frontiers | Frontiers in Communications and Networks

TYPE Original Research
PUBLISHED 16 April 2025
DOI 10.3389/frcmn.2025.1538965

OPEN ACCESS

EDITED BY
Tong Wang,
Hubei University of Economics, China

REVIEWED BY
Yilei Wang,
Qufu Normal University, China
Shitharth Selvarajan,
Leeds Beckett University, United Kingdom

*CORRESPONDENCE
Minhee Jun,
junm@cua.edu

RECEIVED 03 December 2024
ACCEPTED 01 April 2025
PUBLISHED 16 April 2025

CITATION
Jun M (2025) Platform framework for blockchain-enhanced healthcare AIoT systems. *Front. Commun. Netw.* 6:1538965. doi: 10.3389/frcmn.2025.1538965

Platform framework for blockchain-enhanced healthcare AIoT systems

Minhee Jun*

Greens Laboratory, Department of Electrical and Computer Engineering, The Catholic University of America, Washington, DC, United States

Blockchain and Artificial Intelligence (AI) technologies offer immense potential when integrated with the Internet of Things (IoT) across multiple sectors, including healthcare. Blockchain remains an active research topic, particularly regarding its scalability and the time efficiency of its verification process. However, limited attention has been given to the practical challenges of integrating blockchain with AIoT (AI with IoT) in healthcare applications, that face persistent privacy and security challenges due to the sensitive nature of personal data. These challenges include time-consuming data retrieval and increased memory usage, which impact the practical implementation of blockchain-based AIoT systems. To address these challenges, this paper proposes a platform framework that integrates edge AI with a sharding-based proof-of-authority (PoA) blockchain for healthcare systems. The proposed framework incorporates three key strategies for blockchain applications in healthcare: 1) a blockchain version manager for AI adaptors, 2) IoT preprocessing for blockchain data management, and 3) the Shall Fragment Cube (SFC) approach for blockchain decision archiving. Theoretical analysis demonstrates that the use of a sharding blockchain significantly enhances memory efficiency and reduces data retrieval time in healthcare AIoT applications. Moreover, simulation results indicate that the SFC approach reduces data retrieval time by approximately 50%. Thus, the proposed system design provides a practical and reliable solution for integrating blockchain into future healthcare AIoT systems, unlocking transformative potential across multiple application domains.

KEYWORDS

Artificial-intelligence-of-things (AIoT), Artificial intelligence (AI), internet-of-things (IoT), blockchain, smart systems, platform framework, health care

1 Introduction

The Artificial-Intelligence-of-Things (AIoT) represents a powerful convergence of advanced Artificial Intelligence (AI) and Internet-of-Things (IoT), offering transformative potential to drive innovation and shape the future (Era et al., 2024; Singh et al., 2020). Recent breakthroughs, exemplified by AI language models such as ChatGPT and CoPilot, showcase AI's rapid advancement toward human-like intelligence, achieving remarkable accuracy when trained on extensive datasets. However, a critical challenge in advancing AI lies in the substantial costs of generating or accessing the vast amounts of data required for training. To addresses this challenge, IoT can provide the real-world data necessary for AI training and decision-making. Recently, IoT systems have increasingly been adapted for the AI implementation, unlocking their full potential by

enabling smarter, more efficient, and autonomous operations, which drive innovation across a wide range of applications. By integrating real-time IoT data streams with AI's analytical capabilities, AIoT enables complex advisory and decision-making processes, delivering optimized solutions across a range of fields. This synergy can create more efficient AI systems that significantly enhance automation and decision-making across various sectors, included in smart cities, healthcare, and industrial operations. To address these issues, blockchain technology emerges as a promising complementary solution due to its secure, decentralized, and immutable nature in managing digital records (Kilroy et al., 2023). Blockchain operates as a distributed ledger that records transactions across a peer-to-peer network, ensuring transparency and eliminating the need for centralized control. Unlike traditional systems, blockchain transactions are validated through consensus mechanisms, enhancing security and trustworthiness. Despite its advantages, blockchain remains an active research area, especially concerning its scalability and the efficiency of its verification processes. Recent studies (Pal et al., 2023; Kuznetsov et al., 2024; Salama et al., 2023) have explored the integration of blockchain with AIoT applications, highlighting its potential to enhance security, reliability, and functionality. Notably, blockchain adoption is expected to facilitate secure and responsible AIoT data management across various sectors, including healthcare.

However, practical challenges persist when integrating blockchain with AIoT in healthcare applications. Healthcare AIoT systems must address critical issues such as data privacy, security vulnerabilities, and operational efficiency. The sensitive nature of healthcare data necessitates robust privacy safeguards, yet AIoT systems remain susceptible to cyber threats, including data leakage by querying on AI model. Additionally, blockchain's implementation in AIoT introduces challenges such as time-intensive data retrieval and increased memory usage, which may hinder real-time performance.

Overcoming these limitations is essential for the development of scalable and secure AIoT solutions in healthcare. To tackle these challenges, this study proposes a platform framework that integrates blockchain with healthcare AIoT systems through three critical design aspects: AI-driven privacy and security for healthcare data, a blockchain-based efficient data retrieval framework, and key strategies for seamless AIoT-blockchain integration. First, to safeguard sensitive healthcare data, this study adopts an *Edge AI* approach, which enables local data processing instead of relying on cloud storage. By processing data closer to its source, Edge AI enhances privacy protection, reduces latency, and minimizes operational costs. Given the stringent privacy requirements in healthcare, this localized approach mitigates data exposure risks while ensuring secure storage and processing. Second, to optimize blockchain performance in healthcare AIoT applications, this study introduces a *sharding-based PoA blockchain model*. Unlike traditional consensus mechanisms, sharding partitions the blockchain into smaller, manageable segments, allowing parallel processing to improve scalability and reduce latency. Furthermore, the PoA consensus mechanism, which relies on designated authorities for transaction validation, lowers computational overhead while maintaining security. Third, to enable seamless integration of blockchain with healthcare AIoT systems, this study introduces three essential strategies in blockchain: a Blockchain Version Manager for AI Adaptors to facilitate dynamic optimization and data protection; IoT Preprocessing for Blockchain Data Management to improve data structuring; and *The Shall Fragment Cube (SFC) Approach* for efficient data retrieval from blockchain decision archivier, making AIoT applications more practical in real-time healthcare environments.

This study contributes to the practical implementation of blockchain within healthcare AIoT systems through the following key contributions. First, it identifies and addresses the major challenges of integrating blockchain with AIoT in healthcare, particularly concerning data privacy, retrieval time, and memory overhead. Second, It proposes a *privacy-enhancing* Edge AI framework and a *sharding-based PoA blockchain* model to optimize security and efficiency in healthcare applications. Third, it introduces a structured approach for AIoT-blockchain integration, featuring a blockchain version manager, IoT preprocessing, and the SFC model to facilitate scalable and effective data management.

The remainder of this paper is structured as follows: Section 2 discusses the evolution of AIoT data collection, IoT adaptation, and their synergistic impact. Section 3 reviews existing challenges in AIoT systems and the benefits of blockchain integration, along with recent advancements in blockchain for IoT and AI. Section 4 presents the proposed platform framework and its key strategies for blockchain adoption in healthcare. Section 5 evaluates the proposed framework through simulations. Sections 6 and 7 provide a discussion of findings and conclude the study.

2 Background—AIoT systems

2.1 Data collection evolution for AI system developments—IoT adaptation

The AI development process has been moved forward like the following three stages, as shown in Figure 1. In the initial stage of Figure 1A, AI developers lay the groundwork for the entire process. This involves setting up methods for data collection, preprocessing the collected data, and simulating AI models to define their potential capabilities. This initial stage is pivotal for establishing a solid foundation for the subsequent phases, ensuring clarity in goals and workflows. During this phase, data collection involves significant costs, primarily due to the setup and investigation required to establish data collection mechanisms. In Figure 1B, the developing stage transitions into active AI model development and training. At this point, data collection often becomes a separate process from the direct control of AI developers, as research in AI model development has grown into a highly active field. Data is sourced from various sectors and undergoes preprocessing, a task handled by dedicated data collection specialists, ensuring its quality and usability for AI development. The developing stage's AI development involves building, training, and refining the AI model while its data collection performs data collection, preprocessing, and annotation to prepare high-quality datasets, where emphasizes standardized data processing and comparison to evaluate the performance of various AI models. In the final stage of Figure 1C, the research focus

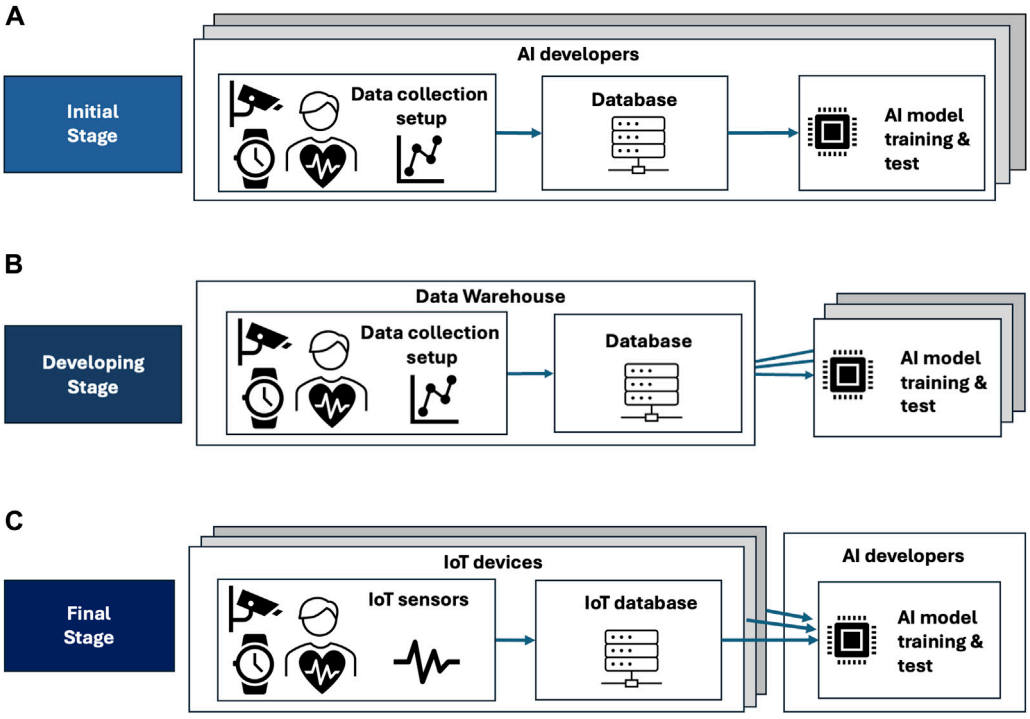

FIGURE 1
(A): Initial Stage–AI developers design the AI model and conduct preliminary testing using data they have collected themselves. **(B)**: Developing stage–The AImodel is developed with the support of an independent DataWarehouse resource specializing in data collection, ensuring high-quality and relevant data for the model. **(C)**: Final Stage–IoT sensors are integrated to supply real-time, practical data to the developed AI model, enabling it to function effectively in real-world applications.

shifts to deploying the AI model into production environments and ensuring its seamless integration with IoT systems. IoT devices provide continuous data streams, supporting the model's decision-making and enabling real-time updates. Activities in this stage include monitoring performance, gathering feedback. By leveraging IoT-generated data for retraining, this stage provides real-time and time-series data, enabling seamless adaptation of AI models to practical, real-world scenarios. The outcome of this stage is a fully operational and optimized AI system, designed for sustained deployment and use.

