scientific reports

OPEN

Leveraging blockchain and IoMT for secure and interoperable electronic health records

Soufiane Ben Othman[1]✉ & Masresha Getahun[2]✉

The Internet of Medical Things (IoMT) is transforming healthcare by seamlessly connecting medical devices, wearables, and sensors to enable personalized, real-time health monitoring and treatment for consumers. As IoMT continues to advance, ensuring the security and privacy of transmitted data has become a critical concern. Blockchain technology has emerged as a promising solution to enhance privacy and security, particularly in sensitive areas such as medical data within the Internet of Things. By integrating blockchain with IoT, secure transmission of medical data can be achieved, paving the way for improved healthcare services, enhanced consumer privacy, and accelerated medical advancements. In this paper, we propose EHRGuard: Enhancing Privacy and Security of Electronic Health Records through Blockchain Technology. EHRGuard is a novel system that leverages blockchain technology to address key challenges in the management of Electronic Health Records (EHRs), with a focus on improving privacy, security, and interoperability in healthcare data systems for consumers. The framework utilizes the Internet of Medical Things (IoMT) to collect real-time health data from consumers through sensors and integrates blockchain technology to ensure data anonymity, security, and integrity. By combining IoMT and blockchain, EHRGuard enables the seamless and secure gathering of real-time health data, ensuring that sensitive information is protected from unauthorized access and tampering. Experimental results demonstrate that the proposed system outperforms traditional healthcare systems in terms of service quality and consumer data monitoring. This innovative approach not only enhances the security and privacy of EHRs but also fosters trust and efficiency in healthcare systems, ultimately benefiting consumers and advancing medical research and treatment.

Keywords Internet of medical things, Electronic health records, Blockchain

The Internet of Medical Things (IoMT) represents a dynamic and expanding ecosystem of internet-connected medical devices, applications, and systems seamlessly integrated with healthcare IT infrastructure[1]. This transformative technology is revolutionizing healthcare by facilitating real-time data collection, transmission, and analysis, ultimately enhancing patient care and streamlining operational efficiency. IoMT spans a diverse array of tools, ranging from wearable devices like fitness trackers and smartwatches to sophisticated implants such as pacemakers and insulin pumps. These devices capture vital health metrics—heart rate, blood glucose levels, and activity patterns—and relay them to healthcare providers for ongoing monitoring and evaluation. A key strength of IoMT lies in its capacity to enable remote patient monitoring (RPM)[2]. For individuals managing chronic conditions like diabetes or heart disease, this technology offers continuous oversight without the need for frequent clinic visits. This not only improves patient convenience but also empowers providers to spot emerging issues early and respond swiftly. Moreover, IoMT paves the way for personalized medicine, allowing clinicians to craft tailored treatment plans based on real-time insights into a patient's unique health profile. Beyond hardware, IoMT encompasses software platforms that harness advanced analytics and artificial intelligence (AI) to process the flood of data from connected devices[3]. These tools can detect patterns, forecast health risks, and suggest preventive actions. For instance, an IoMT system might flag a patient's rising blood pressure trends, alerting a physician to a potential hypertension risk and enabling timely intervention. This data-driven methodology sharpens clinical decision-making and fosters more effective, proactive care strategies. However, IoMT's promise comes with notable hurdles. Data security and privacy remain pressing concerns, as transmitting sensitive health information online heightens vulnerability to cyberattacks[4]. Compliance with regulations like HIPAA is critical to

[1]Applied College, King Faisal University, Al-Ahsa 31982, Saudi Arabia. [2]Department of Computer Science and Information Technology, College of Engineering and Technology, Kebri Dehar University, Kebri Dehar, Ethiopia. ✉email: sbenothman@kfu.edu.sa; masreshaggetahun@gmail.com

safeguarding patient confidentiality. Interoperability poses another obstacle, requiring seamless communication between devices and systems from various manufacturers. Additionally, the sheer volume of data generated can strain healthcare systems, underscoring the need for robust data management and analytical solutions[5]. Looking forward, the IoMT landscape is poised for substantial growth, fueled by advancements in AI, machine learning, and 5G connectivity[6]. These innovations promise to amplify IoMT's precision and responsiveness, driving a shift toward more proactive and efficient healthcare delivery. As adoption spreads globally, IoMT holds the potential to redefine patient care, lower costs, and elevate health outcomes on an unprecedented scale[7].

The use of blockchain technology on the Internet of Things (IoT) for healthcare provides a secure and privacy-focused approach to managing medical data. Blockchain has emerged as a reliable solution to challenges related to data security, interoperability, and transparency in healthcare[8]. As a decentralized and distributed ledger, blockchain ensures that health records remain tamper-proof, meaning once data is recorded, it cannot be modified or erased. This feature is essential for maintaining the accuracy and trustworthiness of patient information. Furthermore, decentralization removes the need for a central authority, strengthening security and system reliability. Various blockchain-based solutions, such as HealthChain[9], Fortified-Chain[10], and MedShare[11], have been designed to securely manage and exchange medical information. These systems utilize blockchain's core capabilities to improve data privacy, security, and accessibility[12]. For example, smart contract-based access control mechanisms have been proposed to ensure secure sharing of health data among patients and healthcare providers, emphasizing the importance of decentralized trust[13]. Additionally, hybrid cryptographic schemes, such as the Improved Key Generation Scheme of RSA (IKGSR), have been implemented to securely retrieve EHRs in cloud-based healthcare systems, offering robust encryption and decryption methods[14]. Furthermore, intelligent breach detection systems integrated with advanced networks like 6G have shown promise in safeguarding critical healthcare infrastructures from cyber-attacks[15]. Machine learning techniques have also played a crucial role in enhancing cybersecurity by enabling the detection of digital threats, ensuring timely responses to potential security breaches[16]. By employing cryptographic techniques, blockchain protects sensitive health records, allowing patients to have greater control over their data. Individuals can decide who has access to their medical information, ensuring confidentiality while enabling seamless communication with healthcare providers. Another advantage of blockchain is its ability to enhance transparency and accountability in healthcare[17]. Every transaction recorded on the blockchain is auditable, enabling participants to track the history of data exchanges. Smart contracts, which are self-executing agreements with predefined rules, further improve interoperability by automating data-sharing processes between healthcare entities. Despite these benefits, challenges such as scalability and regulatory compliance must be addressed to support broader adoption. As research continues, blockchain's potential to enhance healthcare data security and management becomes increasingly evident[18].

This study presents a privacy-centric healthcare framework that employs a layered architecture to effectively manage and monitor patient health information. The system embraces decentralization by merging blockchain technology with the Internet of Things (IoT), enabling real-time patient oversight, secure handling of Electronic Health Records (EHRs), prescription management, and safeguarded data sharing. Blockchain integration ensures data integrity, robust security, and transparency, preventing unauthorized alterations and fostering trust across healthcare operations. Meanwhile, IoT devices facilitate continuous health monitoring, paving the way for prompt, evidence-based medical decisions. A standout feature of this system is its use of the Internet of Medical Things (IoMT) to collect real-time data from sensors, promoting a proactive stance on patient care. Blockchain enhances privacy through encryption and anonymity, tackling concerns surrounding data confidentiality. Furthermore, the research underscores the value of linking healthcare providers, institutions, and stakeholders via a decentralized blockchain network. This setup enhances access control, streamlines secure data exchange, and ensures compliance, all while prioritizing patient privacy and operational efficiency.

The primary contributions of this study can be summarized as follows:

- The article offers an in-depth exploration of blockchain technology and the Internet of Things (IoT) within the healthcare landscape. Its primary aim is to equip readers with a clear grasp of both technologies, highlighting their core features and examining the powerful synergies that emerge from their integration. By doing so, it seeks to demonstrate how combining blockchain and IoT can revolutionize and strengthen the healthcare system.
- The research proposes a novel, lightweight decentralized framework tailored for real-time monitoring and prescription management in healthcare. Leveraging the Internet of Medical Things (IoMT) to gather patient sensor data, this system incorporates blockchain technology to ensure patient data anonymity and security. By linking healthcare facilities, patients, and professionals through a blockchain network, the framework enhances access control and fosters data interoperability across the healthcare sector.
- Furthermore, the study substantiates its proposed system through practical demonstrations, assessing its effectiveness against key performance metrics. These real-world tests validate the theoretical foundation of the decentralized framework, providing tangible evidence of its implications for real-time monitoring and prescription management. This empirical approach bolsters the research's credibility, offering actionable insights into the system's performance and its potential to benefit healthcare stakeholders.

The remainder of this paper is structured as follows: Sect "Related work" reviews related work, providing an overview of existing research in the field. Sect "System model and design goal" discusses the system model and design goals, outlining the foundational principles of our approach. Sect "Proposed EHRGuard description" introduces the proposed EHRGuard system, describing its architecture and core functionalities. Sect "Security analysis and evaluation of the EHRGuard system" presents a security analysis and evaluation, assessing the robustness of our system against potential threats. Sect "Performance analyses" focuses on performance analysis, measuring the efficiency and effectiveness of EHRGuard. Sect "Comparative analysis" provides a comparative analysis, highlighting the advantages of our approach to existing solutions. Sect "Use cases and real-time applications of the EHRGuard system" explores real-world use cases and applications of EHRGuard in healthcare settings. Sect "Scalability analysis for EHRGuard in large-scale medical environments" examines the scalability of EHRGuard in large-scale medical environments, assessing its adaptability for widespread deployment. Finally, Sect "Conclusion" concludes the paper and outlines potential future research directions.

