Blockchain Models: By merging private and public blockchains, we can optimize both security

and performance while adhering to healthcare regulations.

5. Smart Contracts with Dynamic Access Control: Smart contracts are set to advance with more dynamic and context-sensitive access control features. Future innovations may include multi-factor authentication, AI-driven policy enforcement, and adaptive permissions based on real-time risk evaluations. This will guarantee that only authorized individuals can access sensitive health information while ensuring compliance with regulatory standards.

6. Adoption of Quantum-Safe Cryptography: With the rise of quantum computing, conventional cryptographic techniques may face risks of decryption attacks. Future blockchain frameworks will adopt quantum-resistant encryption algorithms to safeguard data and provide long-term security against new cyber threats. Post-quantum cryptography (PQC) is anticipated to become a norm in blockchain-based healthcare systems.

7. Blockchain-Enabled AI Models for Predictive Healthcare: The integration of blockchain and AI will facilitate predictive analytics in healthcare. By securely compiling anonymized patient data from various institutions, AI can offer valuable insights into disease trends, treatment efficacy, and personalized medicine. This will enhance clinical decision-making and enable early disease detection while ensuring patient privacy through blockchain-based data governance.

The future of AI-driven blockchain frameworks for healthcare data exchange looks bright, as ongoing advancements improve security, efficiency, and interoperability. With the evolution of emerging technologies like quantum computing, decentralized identity, and AI-driven analytics, healthcare systems stand to gain from more robust, scalable, and intelligent data-sharing methods. Nevertheless, continued research, regulatory changes, and collaborative innovation will be essential for successful adoption and meaningful real-world impact.

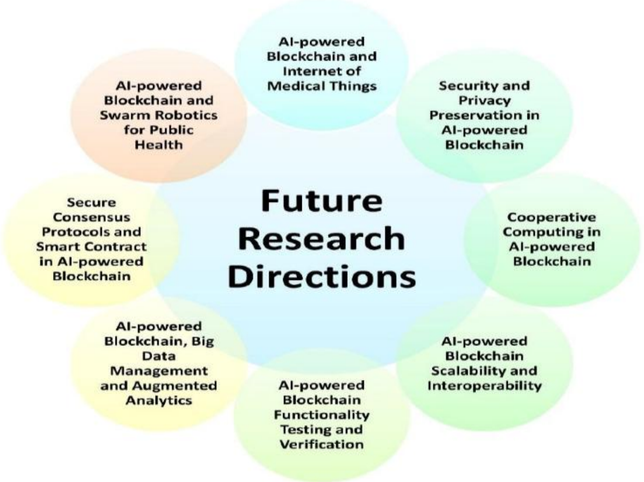
AI-powered Blockchain and Internet of Medical Things
Security and Privacy Preservation in AI-powered Blockchain
Cooperative Computing in AI-powered Blockchain
AI-powered Blockchain Scalability and Interoperability
AI-powered Blockchain Functionality Testing and Verification
AI-powered Blockchain, Big Data Management and Augmented Analytics
Secure Consensus Protocols and Smart Contract in AI-powered Blockchain
AI-powered Blockchain and Swarm Robotics for Public Health
Future Research Directions

Fig. 5 AI-Powered Blockchain Technology Future Research

VI. CONCLUSION

The blockchain framework driven by AI for secure healthcare data exchange presents a groundbreaking solution to the issues surrounding medical data security, privacy, and interoperability. By merging the decentralized and unchangeable nature of blockchain with AI’s smart threat detection and automation features, this approach guarantees secure record-keeping, safe data transactions, and effective management of patient-centred data. Healthcare organizations can take advantage of real-time fraud detection, automated consent management, and smooth data sharing while adhering to global data protection laws [1].

However, despite its many benefits, several challenges need to be tackled for effective implementation. Integrating blockchain and AI into current healthcare systems demands significant technological investments, a skilled workforce, and clearly defined interoperability standards. Scalability is a major concern, as blockchain networks must handle large amounts of healthcare transactions efficiently without delays. Furthermore, ensuring compliance with data privacy regulations like HIPAA and GDPR remains a persistent challenge, requiring standardized legal frameworks for blockchain-based healthcare solutions.

Looking forward, improvements in blockchain scalability methods such as sharding, layer-2 protocols, and hybrid models will boost transaction efficiency and lessen computational demands. AI-driven security advancements will keep progressing, allowing for proactive threat detection, adaptive authentication methods, and real-time fraud prevention. Decentralized identity management (DID) will also empower patients, giving them complete control over their medical data and improving secure interoperability across platforms. These developments will lead to a more robust and patient-focused healthcare data ecosystem.

In conclusion, despite the challenges that lie ahead, the promise of AI-driven blockchain frameworks to transform healthcare data sharing is significant. Overcoming issues related to scalability, regulations, and integration will require ongoing research, technological advancements, and thoughtful policy development to achieve widespread use. By encouraging collaboration among researchers, healthcare professionals, policymakers, and tech developers, this framework can facilitate secure, transparent, and efficient exchanges of healthcare data, ultimately enhancing patient outcomes and reinforcing the global healthcare system [5],[17].