2.2 AIoT systems' synergies

2.2.1 The role of IoT in AIoT systems

IoT plays a pivotal role in enhancing the capabilities of AI by providing vast amounts of real-world data and enabling AI systems to interact with the physical environment (Baranwal Somy et al., 2019). First, IoT sensors offer a practical solution for balancing cost-effectiveness with enhanced AI system capabilities. Traditional methods of data collection require significant initial investments in infrastructure and devices, along with ongoing maintenance and upgrades for additional AI model training. IoT sensors reduce the randomness of data collection processes while providing reliable and scalable data inputs, lowering the cost barriers associated with infrastructure setup. Second, Big data is an essential component of AI system development, and IoT addresses challenges in data collection by generating large volumes of real-world, real-time data from various sensors. This data serves as the foundation for AI systems to analyze patterns, derive insights, and make predictions. By offering diverse and abundant data sources, IoT strengthens the ability of AI to perform complex decision-making and improve model accuracy. Third, IoT environments act as dynamic, real-world testing platforms for AI algorithms and models. Through constant streams of user-generated data, IoT enables AI systems to learn, adapt, and improve continuously in response to new contexts. This real-time feedback loop ensures that AI models evolve and remain relevant in changing environments. Thus, integrating IoT networks, AI systems gain access to critical data, fostering advancements in training, analysis, and adaptation for real-world applications.

2.2.2 The role of AI in AIoT systems

AI enhances IoT systems by analyzing data, predicting trends, and enabling autonomous decision-making, optimizing efficiency and reducing human intervention (Singh et al., 2020; Sherin et al., 2023). First, AI can forecast trends, predict potential issues, and identify maintenance needs based on sensor data from IoT devices. Building on its data analysis, AI offers predictive capabilities that are especially vital for smart systems, such as smart agriculture, where anticipating conditions like weather changes, soil health, or equipment failures can lead to more informed decision-making and resource optimization. Second, AI transforms IoT systems by enabling automatic management and autonomous decision-making.

Based on the insights and predictions derived from IoT data, AI reduces the need for human intervention in repetitive and exhaustive tasks. This streamlined decision-making process not only saves time and costs but also facilitates the development of smarter, more efficient systems for future applications, ensuring scalability and reliability in diverse domains. Third, AI plays a critical role in enhancing IoT systems by processing the vast amounts of data generated by IoT devices and extracting meaningful insights. By analyzing and identifying unusual patterns in IoT data streams, AI can distill valuable information into compressed parameters, making data storage and retrieval more efficient. This ability to process and summarize large datasets allows IoT systems to function more intelligently and efficiently in real-world applications. Thus, incorporating AI into IoT systems unlocks their full potential by enabling smarter, more efficient, and autonomous operations, while the convergence of AI and IoT drives innovation across diverse industries including Healthcare. In conclusion, exploring the synergies of integrating AI and IoT technologies highlights that AIoT holds promise for the future, with its ability to operate autonomously with human-like intelligence, and significantly enhance efficiency while reducing operational costs.

3 Literature review

It is found that AIoT technology is a promising future technology by integration of AI and IoT technologies. Despite of its immense potential, AIoT systems face dominant challenges from IoT-related limitations and AI-related limitations.

3.1 AIoT systems' challenges

3.1.1 AI-related challenges in AIoT systems

AIoT systems face several critical limitations in their AI components that must be addressed to ensure reliability, adaptability, and security in dynamic and interconnected environments (Kawamoto and Kobayashi, 2020). First, reliable AI systems are essential for building user trust and meeting regulatory compliance. These systems must not only meet technical standards but also align with socially responsible principles such as safety and accountability. This includes addressing risks associated with accidents or incorrect decisions to reduce unexpected failures and enhance the practical utility of AI in real-world applications. Second, AIoT systems need to maintain AI model for system adaptability in dynamic, real-world contexts. Adapting to changing environments and infrastructure, AI systems are susceptible to model and data drift over time, as changes in data distribution or user behavior can degrade their performance. Furthermore, managing multiple versions of AI models is particularly complex in distributed AIoT systems. Robust mechanisms are needed to address these challenges to maintain system reliability. Third, the interconnected and dynamic nature of AIoT systems exposes them to evolving threats and adversarial attacks. Ensuring the security of AI systems, AIoT systems can remain resilient, trustworthy, and capable of adapting to emerging challenges in a rapidly changing threat landscape. Addressing these limitations is crucial for the sustainable development and widespread adoption of AIoT systems. Thus, AIoT systems must address limitations in reliability, adaptability, and security by ensuring trustworthiness, managing model drift and updates, and implementing robust cybersecurity measures to thrive in dynamic and interconnected environments.

3.1.2 IoT-related challenges in AIoT systems

The rapid expansion of IoT systems brings immense potential for innovation but also introduces critical challenges in data privacy, management, and security that must be addressed to ensure their reliability and user trust (Wu et al., 2022; Douligeris and Mitrokotsa, 2004; AuthorAnonymous et al., 2023). First, IoT data management presents significant privacy challenges as sensitive information transmitted between IoT devices can be intercepted if robust security measures are not implemented. Many IoT devices lack the processing power required to support advanced security protocols, making them susceptible to unauthorized access. The collection of vast amounts of personal data further amplifies these privacy concerns. To gain user trust and ensure effective IoT data collection, it is crucial to prioritize robust data privacy measures and implement comprehensive security frameworks. Second, the hybrid nature of IoT data, encompassing structured, unstructured, and semi-structured formats, adds complexity to data management in AIoT systems. This heterogeneity, combined with the sheer volume of data from diverse sensors and devices, poses challenges for efficient processing, storage, and analysis. Robust frameworks capable of managing data variability and ensuring scalability are essential for IoT systems to deliver timely and reliable decision-making capabilities. Without these solutions, IoT networks may face significant bottlenecks, reducing their effectiveness and performance. Third, IoT devices are inherently vulnerable to cyberattacks due to their limited security features and interconnected nature. These vulnerabilities allow hackers to exploit unsecured devices, gain control of entire networks, launch large-scale attacks, or spy on users. The openness and heterogeneity of IoT systems further exacerbate these risks by creating multiple points of entry for potential breaches. Strengthening IoT security through advanced protection measures, such as access control, data encryption, and intrusion detection, is critical to maintaining user trust and ensuring the resilience of AIoT systems in the face of evolving threats. Thus, effective IoT implementation requires addressing challenges in data privacy, hybrid data management, and cybersecurity to ensure secure, efficient, and reliable systems.

With the understanding of challenges and opportunities in AIoT systems, the discussion naturally transitions to blockchain technology, a transformative innovation that addresses key issues such as security, transparency, and data integrity.

3.2 Blockchain overview

Blockchain technology, first introduced with Bitcoin in 2008 by an individual under the pseudonym Satoshi Nakamoto, has evolved into a revolutionary framework for secure and decentralized data management (Bodkhe et al., 2020; Ferdous et al., 2020; Deng et al.,

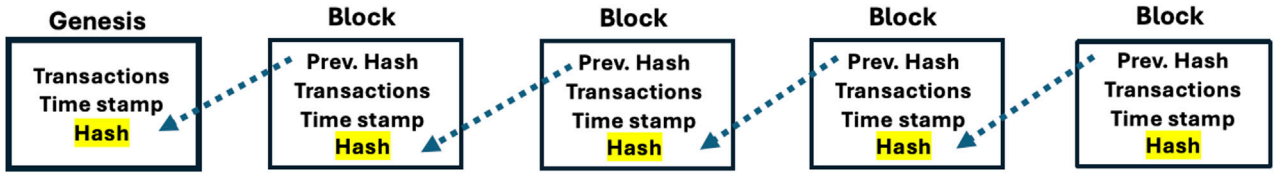

FIGURE 2
Single-chain blockchain structure: A single-chain blockchain is a linear, sequential structure where blocks are added in a continuous chain, one after another. Each block contains a hash of the previous block. This type of blockchain is widely used in cryptocurrencies like Bitcoin and Ethereum, prioritizing security and decentralization.

2022; Chen et al., 2018). At its core, blockchain operates as a distributed ledger where data is organized into immutable blocks linked sequentially in a chronological chain. Each block contains essential components: transaction data, a timestamp, and a cryptographic link to the previous block (called a hash) as shown in Figure 2. Blockchain's operation relies on decentralized nodes that validate and record transactions, ensuring transparency and security without the need for centralized oversight. Consensus algorithms are fundamental to maintaining the trust and immutability of blockchain networks (Zoican et al., 2018). These algorithms, including Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS), validate and confirm transactions by requiring agreement among network participants before appending new blocks, while Proof-of-Authority (PoA) (Hammad et al., 2023) has a limited pre-approved number of trusted authorities valide new blocks (Ferdous et al., 2020; Deng et al., 2022). Two primary types of blockchain networks facilitate different use cases: public blockchains, which are open and permissionless, allowing anyone to participate (e.g., Bitcoin and Ethereum); and private blockchains, which are permissioned, restricting access to specific organizations or users for enhanced control and privacy. A key feature of blockchain is the integration of smart contracts—self-executing agreements with terms encoded directly into their structure (Baranwal Somy et al., 2019; Salama and Al-Turjman, 2022). Smart contracts enable automatic, transparent, and tamper-proof execution of processes, such as financial transactions, supply chain management, and digital identity verification, reducing the need for intermediaries. This automation enhances blockchain's ability to deliver efficient and secure operations across a wide range of applications (Douligeris and Mitrokotsa, 2004; Chaganti et al., 2022; Mollah et al., 2021). Blockchain technology is built on a structured architecture with five hierarchical layers (Uddin et al., 2021): Data layer securely stores transaction records in an immutable, tamper-resistant ledger. Network Layer facilitates communication and synchronization among decentralized nodes. Consensus Layer validates transactions using robust consensus algorithms. Execution layer processes smart contracts, enabling automated and programmable functions. Application layer provides user-facing functionalities and interfaces for various use cases. Together, these layers form a versatile and robust architecture capable of supporting a wide range of industries and applications.

Blockchain technology offers a range of significant benefits, making it a powerful solution for various industries (Sherin et al., 2023; Harris and Waggoner, 2019; Salama and Al-Turjman, 2022;

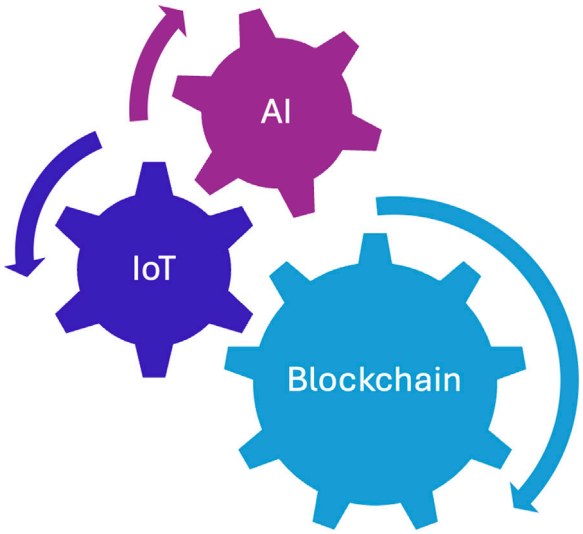

FIGURE 3
Blockchain strengthens IoT by addressing data privacy, access control, data management, and cybersecurity, while also supporting AI with improved reliability, system management, and context awareness. Integrating blockchain technology, AIoT systems achieve greater stability and enhanced services.