Related work

This section reviews studies in the healthcare sector that have strategically integrated blockchain and the Internet of Things (IoT) to enhance the security of Electronic Health Records (EHRs).

The authors in[19] propose a system aimed at enhancing healthcare by ensuring secure data management via a lightweight blockchain. This paper introduces an innovative platform for monitoring patient vital signs through the implementation of smart contracts on a blockchain. The system is constructed using Hyperledger Fabric, a distributed ledger framework tailored for enterprise-level blockchain applications. By utilizing the Libelium e-Health toolkit for physiological data acquisition, the proposed solution offers patients several benefits, including an unalterable historical log and universal access to medical information at any location and time. Performance evaluation is conducted using Hyperledger Caliper, a standard benchmark tool, measuring transaction per second, transaction latency, and resource utilization. The findings reveal that the proposed system surpasses conventional healthcare systems in the monitoring of patient data.

The DITrust Chain system, proposed in[20], is a blockchain-based framework designed to enhance security and privacy in Internet of Medical Things (IoMT) environments. It features a multi-layered architecture: the first layer collects and processes data through sensors and actuators; the second layer uses gateways and network technologies like Bluetooth, WiFi, and ZigBee to securely transmit data; the third, or middleware layer, includes blockchain decision units, data analytics, and application support to manage data integrity and services; and the final application layer delivers system functionalities to end-users via web service protocols and service composition technologies. This structure ensures seamless integration, robust data protection, and improved patient confidentiality, with experimental results showing it outperforms traditional access control methods in IoMT settings.

In[21], the authors introduce a novel privacy-preserving scheme called BIoTHR, which leverages blockchain and swarm exchange techniques to enable secure and seamless transmission of user data, such as electronic health records (EHRs), across peer-to-peer networks. This framework integrates blockchain technology with IoT to create a robust system for EHR management, ensuring real-time monitoring and secure data transmission through autonomous encryption–decryption mechanisms and dynamic server assistance. Key algorithms like swarm-listen, announcement, peer open, and peer closing are employed to optimize system functionality, while open-source tools such as GnuPG, IPFS, and Golang are used for development. The scheme is tested using simulated IoT-based health sensor nodes, including body temperature, pulse rate, oxygen saturation (SPO2), galvanic skin response, and blood glucose, within the blockchain-assisted swarm exchange framework. Evaluation results demonstrate that the proposed scheme outperforms existing methods in blockchain-IoT integration, swarm exchange, and EHR transmission, offering enhanced security and efficiency for e-healthcare services.

Samuel et al. in[22] propose the Patient-Centric Healthcare Framework (PCH), a novel reference architecture designed to enhance semantic interoperability in healthcare systems by integrating Blockchain, Cloud, and IoT technologies. The framework features a five-tiered architecture that emphasizes collaboration and secure data processing, with a focus on practical implementation. The design process includes a layering diagram, system context, and detailed reference architecture to outline component topology and interactions. Using electronic medical records as an example, the framework demonstrates how healthcare data is processed while maintaining robust security measures. The authors evaluate PCH against existing Blockchain-based healthcare frameworks, with results showing that PCH offers superior solutions for securing healthcare data, enabling efficient data sharing, and improving overall interoperability, making it a promising approach for modern healthcare systems.

Pratima et al. in[23] propose EHDHE, a decentralized blockchain-based IoT application designed to enhance the security of healthcare documents in digital healthcare ecosystems. The application acts as a communication intermediary, connecting hospitals, patients, and doctors, and features the generation of unique identification numbers for medical certificates and the use of the Proof of Work (PoW) consensus algorithm to create new blocks in the blockchain network. Its primary goal is to ensure the security and privacy of medical certificates by preventing unauthorized access and storing medical data as hashed blocks within the blockchain, thereby mitigating fraudulent activities. The authors evaluate the application through extensive experimental tests, analyzing parameters such as latency, computation time, processing time, throughput, and network usage to assess its performance and robustness. The results demonstrate that EHDHE is a secure and efficient solution for managing healthcare documents in IoT-enabled ecosystems.

Bora et al. in[24] propose PPFchain, a novel privacy-preserving blockchain-based federated learning (FL) framework designed for sensor networks. PPFchain leverages a distributed architecture to ensure data privacy, reliability, and low-cost on-demand anonymity within an IoT-based blockchain network. Key features include the integration of fog node architecture at the edge of the off-chain IoT network, which reduces contract payload and minimizes end-to-end delay, and the use of digital signatures with public key cryptography to protect administrator privacy. FL is employed to enhance data privacy while maintaining system performance. The framework is evaluated using benchmark metrics for event and storage-based smart contracts within a distributed architecture. Additionally, the authors introduce a 5G-enabled block-sensor platform that balances security-privacy concerns with computation-communication costs, paving the way for next-generation blockchain-sensor applications in 5G-enabled environments. This innovative approach addresses critical challenges in security, privacy, and efficiency, demonstrating its potential for advanced IoT and blockchain integration.

In reference[25], the authors propose an innovative blockchain-based architecture designed to decentralize Electronic Health Records (EHR) and enable smart contract-driven service automation while ensuring robust security and privacy. The architecture employs a hybrid computing model, integrating blockchain-based distributed data storage to overcome limitations of cloud-centric Internet of Medical Things (IoMT) healthcare systems, such as high latency, elevated storage costs, and single points of failure. A standout feature is the decentralized selective ring-based access control mechanism, which, along with device authentication and patient record anonymity algorithms, significantly enhances system security. The authors evaluate the system's latency and cost-effectiveness in data sharing, demonstrating its efficiency. Logical system analysis confirms that the architecture meets the security and privacy requirements of decentralized IoMT smart healthcare systems. Experimental results reveal that the fortified-chain-based Healthcare Privacy System (HCPS) requires minimal storage and achieves millisecond-level response times, outperforming traditional centralized HCPS. These findings highlight the architecture's decentralized automated access control, security, and privacy capabilities, affirming its suitability for decentralized IoMT smart healthcare systems.

In reference[26], the authors present BEdgeHealth, a novel decentralized health architecture that combines Mobile Edge Computing (MEC) and blockchain technologies to enable efficient data offloading and secure data sharing within distributed hospital networks. The architecture offers two key advantages: (1) a smart contract system that provides authentication and traceability for data-sharing activities, eliminating the need for external authority. The smart contract tracks events like data uploads and user access and any modifications to data records alter their hash values, which are also traceable. (2) The integration of smart contracts with the InterPlanetary File System (IPFS) enhances the data retrieval rate, ensuring efficient and secure data access. The system includes a privacy-aware data-offloading scheme, where mobile devices can offload health data to nearby MEC servers for efficient computation, and a secure data-sharing scheme that leverages blockchain and IPFS for secure exchanges among healthcare users. By combining smart contract-based authentication with MEC, the architecture enables decentralized user access verification at the network edge without relying on a central authority. Real-world experiments demonstrate that BEdgeHealth significantly improves Quality of Service (QoS) while ensuring data privacy and security, outperforming existing schemes in terms of efficiency and reliability.

System model and design goal

In this section, we introduce EHRGuard, an innovative framework designed for Remote Patient Monitoring with a focus on ensuring the security of patient health data through the integration of blockchain and IoT. Within this section, we provide a comprehensive demonstration of the proposed architecture, showcasing its various facets. Subsequently, we outline diverse prerequisites for establishing a secure authentication scheme in healthcare applications that leverage IoT technology.

System architecture

The proposed system is structured with a modular architecture, wherein each layer operates independently of the others. This decoupling feature provides developers with the flexibility to integrate or remove modules without causing disruptions to the overall system. The architecture of the proposed system is shown in Fig. 1 and refers to five major components: Patient with wearable IoT devices, healthcare professionals, permissioned blockchain, an off-chain database and Electronic Health Record.

- Patient with wearable IoT devices: The proposed system integrates heterogeneous IoT-based medical sensors—categorized into ingestible/implantable sensors, environmental sensors, and camera-based sensors—to enable continuous health monitoring by measuring physiological parameters and transmitting data wirelessly to a server. Each patient's IoT devices and sensors are registered on a blockchain to ensure data integrity and prevent tampering, with a health administrator overseeing initial registration using details like name, date of birth, and contact information. Patients access the system via email ID and a generated password, while four key sensors (EMG, SpO2, body temperature, and pulse rate) monitor health metrics, with predefined normal and abnormal ranges triggering automated notifications for potential health issues. This real-time monitoring, combined with blockchain security and automated alerts, ensures timely interventions, enhances patient care, and supports early detection of health complications. Table 1 defines normal and abnormal ranges for these parameters, with automated notifications triggered when any sensor detects values outside the normal range, indicating a potential health issue.
- Healthcare professionals: Access to patient health data is restricted to authorized healthcare professionals, such as doctors, practitioners, and hospital administrators, ensuring privacy and security. A blockchain network facilitates the retrieval of patient health information, with doctors acting as light nodes accessible via smartphones or computers, while hospitals operate as full nodes, storing a complete replica of the blockchain and participating in the consensus process. Other users, although they may possess a copy of the blockchain, are not permitted to engage in the consensus mechanism, maintaining a controlled and secure environment for sensitive health data. This hierarchical structure ensures that only trusted entities can access and manage patient information, enhancing data integrity and confidentiality. The different participants and their privileges in the proposed system are mentioned in Table 2.
- Electronic health record: An electronic health record (EHR) is a comprehensive digital version of a patient's medical history, encompassing critical health information such as diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory test results. EHRs enable real-time access to patient data by authorized healthcare professionals, improving care coordination among providers and enhancing healthcare outcomes. In the proposed system, healthcare professionals exclusively create an EHR for each patient, including essential details like birth information, residence, contact number, patient ID, medical