VII. REFERENCES

[1] Bathula, A. (2024). Efficient blockchain-based framework for secure online data sharing in education and ai-driven healthcare domains (Doctoral dissertation, Bennett university).

[2] Das, S. R., Jhanjhi, N. Z., Asirvatham, D., Rizwan, F., & Javed, D. (2025). Securing AI-Based Healthcare Systems Using Blockchain Technology. In AI

Techniques for Securing Medical and Business Practices (pp. 333-356). IGI Global.

[3] Ramachandran, M. (2024). AI and blockchain framework for healthcare applications. Facta Universitatis, Series: Electronics and Energetics, 37(1), 169-193.

[4] Devarapu, K. (2020). Blockchain-Driven AI Solutions for Medical Imaging and Diagnosis in Healthcare. Technology & Management Review, 5(1), 80-91.

[5] Rathore, N., Kumari, A., Patel, M., Chudasama, A., Bhalani, D., Tanwar, S., & Alabdulatif, A. (2025). Synergy of AI and Blockchain to Secure Electronic Healthcare Records. Security and Privacy, 8(1), e463.

[6] Omidian, H. (2024). Synergizing blockchain and artificial intelligence to enhance healthcare. Drug Discovery Today, 104111.

[7] Kasula, B. Y. (2023). Synergizing AI, IoT, and Blockchain: Empowering Next-Generation Smart Systems in Healthcare. International Journal of Sustainable Development in Computing Science, 5(2), 60-64.

[8] Boi, B., & Esposito, C. (2025). The Role of Blockchain in AI-Driven Medical Cyber-Physical Systems. In Artificial Intelligence Techniques for Analysing Sensitive Data in Medical Cyber-Physical Systems: System Protection and Data Analysis (pp. 127-142). Cham: Springer Nature Switzerland.

[9] Taherdoost, H. (2025). AI-powered blockchain technology in healthcare. In The Digital Doctor (pp. 25-39). Academic Press.

[10] Tatineni, S. (2022). Integrating AI, Blockchain and cloud technologies for data management in healthcare. Journal of Computer Engineering and Technology (JCET), 5(01).

[11] KM, S. K., & Parkar, T. V. (2025). AI, Blockchain, and Cybersecurity: Shaping the Future of Data Integrity and Security in Healthcare. In Intelligent Systems and IoT Applications in Clinical Health (pp. 27-52). IGI Global.

[12] Sabharwal, S. M., Chhabra, S., & Aiden, M. K. (2024). AI and Blockchain for Secure Data Analytics. In Next-Generation Cybersecurity: AI, ML, and Blockchain (pp. 39-81). Singapore: Springer Nature Singapore.

[13] Pamulaparthyvenkata, S., Murugesan, P., Gottipalli, D., & Palanisamy, P. (2024, September). AI-Enabled Distributed Healthcare Framework for Secure and Resilient Remote Patient Monitoring. In 2024 5th International Conference on Smart Electronics and Communication (ICOSEC) (pp. 2034-2041). IEEE.

[14] Simonoski, O., & Bogatinoska, D. C. (2024). Block MedCare: Advancing healthcare through blockchain integration with AI and IoT. *arXiv preprint arXiv:2412.02851*.

[15] Kumari, S., Tyagi, A. K., & Ahmad, S. S. (2025). Blockchain technology in AI-powered smart hospital. In Blockchain and Digital Twin for Smart Hospitals (pp. 109-132). Elsevier.

[16] Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., ... & Rahman, M. H. (2021). Blockchain and artificial intelligence technology in e-Health. Environmental Science and Pollution Research, 28, 52810-52831.

[17] Upadhyay, J., Singh, S. K., Kar, N. K., Pandey, M. K., Gupta, P., & Tiwari, P. (2024). Healthcare Data Security Using AI and Blockchain: Safeguarding Sensitive Information for a Safer Society. In Next-Generation Cybersecurity: AI, ML, and Blockchain (pp. 159-178). Singapore: Springer Nature Singapore.

[18] Biswas, I., & Singh, R. K. (2024). "Application Of AI And Blockchain In Healthcare Industry"–A Review. Journal of Advanced Zoology, 45(2).

[19] Aydin, F., & Başaran, C. H. (2025). Blockchain revolution: Transforming digital health for a secure future. In Digital Healthcare, Digital Transformation and Citizen Empowerment in Asia-Pacific and Europe for a Healthier Society (pp. 475-502). Academic Press.

[20] Bathula, A., Gupta, S. K., Merugu, S., Saba, L., Khanna, N. N., Laird, J. R., ... & Suri, J. S. (2024). Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review. Artificial Intelligence Review, 57(9), 238.