Saad et al., 2020; Li et al., 2020). One of its key advantages is immutability, ensuring that once data is recorded in a blockchain, it cannot be altered or deleted, fostering trust and accountability. Transparency is another vital feature, as blockchain allows all authorized participants to access the same version of the ledger, reducing information asymmetry and enhancing trust. Additionally, traceability enables precise tracking of transactions and assets, which is particularly valuable in industries like supply chain management and finance. Blockchain also provides robust security against cyberattacks, including Distributed Denial of Service (DDoS) attacks, by leveraging decentralized nodes and cryptographic algorithms to prevent single points of failure. Finally, the inclusion of smart contracts automates processes and enforces agreements without intermediaries, ensuring efficiency, accuracy, and tamper-proof execution. Together, these features make blockchain a secure, transparent, and efficient technology for applications demanding trust and reliability.

Based on the unique characteristics, blockchain technology builds users' trust in AI-driven decision-making due to offer

greater opportunities, and it is expected to support robust and secure AI system in future in (Kilroy et al., 2023). Furthermore, the blockchain technology's functions seems to be a good answer for these challenges of future AIoT systems.

3.3 Blockchain adaptation to overcomes AIoT challenges

Blockchain technology presents a promising solution for addressing the critical challenges faced by AIoT systems, mentioned in Section 3.1 as shown in Figure 3, including data privacy, security, adaptability, and transparency, enabling more efficient and reliable operations in dynamic environments.

The integration of AI and blockchain has garnered significant research attention in recent years. For instance, (Harris and Waggoner, 2019), proposes a blockchain-based platform for smart contracts that integrates machine learning and blockchain frameworks, enabling continuous updates to AI models. A key challenge identified in this study is maintaining model integrity in the presence of low-quality or ambiguous data. To address this, the authors highlight the need for mechanisms to recover corrupted AI models, identifying this as a critical area for future research. Similarly, (Kawamoto and Kobayashi, 2020), introduces an AI pedigree verification platform built on blockchain technology. This system tackles the challenges of reproducing AI models, even when using identical datasets and algorithms, by providing a blockchain-backed solution to improve reproducibility. By ensuring comprehensive data verification, the platform addresses a fundamental barrier to developing trustworthy AI systems. Furthermore, (Salama and Al-Turjman, 2022), proposes an innovative AI-based blockchain data processing approach aimed at facilitating real-time learning within distributed big data frameworks. While this study focuses on AI's potential to enhance blockchain systems, it also underscores the reciprocal benefits of using blockchain to strengthen AI systems in terms of security, privacy, and traceability.

Recent research has increasingly explored the integration of blockchain technology with AI to address vulnerabilities in IoT data collaboration and enhance AI model performance. (Chavali et al., 2020). emphasize the complementary relationship between AI and blockchain, highlighting how blockchain can resolve several critical challenges in AI development, including accessing large datasets, ensuring unbiased learning, and safeguarding privacy. The study demonstrates blockchain's potential to improve AI transparency, facilitate decentralized data sharing, and create secure audit trails. Together, these findings envision a long-term symbiotic relationship between AI and blockchain, paving the way for mutually transformative advancements in both technologies.

The integration of blockchain technology supports the creation of secure, shared marketplaces for exchanging data, models, and computational resources, positioning AI and blockchain as central drivers of digital transformation and intelligence augmentation. Blockchain's decentralized architecture offers a secure and transparent framework that addresses critical challenges such as ensuring data quality, mitigating bias, and protecting privacy. For instance, (Baranwal Somy et al., 2019), explores the use of blockchain to build trust in an AI marketplace for collaborative machine learning. Their proposed platform enables secure data sharing and collaborative model training by recording all transactions on a blockchain. This approach ensures transparency in processes such as data partitioning, distribution, and training scheduling while safeguarding the confidentiality of data and models. Similarly, (Dinh and Thai, 2018), highlights blockchain's transformative potential for AI through secure data marketplaces. They propose that blockchain empowers users by granting them control over their data, allowing it to be monetized via smart contracts without intermediaries. This not only mitigates privacy risks but also enhances AI training by ensuring access to abundant, high-quality data. Collectively, these studies emphasize the importance of blockchain-enabled AI data provisioning platforms as foundational tools for future advancements in AI.

These foundational studies highlight the transformative potential of integrating AI, IoT, and blockchain, while also identifying key challenges and opportunities for future research. By leveraging blockchain's capabilities, trustworthy AIoT infrastructures can be developed, enabling these technologies to reach their full potential across diverse applications, including healthcare, supply chain management, and smart cities.

For instance, (Alrebdi et al., 2022; AuthorAnonymous et al., 2023; Haleem et al., 2021; Shmatko and Kliuchka, 2022), demonstrate how blockchain streamlines medical record management and supply chain processes, empowering patients with greater control over their data. Similarly, (Sherin et al., 2023), explores the integration of AI and blockchain to create intelligent supply chains, where AI analyzes large datasets to identify patterns and anomalies, and blockchain ensures traceability and transparency, thereby enhancing efficiency. In the context of smart cities, (Singh et al., 2020), proposes a blockchain framework that incorporates IoT within AI systems to improve urban management and functionality. Additionally, studies such as (Mollah et al., 2021; Wang et al., 2017; Gai et al., 2019) showcase blockchain's role in smart grid systems, where it enhances data security, facilitates decentralized energy trading, and optimizes grid management efficiency. The integration of blockchain with AIoT (AI and IoT) presents a promising avenue for addressing critical challenges, particularly in mitigating cybersecurity risks. While significant progress has been achieved, further research is needed to fully harness the synergistic benefits of these technologies, ensuring their transformative impact across industries.

Finally, (Pal et al., 2023; Kuznetsov et al., 2024; Salama et al., 2023), highlight that while blockchain holds significant potential to enhance the security of AI agents and IoT sensors, there remains a notable gap in comprehensive research on this topic. They emphasize the urgent need to investigate how blockchain platforms can be effectively utilized to develop secure and responsible AIoT systems.

3.3.1 Key benefits of blockchain in AIoT applications

First, blockchain technology offers powerful solutions to address key challenges in AIoT systems, particularly those related to data privacy, security, adaptability, and transparency (Uddin et al., 2021). By enabling pseudonymous transactions, blockchain protects user identities while facilitating secure data exchange. Users can define permissions for data access, ensuring sensitive information is only

available to authorized parties. This approach enhances data security and trust, promoting data integrity and encouraging collaborative AI development across different organizations. These capabilities are especially critical in AIoT environments, where vast amounts of data must be shared responsibly to support AI model training and decision-making. Second, smart contracts, a core feature of blockchain, can automate essential processes in AIoT systems, such as device authentication, data exchange, and payment settlements. By reducing reliance on intermediaries and manual operations, blockchain-driven automation lowers operational costs and minimizes delays. This efficiency is vital for managing the complex and dynamic nature of AIoT systems, where seamless coordination between devices and systems is required. Smart contracts also enhance system reliability by ensuring that predefined conditions are automatically executed, reducing the risk of human error. Third, blockchain's cryptographic techniques address security vulnerabilities in AIoT systems by securing data transmission between IoT devices and reducing the risk of unauthorized access (Sengupta et al., 2020). Once data is recorded on the blockchain, it becomes immutable, ensuring the integrity of information collected by IoT devices. This feature is critical in AIoT applications, where accurate and reliable data is essential for training AI models and generating meaningful insights. By securing the data pipeline, blockchain prevents tampering and fosters trust in AI-driven outcomes.

Furthermore, another major benefit of blockchain is its ability to enhance transparency and accountability (Chavali et al., 2020). Every transaction or data input recorded on the blockchain is traceable, providing a clear audit trail for AI decision-making processes. This transparency is crucial for industries that require compliance with regulations and ethical standards, such as healthcare, finance, and autonomous systems. By enabling detailed monitoring of how AI algorithms reach their conclusions, blockchain ensures that AIoT systems operate with greater accountability and reliability. Lastly, blockchain can support better AI model management (Kawamoto and Kobayashi, 2020) and data quality in AIoT systems (Harris and Waggoner, 2019). By leveraging decentralized networks, AI models can be trained and deployed without the risk of single points of failure, ensuring continuous availability even in distributed environments. This decentralization also enables edge computing, allowing AI models to process data closer to the source. This proximity improves response times, reduces latency, and enhances the overall efficiency of AIoT systems. By integrating blockchain, AIoT systems can overcome critical challenges and unlock their full potential for innovation and reliability.

3.4 Additional blockchain contributions

Blockchain plays an auxiliary role in AIoT systems by supplying contextual data, enabling AI systems to make more informed decisions. While IoT devices provide real-time data streams, blockchain can add layers of contextual information like age, gender, occupation, or preferences, enhancing AI's ability to tailor personalized services for users. For example, in healthcare, blockchain securely provides additional personal data, while IoT devices may monitor biometric and vital signs such as heart rate and blood pressure, to help AI deliver more accurate diagnostics or treatment recommendations. This synergy improves AI's accuracy and effectiveness in creating user-specific experiences across various applications.

Also, blockchain supports the training and adaptation of AI models in AIoT systems by enabling decentralized learning methods, such as federated learning (Salama and Al-Turjman, 2022). IoT devices generate a continuous flow of data that allows AI models to learn and adapt in real time. Blockchain can facilitate the training of these models across multiple devices without the need to share raw data, preserving user privacy and ensuring data security. This decentralized approach allows multiple parties to contribute to and benefit from shared AI models, fostering innovation through collaborative development. By promoting collective efforts, blockchain enables more efficient AI model training and enhances the scalability of AIoT systems.

Blockchain can facilitate secure and decentralized data sharing among entities while ensuring data privacy and ownership (Baranwal Somy et al., 2019). Blockchain's immutable ledger ensures that data cannot be tampered with, providing a secure and trustworthy source for AI to analyze. This can be particularly useful in sectors where AI data integrity and sharing is crucial, such as finance, healthcare, and supply chain management.

By addressing the inherent challenges and additional contributions for AIoT systems, blockchain paves the way for more reliable and trustworthy AIoT applications. This synergy not only optimizes device performance but also fosters innovation and growth in various industries leveraging AIoT technologies.

4 Platform framework for healthcare: blockchain-enhanced AIoT system

This section introduces a platform framework designed to enhance healthcare AI systems through blockchain-integrated AIoT. As illustrated in Figure 4, the proposed framework leverages synergistic interactions between healthcare data, AI systems, and IoT devices. By integrating blockchain into healthcare AIoT, AI-driven healthcare applications can securely access personal medical records stored on the blockchain and manage access control for data obtained from personal IoT sensors. While healthcare AIoT focuses on personal data privacy, protection from data thieves, and need-based data sharing, smart cities and other AIoT applications prioritize trust in digital data, prevention of manipulation (e.g., 51% attack), and real-time data sharing as given in Table 1. Thus, to enhance data privacy, healthcare AIoT systems prefer Edge AI over Cloud AI.

Existing blockchain approaches encounter major challenges when applied to healthcare AIoT, particularly in terms of memory overhead and data retrieval time, as outlined below.