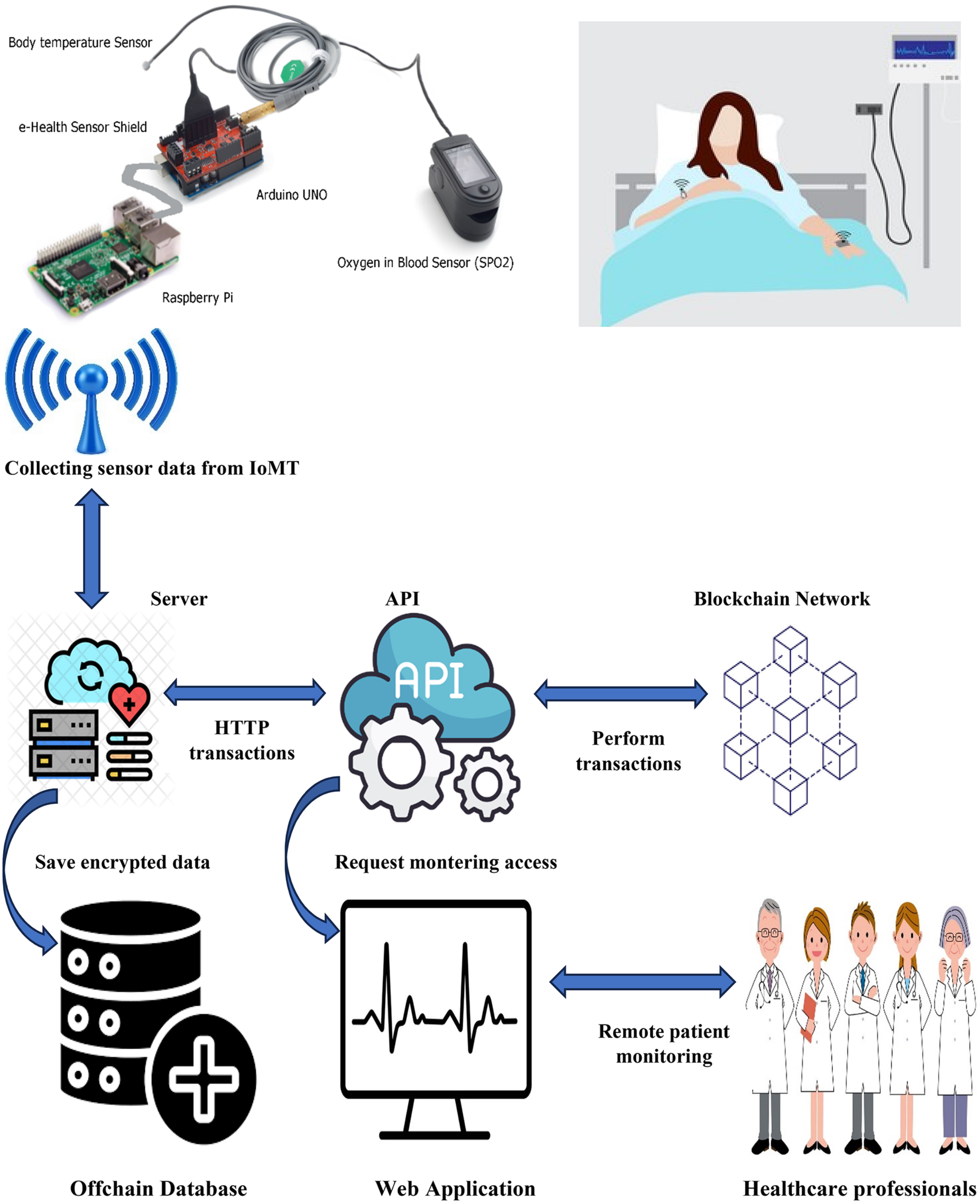


Fig. 1. The proposed EHRGuard architecture.

Sensor	Normal	Abnormal
EMG	40–90mV	450–780mV
SpO_2	96–99%	i < 90
Body temperature	36.5–37.5^0 C	i > 40.0–41.5℃
Pulse rate	70–100 bpm	i < 70

Table 1. Details of sensors used in the proposed system.

Participant-ID	Actor	Privilege
1	Admin	• Add New Users – Healthcare administrators can register new users, including patients, doctors, and hospital staff, by verifying their credentials and assigning appropriate access rights. • Create Records – Upon patient registration, a unique patient ID is generated, and an Electronic Health Record (EHR) is securely created, storing personal details, medical history, and prescriptions. • Access Patient Data – Authorized entities, such as doctors and healthcare providers, can securely retrieve patient data from the off-chain database while verifying integrity through blockchain records. • Update Patient Details – Patients' personal information, such as contact details and residence, can be modified while maintaining historical changes for auditability. • Update Medical Prescriptions & History – Doctors can securely add or modify prescriptions and medical history, ensuring accurate and real-time updates for better patient care. • Remove Users – Administrators can revoke access for inactive or unauthorized users, ensuring data security and compliance with healthcare regulations. • Update User Information – User roles, permissions, and other details can be modified based on authorization levels, ensuring a dynamic and adaptable system.
2	Doctor	• Access Patient Data – Healthcare professionals can securely retrieve patient records, including personal details, medical history, and prescriptions, from the off-chain database. Blockchain ensures data integrity by recording any modifications. • Update Patient Details – Authorized users can modify patient information such as contact details, address, or emergency contacts while maintaining an audit trail of changes. • Update Medical Prescriptions & History – Doctors can add or modify prescriptions and medical history in a secure and traceable manner, ensuring real-time updates for accurate patient care. • Access Patient Health Overview (Real-Time Monitoring) – The system continuously collects and analyzes real-time sensor data (e.g., heart rate, oxygen levels, temperature) from IoT-based medical devices. Alerts are triggered if any vital signs exceed predefined thresholds, enabling timely medical intervention.
3	Patient	Access patient data and patient health overview

Table 2. System Actor's and their access privileges.

history, and medical prescriptions. The medical prescriptions section contains medication data, such as the name, details, prescription date, patient ID, and doctor's information, while the medical history segment includes patient ID, first name, last name, disease description, date, updated date, and status. Only authorized healthcare practitioners can access these records, ensuring data security and privacy. Both the EHR and patient health information collected from IoT sensors can be utilized for research, remote monitoring, and analysis, fostering a more efficient and interconnected healthcare ecosystem that replaces traditional paper-based systems with a seamless, digital approach.

- Permissioned blockchain: A permissioned blockchain is a type of blockchain network where access and participation in the network are restricted to a defined set of participants. Unlike public blockchains where anyone can join and participate in the network, permissioned blockchains require participants to be authorized or granted permission to engage in various activities such as validating transactions, accessing data, and participating in the consensus process[27]. A permissioned blockchain-based data monitoring system can provide a secure, transparent, and efficient solution for various industries such as healthcare, supply chain, and finance, where controlled access and privacy are paramount. In this paper, the proposed system for monitoring patient data is supported by a lightweight, permissioned blockchain carefully crafted to establish a secure and regulated environment for both patients and healthcare professionals. This permissioned blockchain serves as a digital infrastructure, facilitating the secure storage and retrieval of data[28]. To ensure data validation, the associated hash values of each patient's Electronic Health Record (EHR) are recorded on the blockchain after storage and encryption. Furthermore, the permissioned blockchain is designed to store crucial patient monitoring data, specifically Internet of Medical Things (IoMT) sensor values, as transactions. This methodology acts as a safeguard against potential tampering or forgery of records. For instance, when a new set of monitoring data is collected at defined intervals, it is recorded into the blockchain as a transaction if it deviates from the expected norms. Additionally, any modifications or updates made to sensor information, access control lists, medical history, medical prescriptions, treatment plans, vital statistics, and EHRs are recorded as transactions on the blockchain. Additionally, the client application employs the REST API for administering the blockchain network, facilitating transaction requests such as task generation services, as well as user and device registration. Participants, including patients and doctors, have the capability to submit transactions, whether to create a new task or to receive a response from a previously generated task via the healthcare IoT server[29].
- Off-chain database: An off-chain database is a storage system that operates independently of a blockchain, serving as an external repository for data that is not stored directly on the blockchain. This approach is particularly useful for managing large volumes of data, such as files, documents, or detailed records, which would be impractical or inefficient to store on-chain due to limitations in storage capacity, cost, or performance. In the context of healthcare, when a new patient registers with healthcare professionals, a unique patient ID and Electronic Health Record (EHR) are generated[30]. The EHR contains critical information such as birth details, residence, contact information, medical history, and prescriptions. To ensure security, each patient's EHR is encrypted and stored in an off-chain database, alongside other relevant data like sensor details, sensor values, vital statistics, and access control lists. This off-chain storage strategy enhances efficiency and scalability, enabling streamlined access and management of patient information while maintaining data confidentiality. While the off-chain database provides a secure and efficient repository for sensitive patient data, blockchain technology complements it by offering a decentralized, tamper-resistant ledger that records data modifications. This combination ensures real-time access to patient data for healthcare professionals while maintaining data consistency and enabling secure data sharing across entities such as hospitals, doctors, and researchers.

However, for large-scale static healthcare data, a purely blockchain-based architecture may require significant resources. Therefore, integrating an off-chain database with a permissioned blockchain architecture presents a more efficient and resilient solution for managing patient information in remote healthcare settings[31]. This hybrid approach not only preserves data integrity but also achieves a balance between data privacy, security, and accessibility, making it a robust framework for modern healthcare systems.