First, memory efficiency is a bottleneck for large-scale healthcare data. Unlike conventional blockchain applications such as cryptocurrency transactions, which deal with small, discrete data records, healthcare AIoT systems handle massive and continuously generated medical data from electronic health records and IoT-based health monitoring devices. The sheer volume and rapid

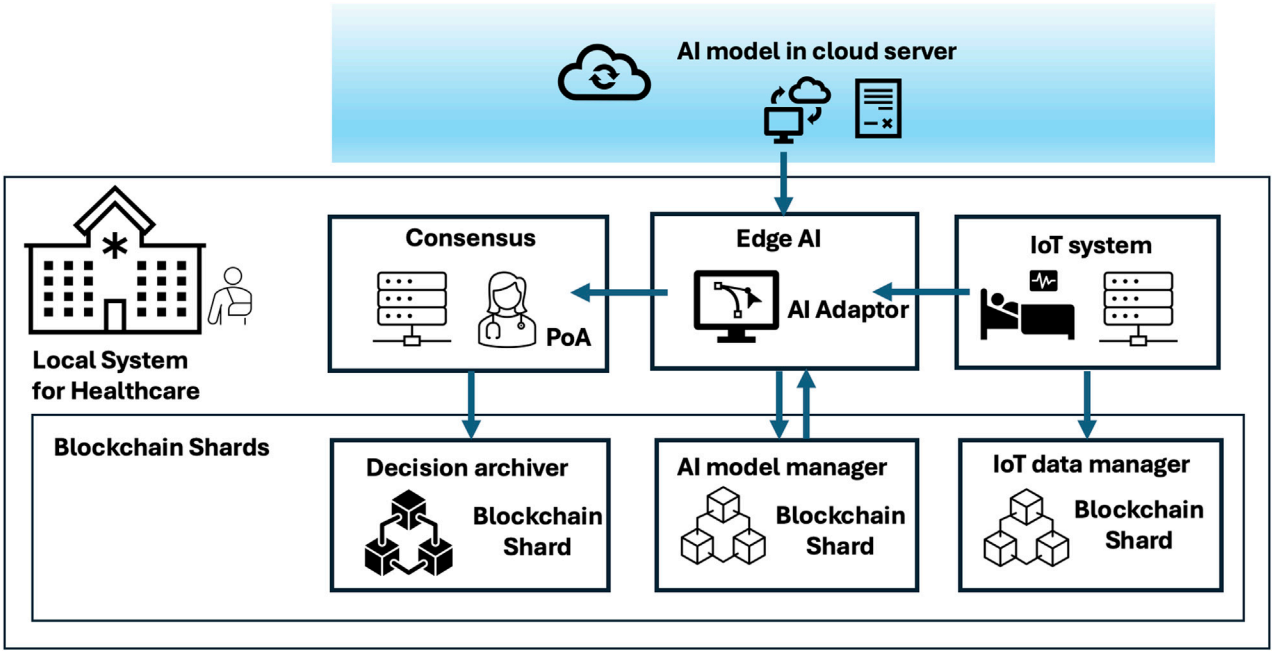

FIGURE 4
The architecture of blockchain-enhanced healthcare AIoT systems consists of three sharding blockchains integrated with the healthcare AIoT framework. It incorporates edge AI, which interfaces with local IoT devices. A blockchain-based data manager securely connects the IoT database with AI agents operating locally or in the cloud. Additionally, a blockchain AI model manager oversees AI model management, considering AI model licenses and medical data expiration. Lastly, a blockchain decision archiver, validated through proof-of-authority (PoA) consensus, records the decision-making processes of AI assistants and medical providers.

TABLE 1 Key aspects of healthcare and smart cities and other applications in terms of data privacy, security concerns, data sharing needs, and AI system architecture. To prioritize data privacy, the AI system in healthcare AIoT is preferred to Edge AI rather than Cloud AI.

	Healthcare	Smart cities and other applications
Data	Privacy of personal information	Trust on digital data
Security agenda	Data thieves (e.g., extraction attacks)	Data manipulation (e.g., 51% attack)
Data Share	In needs	In real time
AI system architecture	Edge AI	Cloud AI

generation of personal medical data introduce memory overhead challenges for blockchain-based storage at nodes. Thus, it is essential for efficient architecture of data memory utilization in order to ensure the feasibility of scalable Healthcare AIoT applications.

Second, the time efficiency of data retrieval is a critical concern in healthcare AIoT applications. While traditional blockchain solutions focus on optimizing transaction verification time for cryptocurrency and smart contracts, they do not address the latency issues associated with retrieving past medical records. In healthcare settings, AI models continuously require access to historical patient data for training and real-time decision-making. Delays in retrieving medical data from a blockchain hinder AI system performance and reduce the system's practical usability for medical providers and patients.

Third, beyond blockchain security, AI models and IoT devices introduce additional security vulnerabilities that must be addressed. AI models processing sensitive medical data are susceptible to data exposure risks, where private information can be inferred from model queries. Public blockchain architectures, while ensuring decentralized security, do not inherently provide protection against AI-specific threats such as model inversion attacks or data leakage. Similarly, IoT sensors collecting personal health data are prone to unauthorized access and malicious tampering. Therefore, a robust security framework is necessary to protect patient privacy and AI model integrity while integrating blockchain with healthcare AIoT.

To address these challenges, this paper proposes an edge AI system architecture with blockchain and IoT integration, offering a scalable and efficient solution for healthcare AIoT systems. The designed framework aims to optimize memory usage for storing and retrieving large-scale medical data in a blockchain-based environment, improve data retrieval efficiency by leveraging sharding and structured storage techniques to minimize latency when accessing historical records, and enhance security by protecting sensitive patient data while maintaining the decentralized benefits of blockchain technology.

4.1 Edge AI system for healthcare applications and blockchain

This paper considers the Edg AI system as the appropriate architecture in health AIoT applications while it has been considered that cloud AI system gets benefits from blockchain directly because blockchain can plays a pivotal role in AI systems by addressing data ownership and privacy concerns while ensuring secure data provenance. For example, when the AI system is developed using federated learning in the distributed network, blockchain empowers data owners with full control over their personal and IoT-generated data, enhancing privacy and security through blockchain-enabled access control mechanisms. Additionally, it facilitates secure data sharing and supports decentralized marketplaces via smart contracts, enabling data owners to monetize their data while maintaining privacy.

However, the cloud AI system is not preferable environment in healthcare applications for the following reasons. First, one of the benefits of this edge AI system in healthcare, rather than cloud AI, is que to patients' privacy and data security of querying sensitive healthcare information in AI system. The well-known act of extracting or stealing sensitive information from an AI model through queries is called Model Extraction Attacks: In Membership Inference Attack, the attacker queries the model to determine whether specific data points were part of the training dataset, potentially leaking sensitive user information; In Data Reconstruction Attack, the attacker exploits query responses to reconstruct actual training data, leading to data leakage; In Adversarial Attacks, carefully crafted queries manipulate the model to reveal sensitive patterns or decision boundaries. Due to the sensitive healthcare data and critically of impacts of AI decisions in healthcare application, the healthcare AI application need to locally be generated in edge-computing environment, and expired an instance of as shown in Figure 5. Moreover, healthcare applications need to operate seamlessly without delay in emergent situations, while additionally connected by heavy IoT sensors' data. The transactions of IoT-generated data are relatively too large compared to cryptocurrency's transaction data, where the conventional blockchain has occupied, and thus, it cause heavy overheads in distributed network and huge memory amount to each node in the network.

Considering this edge AI system and its interaction with IoT-generated data, our platform framework in healthcare AIoT applications is design considers how to the blockchain fit into AIoT applications ensure the privacy and security issues as shown in Figure 4.

First, the blockchain system needs to manage local AI models' instances efficiently while ensuring traceability and their life cycle control. In order to avoid model extraction attack mentioned above, global AI models are deployed locally, and generate individual instances for a patient—referred to as AI adapters—are fine-tuned to adapt to specific individual and environmental contexts as given in Figure 5. As AI adapters evolve, multiple versions of AI models are generated, requiring systematic management by the Blockchain AI-Model Manager, depicted as the middle blockchain subsystem in Figure 4.

Second, the blockchain system needs to frequently handle locally updated data from IoT-generated data from patients. The Blockchain Data Manager, represented as the left blockchain subsystem in Figure 4, By ensuring efficient and secure data transactions, the Blockchain Data Manager fosters trust and provides high-quality, reliable data for AI applications, establishing itself as a foundational component for future AIoT ecosystems.

Third, healthcare AI assistant application needs to retrieve frequently a patient's medical records from multiple resources such as previous hospitals' blockchain decision archiver. and IoT-generated current data for fine-tuning. Blockchain Decision Archiver records the decision-making processes of AI agents programs and medical providers, ensuring transparency and accountability. Moreover, this system clarifies responsibility by enabling the identification of whether errors stemmed from human input, machine processing, or a combination of both. By mitigating reliability risks, this feature is especially valuable for real-world AI deployments, where understanding the origin of faults is essential for resolution and prevention.

Thus, these three blockchain systems can be integrated with edge AI system environments with IoT sensors for healthcare application to address the privacy and security challenges in AI systems, and data overhead issues in IoT sensors. The medical records is locally updated and operated in a medical institute such as hospital while the records can be retrieved from external requests in needs.

4.2 Theoretical analysis of the proposed framework: time and memory efficiency in edge AI system architecture

This section presents a mathematical analysis of memory usage and data retrieval efficiency in a blockchain-based healthcare AIoT system. The analysis compares conventional public blockchains with sharding blockchain architectures in an edge AI system environment, demonstrating the potential efficiency improvements of the proposed framework.

For this analysis, we define the following key parameters: hospitals H in $\mathbf{H} = \{h_1, h_2, \ldots, h_n, \ldots, h_N\}$, where N is the total number of hospitals in the network; patient P in $\mathbf{P} = \{p_1, p_2, \ldots, p_k, \ldots, p_K,\}$, where K represents the average number of patients in each hospital; and medical records R in $\mathbf{R_j} = \{r_1, r_2, \ldots, r_l, \ldots, r_L\}$ where L represent the average number of records per patient.

When a patient visits a hospital, the healthcare AI assistant accesses previous medical records stored in other hospitals through a secure blockchain network. The total number of records stored on the blockchain is given by $L_{\text{total}} = \sum_{h_n \in \mathbf{H}} \sum_{p_k \in \mathbf{P}} L_k$. The expected total number of medical records is.

$$\mathbf{E}[L] = N \cdot K \cdot \mathbf{E}[L_k] = N \cdot K \cdot L.$$

4.2.1 Memory requirements in blockchain architectures

4.2.1.1 Conventional blockchain memory usage

In a public blockchain, if there are D nodes participating in the distributed network, the memory required per node is $\Theta(N \cdot K \cdot L)$ Table 2. In a public blockchain, if there are D nodes participating in the distributed network, the memory required per node is $\Theta(D \cdot N \cdot K \cdot L)$.

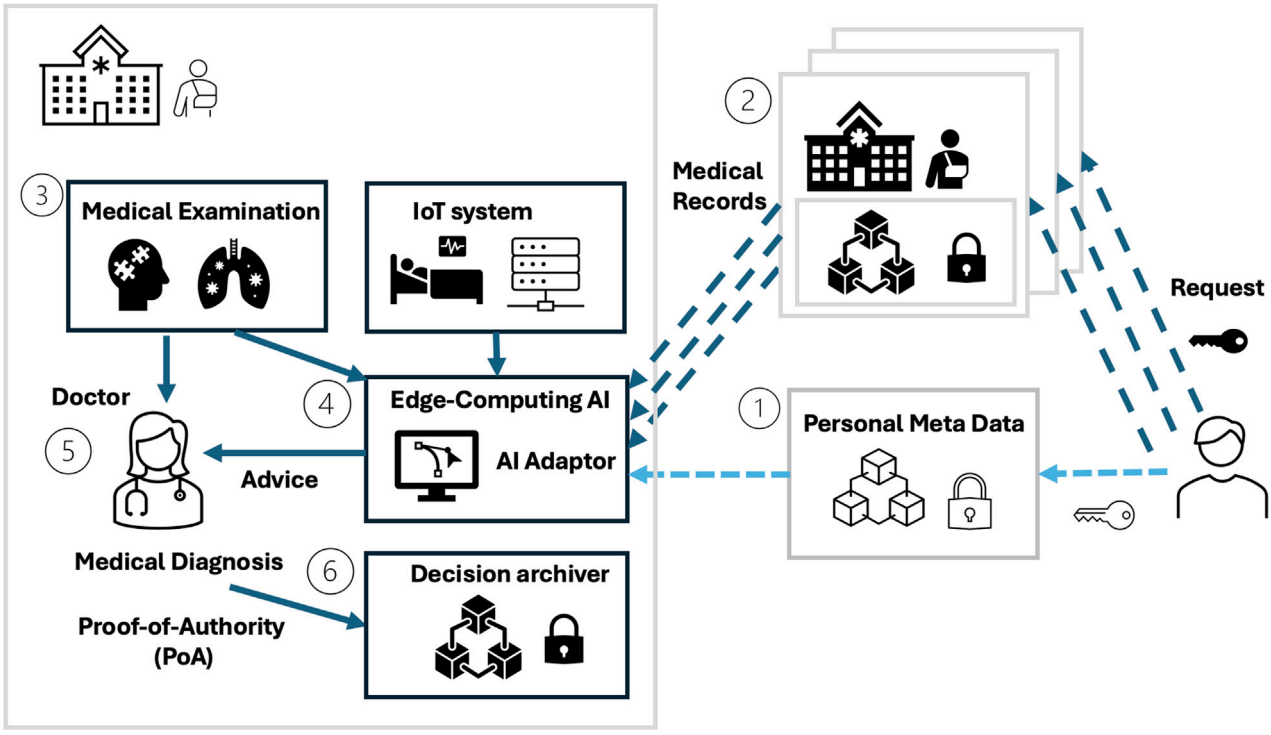

FIGURE 5
A representative scenario of a blockchain-enhanced healthcare AIoT system unfolds when a patient visits a hospital. The hospital can retrieve (1) personal information, (2) past medical records, and (3) medical examination and test results through blockchain technology. A healthcare AI assistant supports the medical doctor by generating (4) an AI adapter—a newly instantiated healthcare AI model tailored to the patient's case using the acquired data from (1), (2), and (3). Subsequently, (5) the medical doctor makes the final diagnosis based on all relevant data and insights and (6) authorizes the information to be recorded in the decision archiver.

TABLE 2 Theoretical analysis table.

	Memory	Data retrieval time
Conventional blockchain	$\Theta(D \cdot N \cdot K \cdot L)$	$\Theta(N \cdot K \cdot L)$
Sharding blockchain	$O(N \cdot K \cdot L)$	$O(K \cdot L)$

4.2.1.1.1 Observations on practical data range. First, given that $N \cdot K$ represents the total number of patients, this figure can be hundreds of millions in large-scale national healthcare systems (e.g., the U.S.). Second, to ensure security and resistance to cyberattacks such as the 51% attack, a blockchain network requires a minimum number of participating nodes. For example, Bitcoin's PoW requires at least 15,000 nodes, and Ethereum's PoS requires at least 6,000 nodes. Third, the number of hospitals in the U.S. is a few thousand, and L (number of medical records per patient) is continuously increasing due to the digitization of healthcare records.

Given these constraints, storing all patient records in a conventional blockchain introduces severe memory challenges. For instance, assuming each block is 512 kB and L = 1 (a highly conservative estimate, as real-world L is much larger). The total memory requirement in a conventional blockchain is estimated to be at least hundreds of petabytes (10^{15} bytes). In addition, since medical data is generated daily, the actual L value is much greater than 1, further exacerbating storage limitations. This demonstrates the practical infeasibility of using a conventional blockchain for a nationwide healthcare AIoT system due to the high cost and resource demands.

4.2.1.2 Sharding blockchain memory efficiency

In contrast, a sharding blockchain architecture significantly reduces memory requirements by storing only relevant medical records in specific shards rather than replicating all data across the entire network. The memory required per hospital is $\Theta(K \cdot L)$. The total memory required across the network is $\Theta(N \cdot K \cdot L)$.

4.2.1.2.1 Example calculation. For instance, Assuming the same block size (512 kB) and L = 1, the total memory usage across the sharded blockchain network is approximately hundreds of *terabytes* instead of hundreds of *petabytes* in a conventional blockchain.

Each hospital only needs less than a terabyte of memory storage, making blockchain integration practically feasible for healthcare AIoT applications.

This theoretical analysis provides a strong foundation for the simulation results and validates the efficiency improvements demonstrated by the proposed framework.

4.2.2 Data retrieval time from blockchain

An essential factor in evaluating the efficiency of a blockchain-integrated healthcare AIoT system is the data retrieval time, as it directly impacts AI-driven medical decision-making and real-time access to patient records. The primary bottleneck in data retrieval stems from the search complexity involved in locating stored medical records across the blockchain network. Medical records are frequently accessed by healthcare providers and AI systems while new records are continuously generated for each patient case.

4.2.2.1 Data retrieval time in a conventional blockchain

In a conventional blockchain, retrieving a medical record requires searching through all stored records across the distributed network. The retrieval time is given by $O(N \cdot K \cdot L)$. If the blockchain operates as a single-chain ledger, the retrieval time is $\Theta(N \cdot K \cdot L)$. For a Directed Acyclic Graph (DAG)-based blockchain, which optimizes data retrieval through a structured search mechanism (e.g., balanced binary tree indexing), the best-case retrieval time is $\Omega(logN + logK + logL)$ which significantly improves efficiency but still scales with network size.

4.2.2.2 Data retrieval time in a sharding blockchain

In contrast, a sharding blockchain significantly optimizes data retrieval by restricting the search space to only the relevant hospital shards rather than scanning the entire network. Since a patient already knows which hospital shard contains their medical records, the retrieval time is reduced to $O(K \cdot L)$. If each shard functions as a single-chain blockchain, the data retrieval time is $\Theta(K \cdot L)$, which is independent of the total number of hospitals (N) in the network, making it considerably more efficient than a conventional blockchain.

Thus, these findings confirm that a sharding blockchain architecture provides a practical and scalable solution for integrating blockchain with healthcare AIoT systems.

4.3 Strategies for blockchain management in healthcare AIoT applications

4.3.1 AI adaptor system for edge AI in healthcare and blockchain AI management

4.3.1.1 Blockchain AI-model manager: efficiently managing AI models and digital assets

As illustrated in Figure 6, the global AI model—hosted on cloud servers—oversees synchronization and resets of local AI models to ensure compliance throughout their lifecycle. Essential metadata, including AI model IDs, lifetimes, versions, licenses, expiration dates, policies, and regulatory information, is securely stored on the blockchain when AI models are transferred from cloud to local edge AI systems.

As AI adaptors evolve, multiple versions of AI models are generated, requiring systematic tracking to ensure traceability and integrity. The Blockchain AI-Model Manager leverages a Directed Acyclic Graph (DAG)-based blockchain (Figure 7) instead of a traditional single-chain blockchain (Figure 2), as DAG-based structures offer higher scalability, efficiency, and throughput. This architectural shift makes DAG-based blockchains ideal for managing the complex lifecycle of AI models, including versioning, ownership tracking, and adaptation to regulatory changes.

The Blockchain AI-Model Manager performs three core functions: version tracking, ownership and lifecycle control, and specialized AI agent management. First, The system tracks AI model versions, securely storing updates on the blockchain to ensure authenticity and traceability. Second, AI models ensure licensing and expiration date protection, and private data is not reused without explicit authorization. Third, the system coordinates multiple task-specific AI agents, ensuring seamless operation, maintenance, and interoperability for scalable healthcare AI applications.

Thus, the Blockchain AI-Model Manager thus ensures efficient AI model lifecycle management, strengthens trust in AI-driven healthcare, and provides a scalable solution for AIoT applications.

4.3.2 IoT system preprocessing and dimensionality reduction

4.3.2.1 Preprocessing IoT data for blockchain-integrated AI systems

Preprocessing IoT sensor data is critical for handling large volumes of real-time time-series data generated by healthcare monitoring devices. These data sources include 1D signals (e.g., heart rate, respiratory rate, EEG, ECG) and 2D data (e.g., medical imaging, motion sensor outputs).

As depicted in Figure 8, the preprocessing pipeline includes *Feature extraction*. Feature Extraction–Identifies meaningful data patterns using basic (e.g., mean, standard deviation) and advanced (e.g., PCA, ICA, n-grams) techniques, reducing dimensionality while retaining essential information.

4.3.2.2 Post-processing for AIoT system monitoring and feedback

Post-processing analyzes AI decision-making history, allowing refinements in preprocessing pipelines. If certain extracted features contribute less to decision accuracy, feature extraction methods can be adjusted accordingly. This iterative process improves model reliability through anomaly detection, AI decision transparency with blockchain-backed verification, and overall AIoT system security by mitigating emerging risks.

Thus, post-processing plays a key role in AI model enhancement, error analysis, and real-time blockchain-based decision tracking.

4.3.3 Blockchain decision archiver and shell fragment cubes (SFC) approach

4.3.3.1 Blockchain decision archiver: secure AI-collaborated medical records

The Blockchain Decision Archiver securely maintains patients information, medical examination and results, symptoms, and AI models and output advice, and medical providers' information and diagnosis. Then, medical providers authorized under Proof-of-Authority (PoA) verification store decisions in the blockchain.