Adversary model of the proposed scheme

The adversary model of the proposed scheme outlines potential threats and adversaries that the system is designed to mitigate or withstand. It helps in understanding the security considerations and scenarios where the system may face challenges. The adversary model typically identifies potential attackers, their capabilities, and the assumed conditions under which they may operate. For example, in a healthcare-related blockchain system, potential adversaries could include:

- Unauthorized users: Adversaries may attempt to gain unauthorized access to the system, posing a threat to the confidentiality of sensitive health data. The model should consider measures to prevent unauthorized login attempts, account hijacking, or any form of unauthorized access.
- Tampering with patient data: Adversaries may try to manipulate or tamper with patient data stored in the blockchain. The system should be resilient against unauthorized modifications to ensure the integrity of health records.
- Eavesdropping and man-in-the-middle attacks: Adversaries may try to eavesdrop on communications or conduct man-in-the-middle attacks to intercept and manipulate data transmissions. The model should address encryption and secure communication protocols to prevent these threats.
- Denial-of-service (DoS) Attackers: Adversaries may attempt to disrupt the availability of the system by launching DoS attacks. The model should include strategies to mitigate and withstand such attacks, ensuring continuous service availability.
- Sybil attacks: Sybil attacks involve adversaries creating multiple fake identities to undermine the network. The adversary model should account for measures to detect and prevent Sybil attacks that could compromise the consensus mechanism.
- Privacy concerns: Adversaries may attempt to breach patient privacy by extracting sensitive information. The model should address privacy-preserving measures, ensuring that patient data remains confidential and is accessible only to authorized parties.
- Blockchain network attacks: Adversaries might target the underlying blockchain network. The model should consider protections against 51% attacks, double-spending attacks, and other vulnerabilities specific to the chosen blockchain technology.

Requirements of security for healthcare IoT system

Securing a healthcare Internet of Things system is crucial to safeguard sensitive patient data, maintain the integrity of medical information, and ensure the reliability of connected devices. Here are key security requirements for a healthcare IoT system:

- Device authentication: Implement secure authentication mechanisms for IoT devices to ensure that only authorized and authenticated devices can connect to the system. This prevents unauthorized access and potential attacks.
- Access control: Enforce strict access controls to regulate who can access and interact with the healthcare IoT system.
- Data encryption: Implement end-to-end encryption for data transmitted between IoT devices, gateways, and the central system. This ensures that health data remains confidential and secure during transmission.
- Integrity checking: Use cryptographic mechanisms, such as digital signatures, to verify the integrity of data collected from IoT devices. This helps ensure that the data has not been tampered with during transit or storage.
- Secure communication: Utilize secure communication protocols (e.g., HTTPS, MQTT with TLS) to protect data exchanged between IoT devices and the central system. This safeguards against eavesdropping and man-in-the-middle attacks.
- Privacy preservation: Implement measures to protect patient privacy, such as anonymization and de-identification of data where appropriate. Aligns with healthcare regulations and safeguards sensitive patient information.

Design goal

The IoMT (Internet of Medical Things) presents unique challenges due to the vulnerabilities of sensor nodes that are often deployed in hostile or hazardous environments. These nodes are susceptible to various attacks, such as network perturbation, data manipulation, and replay attacks, which can compromise the accuracy of data aggregation and potentially mislead healthcare systems. To address these challenges, the proposed system aims to meet several critical objectives:

- Security: The system must ensure the confidentiality, integrity, and authentication of data transmitted through IoT networks. This is particularly vital for healthcare applications, where unauthorized access or data manipulation can have severe consequences. The system should be designed to withstand compromised nodes and prevent data tampering. Additional security measures such as access control and availability must also be implemented to ensure that data remains secure and accessible only to authorized users.

- High energy efficiency: Energy efficiency is essential for maintaining the longevity of sensor networks, especially when nodes are battery-powered or have limited energy resources. The proposed aggregation scheme must minimize energy consumption by reducing computing load and communication overhead. This will not only preserve the energy of sensor nodes but also extend the overall lifetime of the network, ensuring continuous and reliable operation over extended periods.
- Scalability: As the IoMT ecosystem grows, the system must be scalable enough to handle an increasing number of IoT devices, users, and data without compromising performance. The design should allow seamless expansion, ensuring that the system can accommodate additional devices and more data without overwhelming the infrastructure. Scalability is key to ensuring that the solution remains effective as healthcare IoT networks evolve and expand.

Proposed EHRguard description

This section delineates a sequential interaction illustrating how patients are equipped with Internet of Medical Things (IoMT) sensors, healthcare professionals, an off-chain database, and blockchain technology collaboratively operate to establish a secure, transparent, and efficient remote patient monitoring system. The integration of blockchain and off-chain databases is instrumental in fortifying data security, upholding integrity, ensuring accessibility, preserving patient privacy, and facilitating the delivery of remote healthcare services. In the following, we provide a description of each phase.

Collection and transmission of data through IoMT sensors

Figure 2 illustrates a sequence diagram outlining the steps for adding patient health records in the proposed EHRGuard system. The process begins with enrolling each patient into the Health System, followed by the attachment of medical sensors based on a doctor's recommendation. Medical staff affix these sensors to the patient's body, enabling real-time monitoring of vital signs such as respiration rate, pulse rate, oxygen levels, and glucose levels. The Health System maintains a centralized database to store all relevant patient information, including Electronic Health Records. Sensor data is wirelessly transmitted to a gateway powered by a Raspberry Pi, which acts as a bridge for Internet of Medical Things devices. This gateway forwards the collected data to an off-chain database, accessible exclusively to authorized healthcare professionals. The medical IoT server processes queries and leverages blockchain technology to ensure secure, transparent, and tamper-proof data handling. Finally, statistical information is sent to a web application for analysis, enabling healthcare providers to make informed decisions and improve patient care. This integrated approach ensures efficient, secure, and real-time health monitoring and data management.

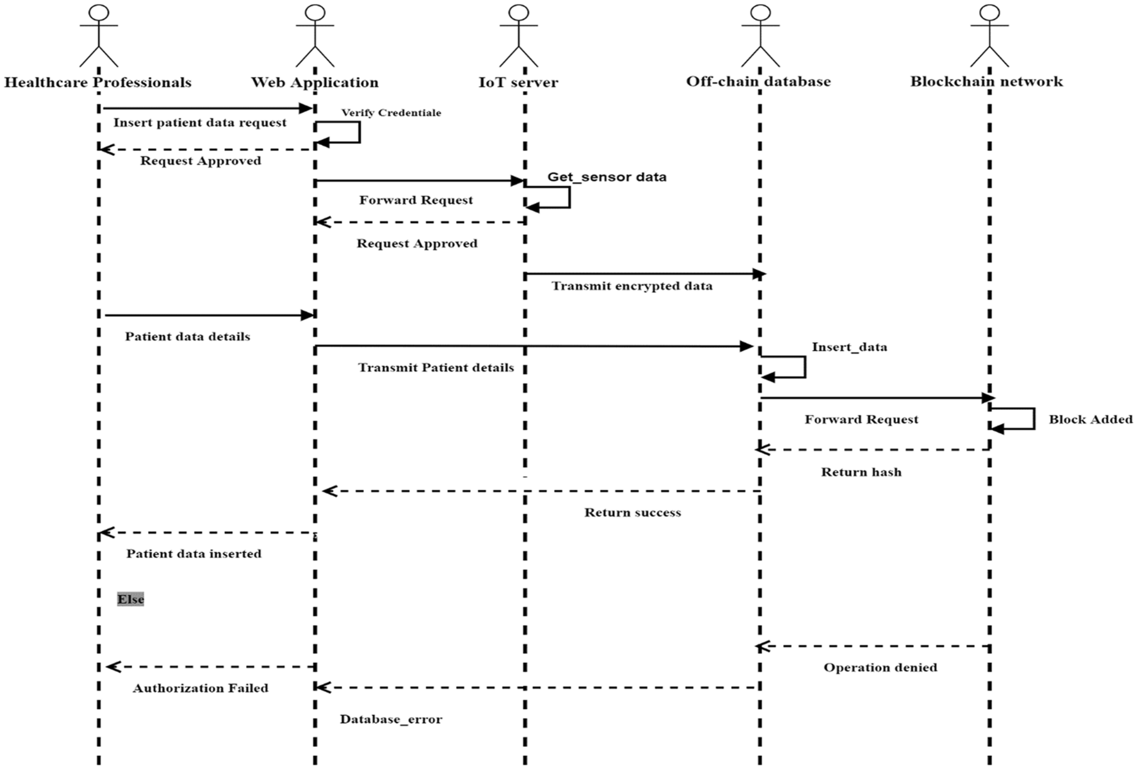
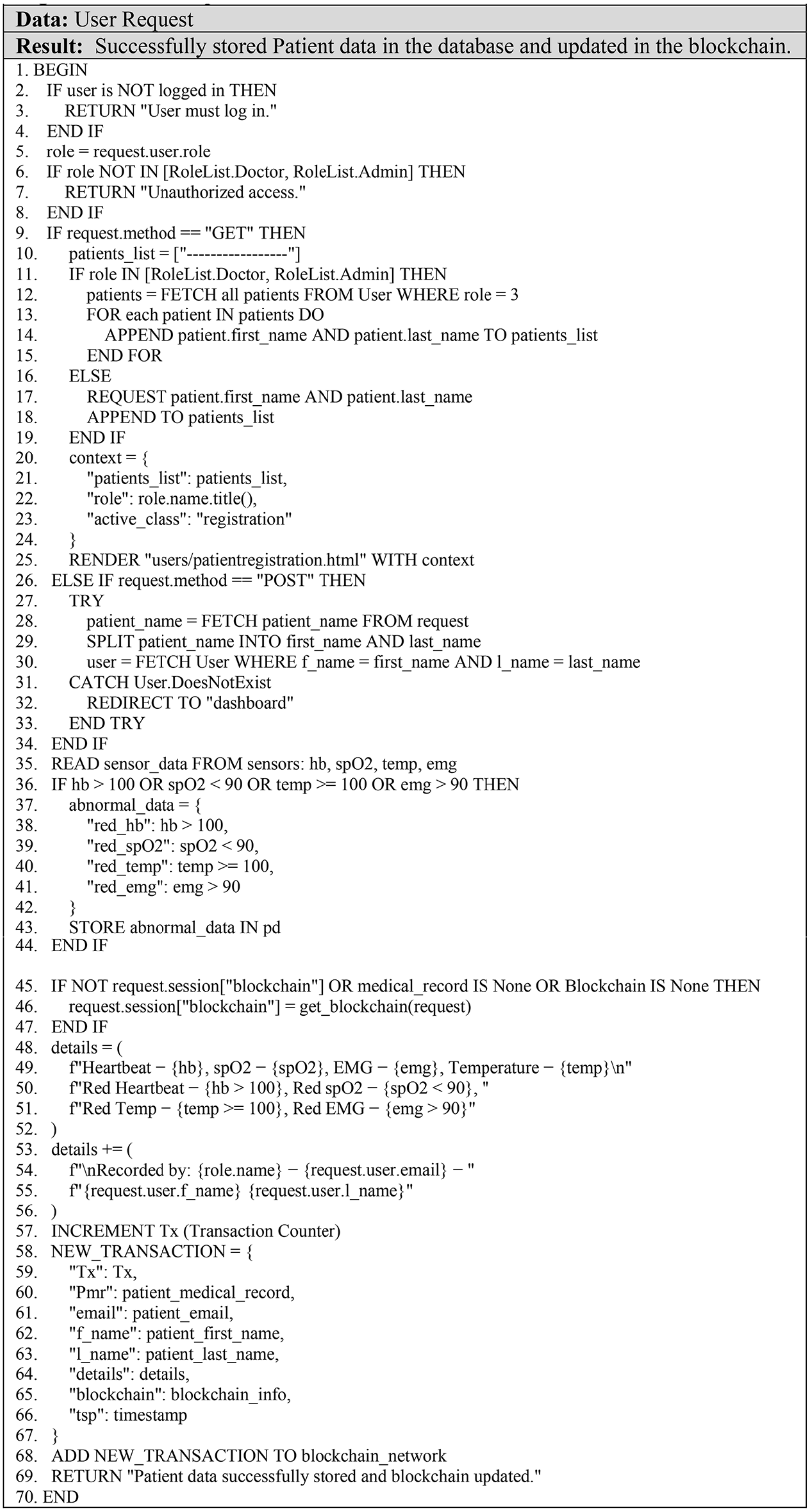


Fig. 2. Sequence diagram for adding patient health records for the proposed EHRGuard system.

Data recordation in database and blockchain

Algorithm 1 is designed to securely add patient health and sensor data to both the database and the blockchain, ensuring the integrity and confidentiality of sensitive information. It handles new patient registration, initiated by an administrator, and records data as a transaction in the form of metadata when either a new patient is registered, or the sensor diagnostic status exceeds normal values. This metadata is used to create a new block in the blockchain. The algorithm ensures that data is only recorded when abnormal behavior is detected, preventing unnecessary entries for normal or ongoing sensor readings. Patient data is first encrypted using a



Data: User Request

Result: Successfully stored Patient data in the database and updated in the blockchain.

```
BEGIN
  IF user is NOT logged in THEN
    RETURN "User must log in."
  END IF
  role = request.user.role
  IF role NOT IN [RoleList.Doctor, RoleList.Admin] THEN
    RETURN "Unauthorized access."
  END IF
  IF request.method == "GET" THEN
    patients_list = ["-----------------"]
    IF role IN [RoleList.Doctor, RoleList.Admin] THEN
      patients = FETCH all patients FROM User WHERE role = 3
      FOR each patient IN patients DO
        APPEND patient.first_name AND patient.last_name TO patients_list
      END FOR
    ELSE
      REQUEST patient.first_name AND patient.last_name
      APPEND TO patients_list
    END IF
    context = {
      "patients_list": patients_list,
      "role": role.name.title(),
      "active_class": "registration"
    }
    RENDER "users/patientregistration.html" WITH context
  ELSE IF request.method == "POST" THEN
    TRY
      patient_name = FETCH patient_name FROM request
      SPLIT patient_name INTO first_name AND last_name
      user = FETCH User WHERE f_name = first_name AND l_name = last_name
    CATCH User.DoesNotExist
      REDIRECT TO "dashboard"
    END TRY
  END IF
  READ sensor_data FROM sensors: hb, spO2, temp, emg
  IF hb > 100 OR spO2 < 90 OR temp >= 100 OR emg > 90 THEN
    abnormal_data = {
      "red_hb": hb > 100,
      "red_spO2": spO2 < 90,
      "red_temp": temp >= 100,
      "red_emg": emg > 90
    }
    STORE abnormal_data IN pd
  END IF

  IF NOT request.session["blockchain"] OR medical_record IS None OR Blockchain IS None THEN
    request.session["blockchain"] = get_blockchain(request)
  END IF
  details = (
    f"Heartbeat − {hb}, spO2 − {spO2}, EMG − {emg}, Temperature − {temp}\n"
    f"Red Heartbeat − {hb > 100}, Red spO2 − {spO2 < 90}, "
    f"Red Temp − {temp >= 100}, Red EMG − {emg > 90}"
  )
  details += (
    f"\nRecorded by: {role.name} − {request.user.email} − "
    f"{request.user.f_name} {request.user.l_name}"
  )
  INCREMENT Tx (Transaction Counter)
  NEW_TRANSACTION = {
    "Tx": Tx,
    "Pmr": patient_medical_record,
    "email": patient_email,
    "f_name": patient_first_name,
    "l_name": patient_last_name,
    "details": details,
    "blockchain": blockchain_info,
    "tsp": timestamp
  }
  ADD NEW_TRANSACTION TO blockchain_network
  RETURN "Patient data successfully stored and blockchain updated."
END
```

Algorithm 1. Insert patient & sensor data in the blockchain.

secure encryption mechanism before being stored in the database, and its hashed reference is uploaded as a transaction to the blockchain. Each data entry is appended as a block, creating a tamper-resistant ledger that guarantees the immutability of patient health data, protecting it from unauthorized changes or deletions. The algorithm also supports flexible mapping between patients and sensors, allowing for one-to-one or one-to-many relationships. Vital sign data is stored as a JSON array and transmitted to the healthcare IoT server via a POST request, with communication between the IoT gateway and the server facilitated by the CoAP protocol. This comprehensive approach ensures secure, efficient, and transparent management of patient health data.

Consensus mechanism and verification of blocks

Proof-of-Work (PoW) is a consensus mechanism that ensures agreement among distributed participants in a blockchain network regarding the state of the ledger. It plays a critical role in creating new blocks and securing the network against malicious activities, such as double-spending attacks and unauthorized tampering with block history. In the proposed system, hospital administration acts as trusted validators, responsible for verifying transactions, constructing blocks, and appending them to the blockchain. The PoW algorithm involves solving a computationally complex scientific puzzle, which serves as a deterrent against adversaries by limiting their economic capabilities to disrupt the network[32]. A hash function is central to this process, providing a random and complex mathematical mechanism to validate transactions stored in the blockchain. Each block contains its hash value, transaction history, and the hash value of the previous block, ensuring a secure and immutable chain. During the PoW process, nodes in the network calculate the hash value of the block header, and upon discovering the target value, a node broadcasts the new block to the network. Other nodes verify the accuracy of the hash value, and once validated, the block is collectively added to the blockchain. Figure 3 illustrates the PoW flow, highlighting its secure and decentralized nature. The key advantages of PoW include its robust security measures and its ability to promote decentralization, making it a reliable foundation for maintaining the integrity and trustworthiness of the blockchain network.

Continuous monitoring and real-time alerts

Algorithm 2 plays a central role in managing patient sensor data by providing an overview of the information received from patients and enabling access to a personalized dashboard for healthcare professionals. This dashboard allows users to review patient data using filters such as date, time, and profile parameters. Upon receiving sensor data, Algorithm 2 analyzes it, focusing on detecting abnormal readings that fall outside the expected range, which are flagged as “red” for visual emphasis. The system generates real-time alerts and notifications for healthcare experts when critical health issues or deviations from predefined parameters are identified, enabling timely treatment adjustments or prescription changes. This rapid detection of abnormalities serves as a vital safety feature, ensuring prompt attention to potential health risks. Conversely, readings within the normal range are integrated into the patient’s record and securely stored in the database, ensuring accurate documentation for future reference or analysis. Essentially, Algorithm 2 acts as a crucial intermediary, managing, analyzing, and presenting patient sensor data in a way that allows healthcare professionals to effectively monitor and respond to patient health. Figure 4 illustrates the sequence diagram for remote patient monitoring, highlighting the system’s workflow.

Medicine prescriptions

Algorithm 3 is responsible for generating and retrieving patient medical prescriptions, which include critical details such as patient ID, medicine ID, medicine name, comprehensive medicine details, doctor information (first name and last name), and the prescription issuance date. Patients are granted access to view only their own prescriptions, while doctors have the authority to create and update them. When healthcare professionals modify a prescription, the updated record is securely stored in both the database and the ledger, ensuring a transparent and accountable system that maintains a comprehensive history of all changes made to medical prescriptions.