While using Blockchain Decision Archiver to retrive medical records from previous hospitals, retrieving high-dimensional medical data remains a challenge. The complexity of healthcare records—spanning patient details, diagnoses, treatments, test

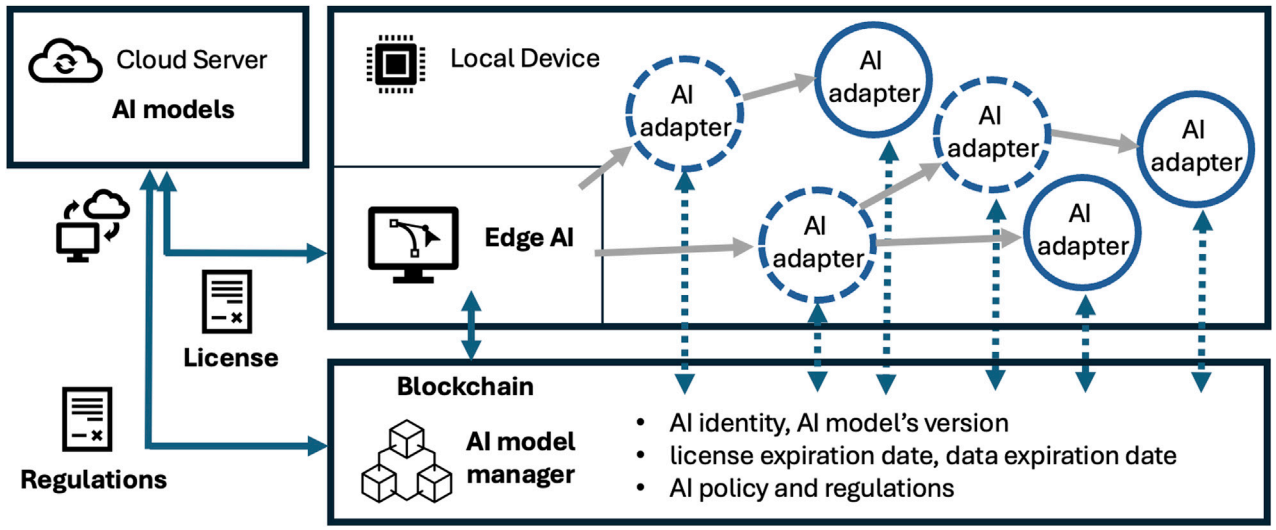

FIGURE 6
The Blockchain AI Model Manager oversees the management of AI models. A local AI model is initialized by downloading the latest AI model from the cloud to a local device, along with essential metadata—including AI versions, licenses, expiration dates, policies, and regulatory details. Once deployed, these AI models, referred to as AI adapters, are customized to individual contexts. As they adapt using personal medical data, multiple AI model versions are generated and systematically managed by the AI Model Manager, ensuring compliance throughout their lifecycle.

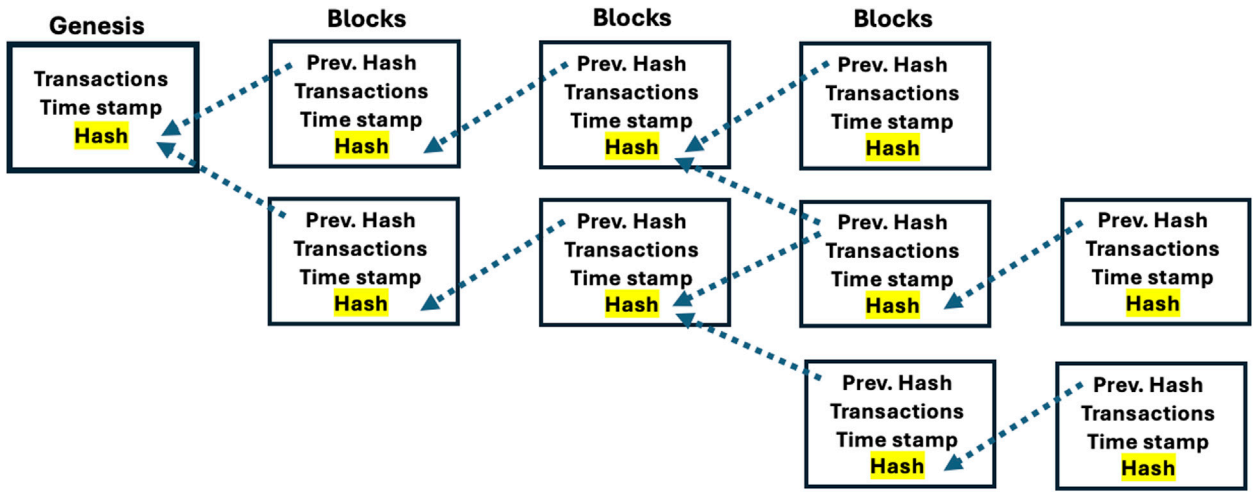

FIGURE 7
DAG-based blockchain architecture:A Directed Acyclic Graph (DAG)-based blockchain organizes data in a graph structure, where transactions are linked directly without forming a linear chain. Unlike single-chain blockchains, DAGs allow multiple transactions to be processed simultaneously, improving scalability and transaction throughput.

results, AI analysis, and medication history—leads to slow data retrieval times when querying medical archives.

4.3.3.2 Shell fragment cubes (SFC) approach for efficient data retrieval

To improve data retrieval time, this paper applies SFC approach —- a data partitioning technique used in high-dimensional databases like data warehouses. The SFC method balances query efficiency and storage optimization by selectively materializing fragmented data cubes.

As illustrated in Figure 9, the SFC-based system operates in two distinct phases. During the Index List Generation Phase (Factory Mode), the system scans blockchain decision archives to generate index lists for each medical data attribute, partitioning these lists into F fragments. It then constructs intersected lists for each attribute tuple set. In the Searching Phase (Field Mode), queries retrieve only the matched tuple set of attributes, utilizing its index list to search for the queried medical data, thereby minimizing the search space and reducing data retrieval time.

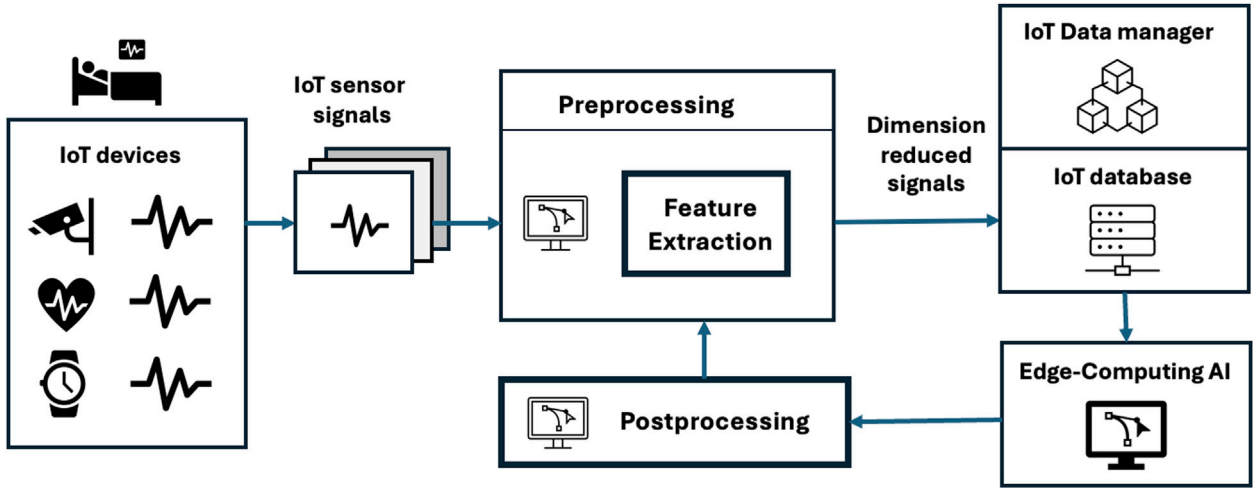

FIGURE 8
Preprocessing IoT sensor signals on IoT devices is essential for managing the high volume of real-time and time-series data generated by these sensors. Before storing the data, it undergoes preprocessing steps, including feature extraction. In the preprocessing, feature extraction is the process of transforming raw data into a set of informative and relevant features (attributes or variables) that can be used for machine learning or data analysis tasks. These processes reduce data complexity, enhance storage efficiency, and prepare the data for further analysis.

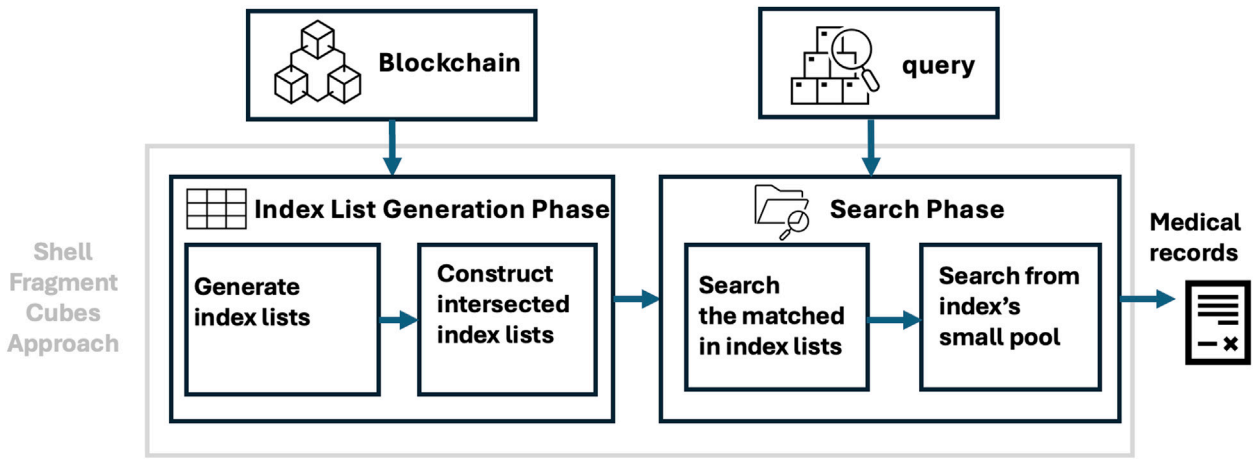

FIGURE 9
The SFC approach consists of the Index List Generation Phase and the Searching Phase.

By applying the SFC approach, the system reduces search complexity when retrieving records from multiple hospital shards, and thus enhances overall efficiency in blockchain-integrated healthcare AIoT systems by reducing retrieval times for AI-driven decision-making.

5 Simulation

To evaluate the efficiency of integrating sharding blockchain into healthcare AIoT systems, two simulations were conducted. The first simulation aimed to assess the impact of sharding blockchain on memory usage and data retrieval speed compared to a conventional blockchain. The second simulation further explored the effectiveness of the SFC approach in optimizing data retrieval times for healthcare records stored in a sharding blockchain framework.

5.1 Simulation settings

5.1.1 Hardware configuration

The simulations were conducted on Google Colab Pro, which offers enhanced computational resources compared to the standard free-tier version. The runtime environment dynamically allocated Intel or AMD CPU cores and NVIDIA GPUs for accelerated processing. The system specifications included 51.0 GB of RAM, 225.8 GB of disk storage, and a Linux-based Google Cloud Virtual Machine (VM) as the operating system.

5.1.2 Software setup

Google Colag Pro supports Jupyter Notebook, in which the software environment for the simulation was set up using Python 3.10+ along with the following essential libraries including NumPy and hashlib (SHA-256 hashing for blockchain).

5.1.3 Dataset for simulation

To replicate real-world healthcare data storage scenarios, a synthetic dataset of medical records was generated. Each record contained attributes such as hospital ID, patient ID, patient name, address, contact details, medical history, and more. After appending a timestamp and cryptographic hash, the final computed size of each record was approximately 512 kB.

5.1.4 Simulation 1: evaluating sharding blockchain for edge AI system in healthcare AIoT applications

As shown in Figure 5, the first simulation focused on testing how sharding blockchain improves data retrieval efficiency in a distributed healthcare network. The scenario involved an AI-powered medical assistant, called AI adaptor, and retrieves a patient's past medical records from different hospital shards. To compare performance, a conventional blockchain was used as the control group, where all participating hospitals shared and stored medical records across a distributed ledger.

The experiment simulated an increasing number of hospitals in the blockchain network, ranging from 10 to 10,000 nodes. Each hospital (node) maintained 100,000 medical records, with 1,000 records per block. Across 200 simulated samples, the memory consumption per hospital and the average data retrieval time were measured.