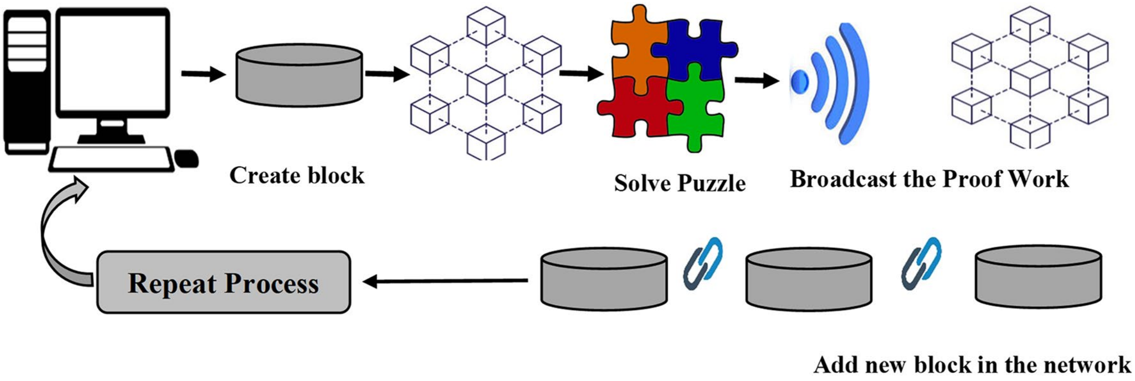
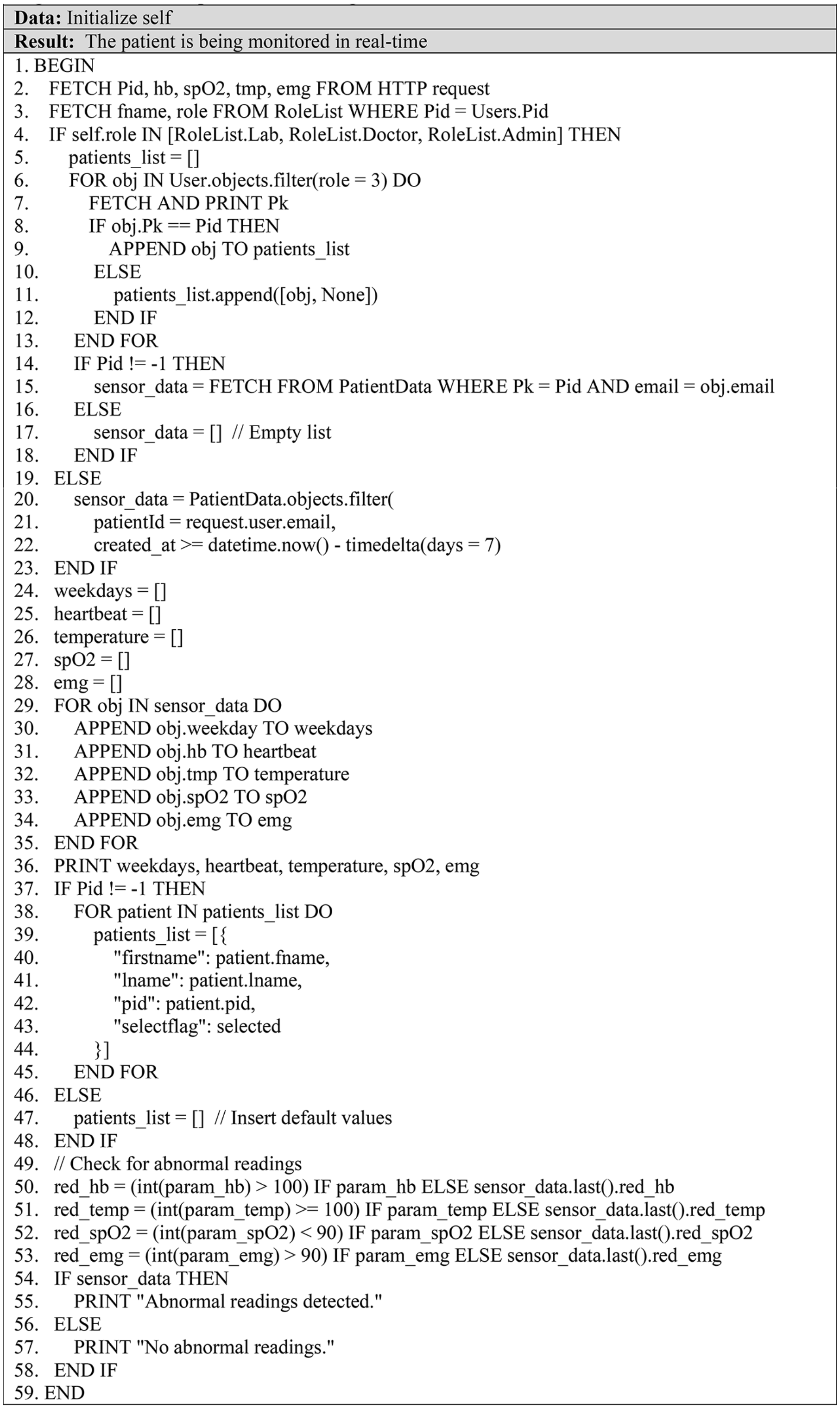


Fig. 3. The proof of work consensus algorithm.



Data: Initialize self

Result: The patient is being monitored in real-time

```
BEGIN
  FETCH Pid, hb, spO2, tmp, emg FROM HTTP request
  FETCH fname, role FROM RoleList WHERE Pid = Users.Pid
  IF self.role IN [RoleList.Lab, RoleList.Doctor, RoleList.Admin] THEN
      patients_list = []
      FOR obj IN User.objects.filter(role = 3) DO
          FETCH AND PRINT Pk
          IF obj.Pk == Pid THEN
              APPEND obj TO patients_list
           ELSE
              patients_list.append([obj, None])
           END IF
      END FOR
      IF Pid != -1 THEN
          sensor_data = FETCH FROM PatientData WHERE Pk = Pid AND email = obj.email
      ELSE
          sensor_data = []  // Empty list
      END IF
  ELSE
      sensor_data = PatientData.objects.filter(
          patientId = request.user.email,
          created_at >= datetime.now() - timedelta(days = 7)
  END IF
  weekdays = []
  heartbeat = []
  temperature = []
  spO2 = []
  emg = []
  FOR obj IN sensor_data DO
      APPEND obj.weekday TO weekdays
      APPEND obj.hb TO heartbeat
      APPEND obj.tmp TO temperature
      APPEND obj.spO2 TO spO2
      APPEND obj.emg TO emg
  END FOR
  PRINT weekdays, heartbeat, temperature, spO2, emg
  IF Pid != -1 THEN
      FOR patient IN patients_list DO
          patients_list = [{
              "firstname": patient.fname,
              "lname": patient.lname,
              "pid": patient.pid,
              "selectflag": selected
          }]
      END FOR
  ELSE
      patients_list = []  // Insert default values
  END IF
  // Check for abnormal readings
  red_hb = (int(param_hb) > 100) IF param_hb ELSE sensor_data.last().red_hb
  red_temp = (int(param_temp) >= 100) IF param_temp ELSE sensor_data.last().red_temp
  red_spO2 = (int(param_spO2) < 90) IF param_spO2 ELSE sensor_data.last().red_spO2
  red_emg = (int(param_emg) > 90) IF param_emg ELSE sensor_data.last().red_emg
  IF sensor_data THEN
      PRINT "Abnormal readings detected."
  ELSE
      PRINT "No abnormal readings."
  END IF
END
```

Algorithm 2. Remote patient monitoring.

Medical history

Algorithm 4 is specifically designed for the creation and retrieval of the patient's medical history. The records within this algorithm include crucial details such as the patient's name, patient ID, a comprehensive history of diseases, or any ongoing medical conditions, along with associated dates for each disease event and the current health status of the patient. To maintain a secure and transparent Electronic Health Record for the patient, a new block is appended to the blockchain whenever there is a recording or update to the medical history. This process