5.1.5 Simulation 2: impact of SFC approach on data retrieval efficiency

In the second simulation, the SFC approach was applied to further optimize data retrieval within the sharding-based blockchain for healthcare AIoT system. The goal was to evaluate whether this method could further reduce data retrieval time as the volume of patient records per hospital increased.

The experiment simulated variations in patient records, with the number of patients per hospital increasing from 10 to 5,000, and the number of medical records per patient ranging from 10 to 5,000. Each scenario was repeated 10 times, measuring the average data retrieval time both with and without the SFC approach. For this simulation, a default fragmentation factor of F = 2 was applied to analyze its impact on retrieval speed.

5.2 Simulation results

In Figures 10, 11, simulation results are illustrated in terms of memory overhead and data retrieval time, respectively, to provide insights into the efficiency of sharding blockchain compared to conventional blockchain for healthcare AIoT applications.

5.2.1 Simulation 1: memory consumption per hospital (node)

Our theoretical analysis (Section 4.2) predicts that memory consumption in a conventional blockchain scales with the number of participating nodes, whereas a sharding blockchain remains unaffected by network growth. Specifically, in a conventional blockchain, each hospital acts as a full node, storing an increasing amount of data as the number of hospitals in the network grows (expected complexity: $\Theta(D \cdot K \cdot L)$, where D is the number of hospitals, K is the number of blocks, and L is the number of records per block). In contrast, for a sharding blockchain, hospitals store only the relevant shard data (expected complexity: $\Theta(K \cdot L)$), significantly reducing memory overhead.

The simulation results in Figure 10 indicate that in a conventional blockchain, the memory required per hospital increases as the network expands (i.e., as more hospitals join the system). In contrast, the memory usage in a sharding blockchain remains stable regardless of network size.

These results align with our theoretical analysis, and confirm that sharding blockchain is more memory-efficient than conventional blockchain, making it a more scalable solution for healthcare AIoT applications.

5.2.2 Simulation 1: medical record retrieval time

The simulation results in Figure 11 also demonstrate that data retrieval time increases with network size in a conventional blockchain but remains constant in a sharding blockchain.

This is because, in a conventional blockchain, searching for a patient's medical records requires scanning all medical data distributed across the entire network. In contrast, a sharding blockchain limits the search scope to the specific hospital shards where a patient's records were previously stored, significantly reducing search time.

These findings validate that sharding blockchain enhances time efficiency, making it a practical and scalable solution for real-time medical data retrieval in AIoT healthcare systems.

5.2.3 Simulation 2: impact of SFC approach on data retrieval time

The simulation results, presented in Figure 12, show that as the total number of records increases, data retrieval time also increases. However, a key finding is that applying the SFC approach nearly halves the data retrieval time compared to the standard sharding blockchain across all test cases.

Both scenarios (with and without SFC) demonstrate increasing retrieval time as K (number of blocks) and L (records per block) grow. However, due to the high-dimensional nature of medical records, the SFC approach improves search efficiency by segmenting and structuring the stored data more effectively.

These results confirm that SFC enhances retrieval performance, making it a valuable optimization technique for managing large-scale healthcare records within a sharding blockchain framework.

6 Discussion

The results from the simulations provide valuable insights into the impact of integrating a sharding-based blockchain and the SFC approach into a healthcare AIoT system. The findings indicate that these enhancements significantly improve memory overhead and data retrieval times compared to conventional blockchain implementations.

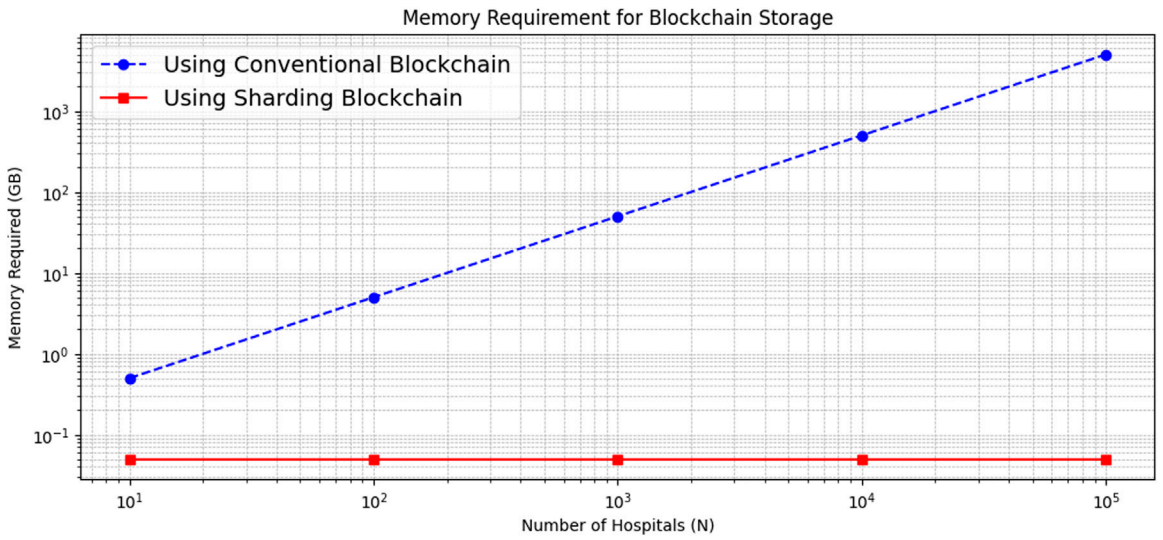

FIGURE 10
Memory required for each hospital (node) in a traditional blockchain (blue) and a shared blockchain (red).

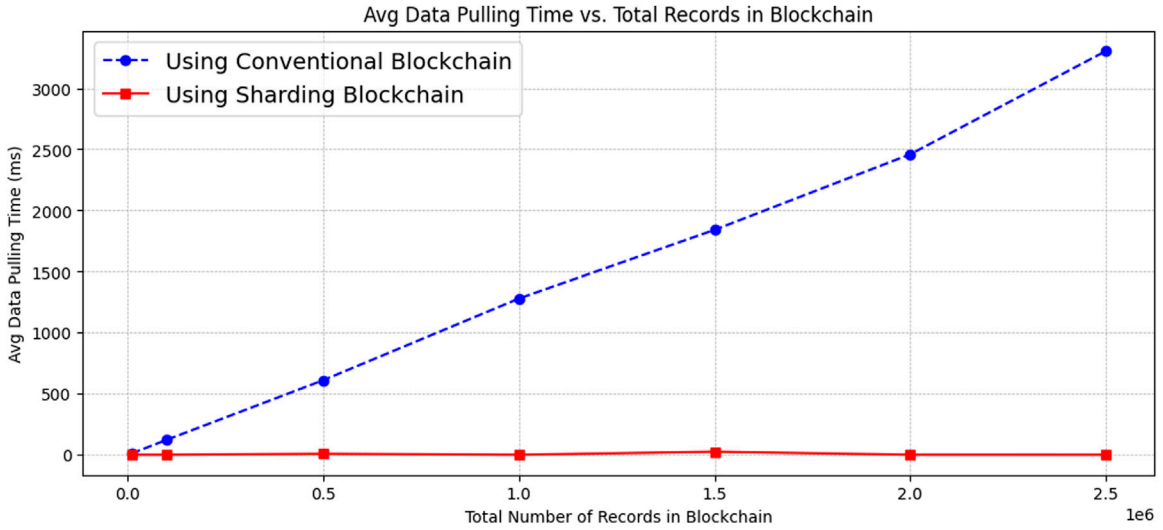

FIGURE 11
Medical record retrieval time in a traditional blockchain (blue) and a shared blockchain (red).

In the first simulation, Sharding blockchain significantly reduces memory overhead and improves data retrieval speed compared to conventional blockchain, making it a more scalable and efficient solution for healthcare AIoT. The decentralized nature of traditional blockchains often results in significant storage overhead, particularly in data-intensive domains such as healthcare AIoT systems. By partitioning the blockchain into smaller, manageable shards, the system effectively distributes storage and processing loads, leading to a reduction in overall memory consumption. Moreover, the simulation results confirmed that sharding enables parallel processing of transactions, thereby expediting data retrieval times as it limits the search scope to relevant hospital shards instead of scanning the entire network. This efficiency is particularly crucial for healthcare applications where timely access to patient records is vital for decision-making.

In the second simulation, the SFC approach further improves retrieval performance, reducing data retrieval time by approximately 50%, making it highly effective for managing large-scale medical records. This technique further refines data retrieval by organizing healthcare records of a high-dimensional data into structured fragments, allowing for more efficient querying and reduced access latency. The results demonstrated that, when compared to a sharded blockchain alone, the SFC approach significantly

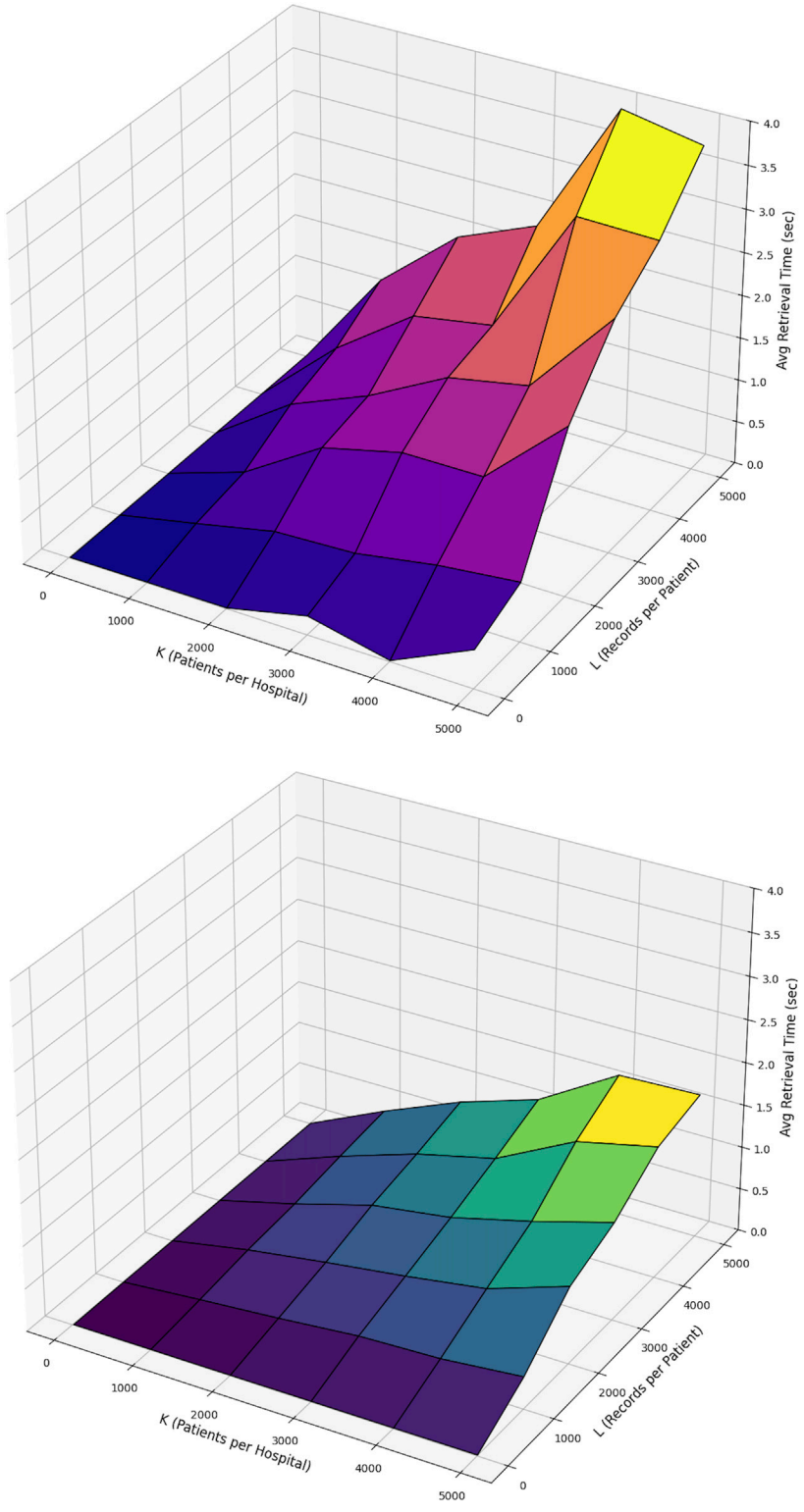

FIGURE 12
The average data retrieval time for a single blockchain using Brute Force approach (Upper) and the SFC aproach (Lower), both plotted on the same scale.

decreases data retrieval times. This enhancement is particularly advantageous for AIoT healthcare systems that require real-time data access, such as remote patient monitoring and predictive analytics applications.