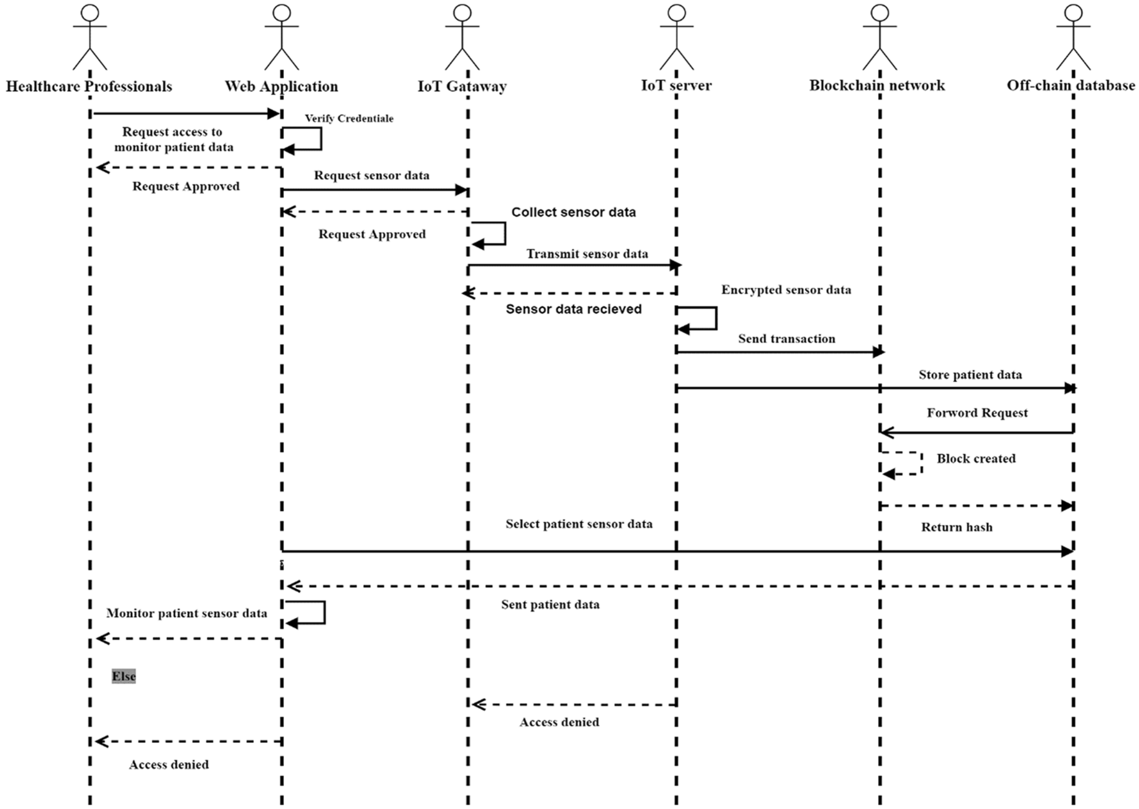


Fig. 4. Sequence diagram for remote patient monitoring for the proposed EHRGuard system.

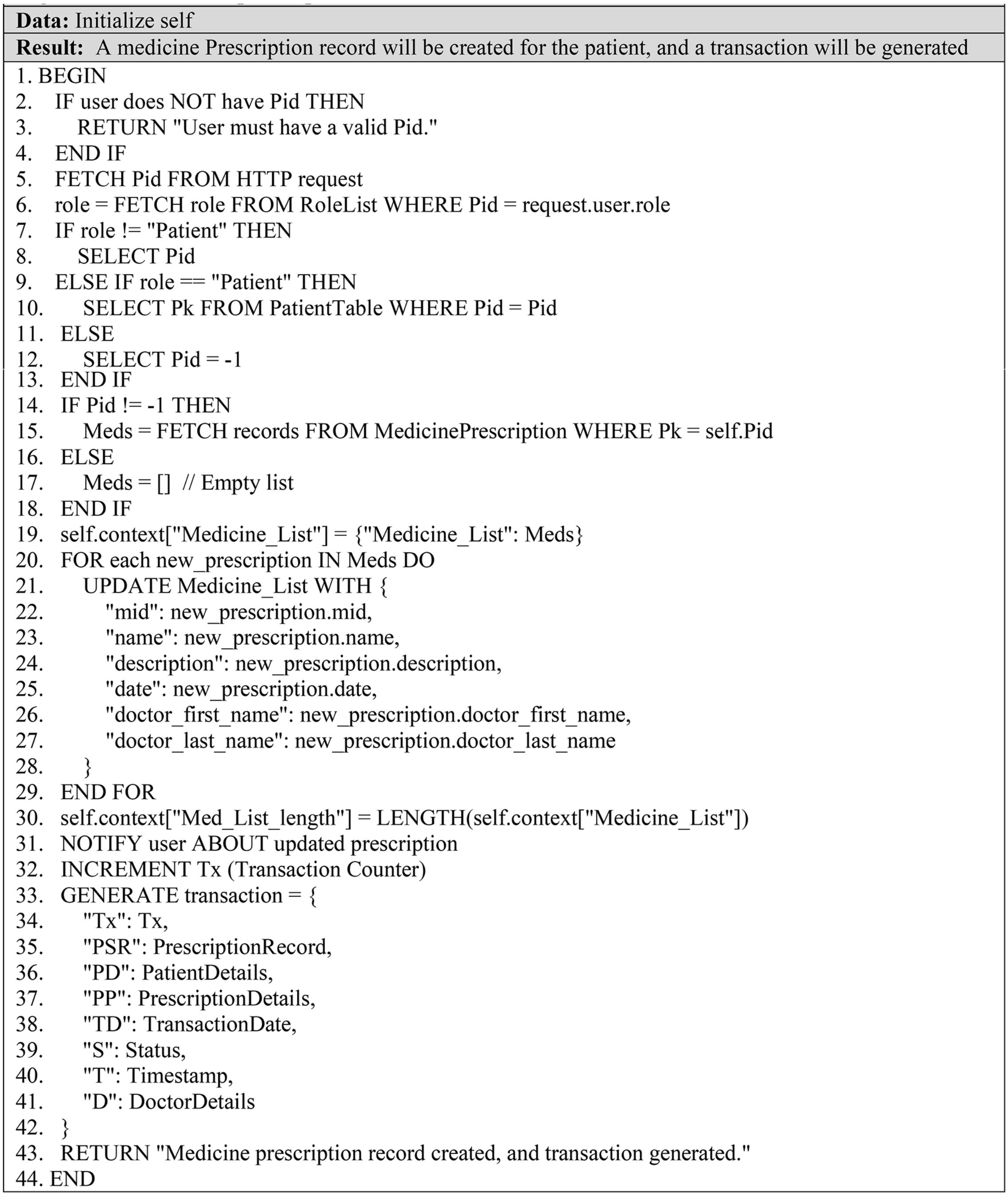
ensures the integrity and immutability of the patient's health information within the blockchain, providing a reliable and transparent history of their medical journey.

Security analysis and evaluation of the EHRguard system

Security analysis

Security analysis involves a thorough analysis of the measures integrated into the EHRGuard system to safeguard patient health information against unauthorized access, data breaches, and potential vulnerabilities. The proposed system leverages blockchain and Internet of Medical Things (IoMT) technologies to ensure that healthcare data remains secure, private, and tamper resistant. This section highlights key security aspects, addressing essential factors such as data integrity, confidentiality, privacy, user control, immutability, scalability, availability, traceability, and transparency.

1. Data Integrity: The off-chain database securely stores patient Electronic Health Records (EHRs) using advanced encryption techniques. The encryption generates keys that are stored within the blockchain blocks. Each block contains a cryptographic hash of the preceding block, forming an interconnected chain. This design ensures that any alteration to the data would result in a mismatch of the hash values, making unauthorized modification almost impossible. The immutability of blockchain guarantees the integrity of patient data, ensuring that it cannot be tampered with or corrupted.
2. Confidentiality: Patient confidentiality is paramount in healthcare systems. The EHRGuard system ensures that only authorized users, such as healthcare providers and medical professionals, can access sensitive patient information. The access control mechanism ensures that unauthorized individuals are unable to view or manipulate patient health records. This restriction upholds the privacy of healthcare data and protects it from exposure to unauthorized parties.
3. Privacy: To protect patient privacy, the EHRGuard system utilizes a permissioned consortium blockchain, which limits access to the system to only those who are authorized to view or manage patient data. Blockchain regulates access to the encrypted data stored in the off-chain database, ensuring that patient records are shielded from unauthorized access. These mechanisms provide an additional layer of security by ensuring that only trusted healthcare providers can access the sensitive health information.
4. User Control: Empowering patients with control over their own health data is a key feature of the EHRGuard system. Patients have the ability to decide who can access their data and can revoke access at any time. This level of control ensures that individuals maintain autonomy over their personal health information and can make informed decisions about its sharing. This approach aligns with modern healthcare principles of patient consent and privacy.