Overall, the simulations provide strong empirical evidence highlight the practical benefits of integrating sharding blockchain and SFC into healthcare AIoT systems, paving the way for more efficient, secure, and scalable medical data management solutions.

7 Conclusion

This paper investigate the integration of blockchain with Artificial-Intelligence-of-Things (AIoT), in a particular focus on healthcare applications. There has been limited attention given to the practical challenges of integrating blockchain with AIoT in healthcare systems, where sensitive personal data, high memory consumption, and time-consuming data retrieval pose significant obstacles. To address these challenges, this paper proposes a platform framework that combines edge AI with a sharding-based proof-of-authority (PoA) blockchain. The framework incorporates three key strategies to enhance the efficiency of blockchain applications in healthcare: Blockchain Version Manager for AI Adaptors–Ensures AI adaptors are securely updated and resistant to data leakage; IoT Preprocessing for Blockchain Data Management–Reduces redundancy and optimizes data storage before recording it on the blockchain; Shall Fragment Cube (SFC) Approach for Blockchain Decision Archiving–Improves data retrieval efficiency by structuring stored medical records more effectively. Theoretical analysis confirms that sharding blockchain significantly improves memory efficiency and reduces data retrieval time. Simulation results further validate these benefits, showing that the SFC approach reduces data retrieval time by approximately 50 Thus, this study has the transformative potential to develop secure, efficient, and scalable smart systems of integrating AIoT and blockchain. This study underscores the critical role of blockchain technology in enabling next-generation AIoT systems, paving the way for more secure, scalable, and high-performance intelligent solutions.

This study does not cover the security aspects of IoT devices within AIoT systems. While blockchain security and AI vulnerabilities are discussed, IoT devices introduce additional risks that require further investigation. Specifically, IoT sensors collecting personal health data are susceptible to unauthorized access and malicious tampering, posing significant threats to patient privacy and data integrity. Therefore, future research should focus on developing a comprehensive security framework to safeguard IoT device data and AI model integrity while integrating blockchain into healthcare AIoT systems.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

MJ: Writing – original draft, Writing – review and editing.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. The author(s) would like to express their gratitude to the department of Electrical and Computer Engineering at the Catholic University of America for their sponsorship and support.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that Gen AI was used in the creation of this manuscript. The author(s) designed the Blockchain platform framework by herself, while the Python codes for its system implementation are performed with Generated AI, GPT-4o.

Publisher's note

References

Alrebdi, N., Alabdulatif, A., Iwendi, C., and Lian, Z. (2022). Svbe: searchable and verifiable blockchain-based electronic medical records system. *Sci. Rep.* 12, 266. doi:10.1038/s41598-021-04124-8

Baranwal Somy, N., Kannan, K., Arya, V., Hans, S., Singh, A., Lohia, P., et al. (2019). "Ownership preserving ai market places using blockchain," in *2019 IEEE international conference on blockchain (blockchain)*, 156–165. doi:10.1109/Blockchain.2019.00029

Bodkhe, U., Mehta, D., Tanwar, S., Bhattacharya, P., Singh, P. K., and Hong, W.-C. (2020). A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access* 8, 54371–54401. doi:10.1109/ACCESS.2020.2981415

Chaganti, R., Bhushan, B., and Ravi, V. (2022). A survey on blockchain solutions in ddos attacks mitigation: techniques, open challenges and future directions. *Comput. Commun.* 197, 96–112. doi:10.1016/j.comcom.2022.10.026

Chavali, B., Khatri, S. K., and Hossain, S. A. (2020). "Ai and blockchain integration," in *2020 8th international conference on reliability, infocom technologies and optimization (trends and future directions) (ICRITO)*, 548–552. doi:10.1109/ICRITO48877.2020.9197847

Chen, J., Duan, K., Zhang, R., Zeng, L., and Wang, W. (2018). An ai based super nodes selection algorithm in blockchain networks

Deng, X., Li, K., Wang, Z., Li, J., and Luo, Z. (2022). "A survey of blockchain consensus algorithms," in *2022 international conference on blockchain technology and information security (ICBCTIS)*, 188–192. doi:10.1109/ICBCTIS55569.2022.00050

Dinh, T. N., and Thai, M. T. (2018). Ai and blockchain: a disruptive integration. *Computer* 51, 48–53. doi:10.1109/MC.2018.3620971

Douligeris, C., and Mitrokotsa, A. (2004). Ddos attacks and defense mechanisms: classification and state-of-the-art. *Comput. Netw.* 44, 643–666. doi:10.1016/j.comnet.2003.10.003

Era, C. A. A., Rahman, M., and Alvi, S. T. (2024). "Artificial intelligence of things (aiot) technologies, benefits and applications," in *2024 4th international conference on*

emerging smart technologies and applications (eSmarTA), 1–6. doi:10.1109/eSmarTA62850.2024.10638992

Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., and Colman, A. (2020). Blockchain consensuses algorithms: a survey. *Corr. abs/2001*, 07091. doi:10.48550/arXiv.2001.07091

Gai, K., Wu, Y., Zhu, L., Xu, L., and Zhang, Y. (2019). Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. *IEEE Internet Things J.* 6, 7992–8004. doi:10.1109/JIOT.2019.2904303

Haleem, A., Javaid, M., Singh, R. P., Suman, R., and Rab, S. (2021). Blockchain technology applications in healthcare: an overview. *Int. J. Intelligent Netw.* 2, 130–139. doi:10.1016/j.ijin.2021.09.005

Hammad, M., Iqbal, J., Hassan, C., Hussain, S., Ullah, S. S., Uddin, M., et al. (2023). Blockchain-based decentralized architecture for software version control. *Appl. Sci.* 13, 3066. doi:10.3390/app13053066

Harris, J. D., and Waggoner, B. (2019). "Decentralized and collaborative ai on blockchain," in *2019 IEEE international conference on blockchain (blockchain)*, 368–375. doi:10.1109/Blockchain.2019.00057

J, A., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., and Eunice, J. (2023). Blockchain for healthcare systems: architecture, security challenges, trends and future directions. *J. Netw. Comput. Appl.* 215, 103633. doi:10.1016/j.jnca.2023.103633

Kawamoto, Y., and Kobayashi, A (2020). "Ai pedigree verification platform using blockchain," in *2020 2nd conference on blockchain research applications for innovative networks and services (BRAINS)*, 204–205. doi:10.1109/BRAINS49436.2020.9223307

Kilroy, K., Riley, L., and Bhatta, D. (2023). *Blockchain tethered AI*. Sebastopol, California O'Reilly Media.

Kuznetsov, O., Sernani, P., Romeo, L., Frontoni, E., and Mancini, A. (2024). On the integration of artificial intelligence and blockchain technology: a perspective about security. *IEEE Access* 12, 3881–3897. doi:10.1109/ACCESS.2023.3349019

Li, X., Jiang, P., Chen, T., Luo, X., and Wen, Q. (2020). A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* 107, 841–853. doi:10.1016/j.future.2017.08.020

Mollah, M. B., Zhao, J., Niyato, D., Lam, K.-Y., Zhang, X., Ghias, A. M. Y. M., et al. (2021). Blockchain for future smart grid: a comprehensive survey. *IEEE Internet Things J.* 8, 18–43. doi:10.1109/JIOT.2020.2993601

Pal, S., Jadidi, Z., Alaeifar, P., and Foo, E. (2023). The role of artificial intelligence and blockchain for future cyber threat intelligence. 1–6. doi:10.1109/ICST59744.2023.10460772

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., et al. (2020). Exploring the attack surface of blockchain: a comprehensive survey. *IEEE Commun. Surv. Tutorials* 22, 1977–2008. doi:10.1109/COMST.2020.2975999

Salama, R., and Al-Turjman, F. (2022). "Ai in blockchain towards realizing cyber security," in *2022 international conference on artificial intelligence in everything (AIE)*, 471–475. doi:10.1109/AIE57029.2022.00096

Salama, R., Al-Turjman, S., Altrjman, C., Al-Turjman, F., Gupta, R., Yadav, S., et al. (2023). Blockchain technology and artificial intelligence's future applications in cyber security. 412–418. doi:10.1109/AECE59614.2023.10428598

Sengupta, J., Ruj, S., and Das Bit, S. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. *J. Netw. Comput. Appl.* 149, 102481. doi:10.1016/j.jnca.2019.102481

Sherin, K., Kaur, N., Joshi, A., B, R., Nayak, P., and Srinivas, K. (2023). "The role of ai and blockchain in supply chain traceability," in *2023 3rd international conference on advance computing and innovative technologies in engineering (ICACITE)*, 918–922. doi:10.1109/ICACITE57410.2023.10183214

Shmatko, O., and Kliuchka, Y. (2022). A novel architecture of a secure medical system using dag. *Sci. Collect. InterConf+*, 202–211doi. doi:10.51582/interconf.19-20.09.2022.019

Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., and Ra, I.-H. (2020). Convergence of blockchain and artificial intelligence in iot network for the sustainable smart city. *Sustain. Cities Soc.* 63, 102364. doi:10.1016/j.scs.2020.102364

Uddin, M. A., Stranieri, A., Gondal, I., and Balasubramanian, V. (2021). A survey on the adoption of blockchain in iot: challenges and solutions. *Blockchain Res. Appl.* 2, 100006. doi:10.1016/j.bcra.2021.100006

Wang, J., Wang, Q., Zhou, N., and Chi, Y. (2017). A novel electricity transaction mode of microgrids based on blockchain and continuous double auction. *Energies* 10, 1971. doi:10.3390/en10121971

Wu, H. Y., Yang, X., Yue, C., Paik, H.-Y., and Kanhere, S. S. (2022). Chain or dag? underlying data structures, architectures, topologies and consensus in distributed ledger technology: a review, taxonomy and research issues. *J. Syst. Archit.* 131, 102720. doi:10.1016/j.sysarc.2022.102720

Zoican, S., Vochin, M., Zoican, R., and Galatchi, D. (2018). "Blockchain and consensus algorithms in internet of things," in *2018 international symposium on electronics and telecommunications (ISETC)*, 1–4. doi:10.1109/ISETC.2018.8583923