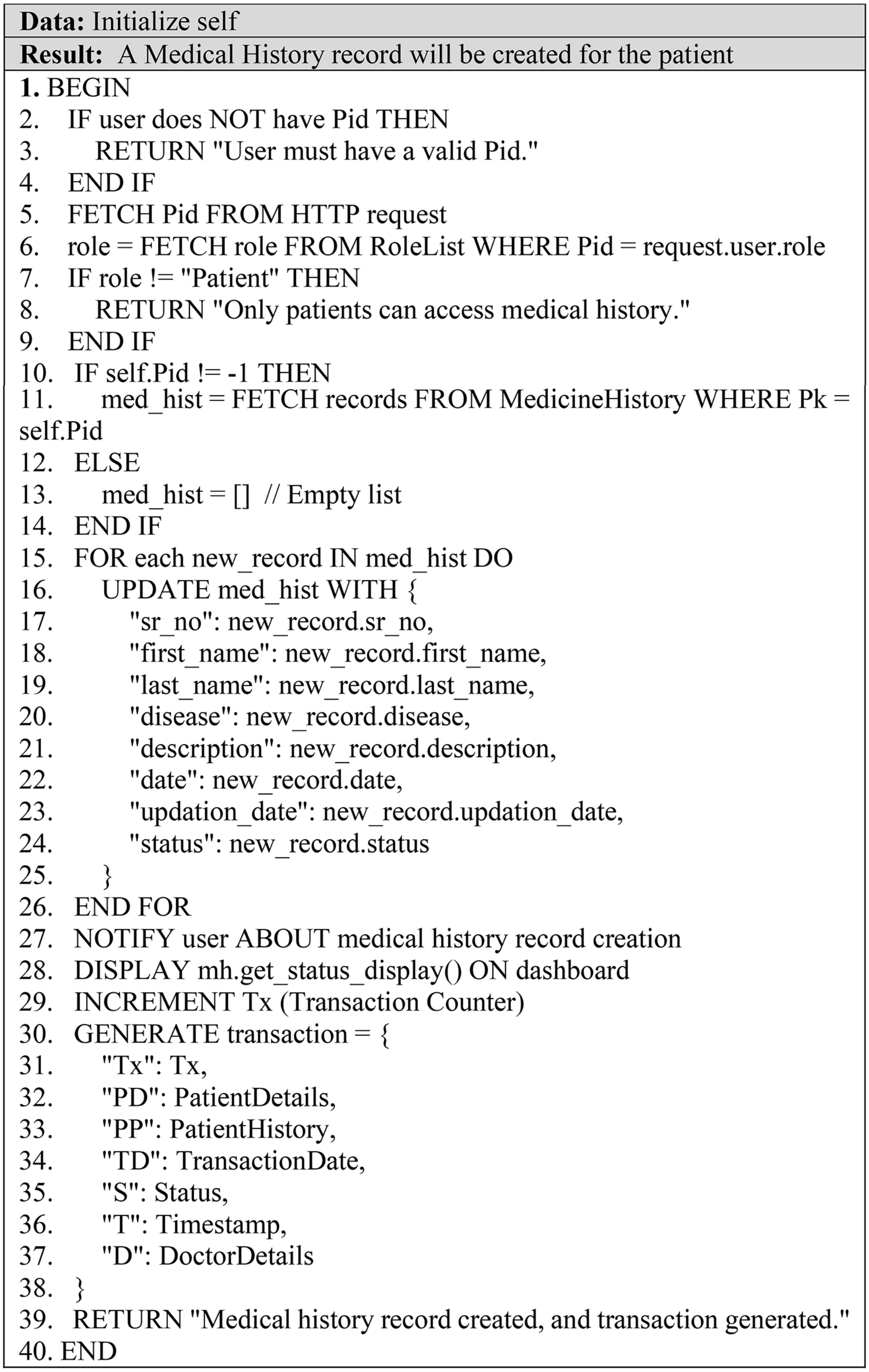
Data: Initialize self

Result: A medicine Prescription record will be created for the patient, and a transaction will be generated

```
BEGIN
  IF user does NOT have Pid THEN
    RETURN "User must have a valid Pid."
  END IF
  FETCH Pid FROM HTTP request
  role = FETCH role FROM RoleList WHERE Pid = request.user.role
  IF role != "Patient" THEN
    SELECT Pid
  ELSE IF role == "Patient" THEN
    SELECT Pk FROM PatientTable WHERE Pid = Pid
  ELSE
    SELECT Pid = -1
  END IF
  IF Pid != -1 THEN
    Meds = FETCH records FROM MedicinePrescription WHERE Pk = self.Pid
  ELSE
    Meds = []  // Empty list
  END IF
  self.context["Medicine_List"] = {"Medicine_List": Meds}
  FOR each new_prescription IN Meds DO
    UPDATE Medicine_List WITH {
      "mid": new_prescription.mid,
      "name": new_prescription.name,
      "description": new_prescription.description,
      "date": new_prescription.date,
      "doctor_first_name": new_prescription.doctor_first_name,
      "doctor_last_name": new_prescription.doctor_last_name
    }
  END FOR
  self.context["Med_List_length"] = LENGTH(self.context["Medicine_List"])
  NOTIFY user ABOUT updated prescription
  INCREMENT Tx (Transaction Counter)
  GENERATE transaction = {
    "Tx": Tx,
    "PSR": PrescriptionRecord,
    "PD": PatientDetails,
    "PP": PrescriptionDetails,
    "TD": TransactionDate,
    "S": Status,
    "T": Timestamp,
    "D": DoctorDetails
  }
  RETURN "Medicine prescription record created, and transaction generated."
END
```

Algorithm 3. Medicine prescriptions.

5. Immutability: The use of blockchain ensures the immutability of patient records. Once data is uploaded to the blockchain, it becomes resistant to modification or deletion. This feature protects the data from both intentional tampering and accidental changes, ensuring that the information remains authentic. The immutability of blockchain significantly strengthens the security of patient data by preventing unauthorized alterations and fostering trust among stakeholders.
6. Scalability: The EHRGuard system's architecture is designed for scalability, enabling it to manage and process large volumes of patient data efficiently. Data is encrypted and securely stored in the off-chain database, with its hash value documented in the blockchain. This approach allows the system to handle substantial amounts of data with lower latency. The integration of off-chain databases and permissioned blockchain ensures the scalability of the system, enabling it to grow as the number of patients and healthcare transactions increases.
7. Availability: Availability is ensured through a decentralized system architecture. By using multiple distributed nodes, the EHRGuard system eliminates single points of failure. If one node becomes unavailable, the system remains operational, and other nodes can continue to provide access to patient data. This decentral-



Data: Initialize self

Result: A Medical History record will be created for the patient

```
BEGIN
    IF user does NOT have Pid THEN
        RETURN "User must have a valid Pid."
    END IF
    FETCH Pid FROM HTTP request
    role = FETCH role FROM RoleList WHERE Pid = request.user.role
    IF role != "Patient" THEN
        RETURN "Only patients can access medical history."
    END IF
    IF self.Pid != -1 THEN
        med_hist = FETCH records FROM MedicineHistory WHERE Pk = self.Pid
    ELSE
        med_hist = []  // Empty list
    END IF
    FOR each new_record IN med_hist DO
        UPDATE med_hist WITH {
            "sr_no": new_record.sr_no,
            "first_name": new_record.first_name,
            "last_name": new_record.last_name,
            "disease": new_record.disease,
            "description": new_record.description,
            "date": new_record.date,
            "updation_date": new_record.updation_date,
            "status": new_record.status
        }
    END FOR
    NOTIFY user ABOUT medical history record creation
    DISPLAY mh.get_status_display() ON dashboard
    INCREMENT Tx (Transaction Counter)
    GENERATE transaction = {
        "Tx": Tx,
        "PD": PatientDetails,
        "PP": PatientHistory,
        "TD": TransactionDate,
        "S": Status,
        "T": Timestamp,
        "D": DoctorDetails
    }
    RETURN "Medical history record created, and transaction generated."
END
```

Algorithm 4. Medical history.

ized approach ensures high availability and enhances system resilience, ensuring continuous access to critical health information even during network disruptions or server failures.

8. Traceability: The use of blockchain introduces transparency into the system. All transactions related to patient records are publicly visible to authorized participants within the network, fostering openness and accountability. This transparency ensures that any changes made to the data are easily verifiable and that the integrity of the health data is maintained. Authorized healthcare providers can confidently access the data, knowing it is securely managed and immutable.

The EHRGuard system offers a comprehensive security framework for healthcare data management, addressing critical issues such as data integrity, confidentiality, privacy, and traceability. By integrating blockchain and IoT technologies, the system ensures that patient health information is secure, transparent, and tamper-resistant. The decentralized nature of blockchain, combined with robust encryption, access controls, and user empowerment, makes EHRGuard a reliable and secure solution for modern healthcare data management. This security evaluation confirms that the system effectively mitigates risks such as unauthorized access, data breaches, and tampering, while ensuring the availability and scalability necessary for large-scale healthcare applications.

Security evaluation under different attack scenarios

In this section, we provide an expanded security evaluation of EHRGuard, focusing on how the system performs under various attack scenarios, including man-in-the-middle (MITM), denial of service (DoS), Sybil, and replay attacks. Each section includes a discussion on the specific mitigation strategies used, along with experimental results to demonstrate how EHRGuard handles these potential threats.

A Man-in-the-Middle (MITM) attack occurs when an attacker intercepts communication between two parties, such as a patient's IoMT device and a healthcare provider's system, potentially compromising patient data. To mitigate this, EHRGuard encrypts all communication between IoMT devices, patients, and healthcare professionals using SSL/TLS protocols, ensuring end-to-end encryption and preventing attackers from modifying or reading transmitted data. Additionally, blockchain technology is employed to verify data integrity, with IoMT devices authenticated and registered on the blockchain network to prevent unauthorized access. We conducted a series of simulations to evaluate the system's resilience to MITM attacks under different conditions. For the first setup, Without Encryption, no encryption mechanisms were employed, simulating an unsecured communication channel between the patient's IoMT device and the healthcare professional's system. In this case, the MITM attacker was able to intercept the data being transmitted, such as heart rate, oxygen levels, and other vital signs. The attacker modified the values, injecting false data into the communication stream, which led to corrupted health information being sent to the healthcare provider. This corrupted data could potentially result in incorrect diagnoses or treatment recommendations, highlighting the critical risk posed by MITM attacks in an unprotected system. For the second setup, With Encryption, we implemented SSL/TLS encryption, which encrypts the communication between the patient's device and the healthcare provider's system. In this case, even though the MITM attacker intercepted the communication, they were unable to read or alter the encrypted data. The encrypted data appeared as gibberish to the attacker, rendering any attempts to modify or inject malicious data ineffective. Furthermore, the blockchain layer ensured that any changes made to the data could be detected and rejected by verifying the data's integrity. The blockchain's immutable ledger made it impossible to alter any data retroactively, guaranteeing that only valid, untampered data could be recorded in the system.

In the Denial of Service (DoS) Attack Evaluation, the focus was on assessing EHRGuard's ability to withstand excessive traffic aimed at overwhelming system resources and denying legitimate users access to patient data. A successful DoS attack could severely disrupt healthcare services by preventing healthcare professionals from accessing critical patient information. EHRGuard implements multiple mitigation techniques, including rate limiting to restrict the number of requests from a single user or device within a set time window and Intrusion Detection Systems (IDS) to monitor and detect abnormal traffic patterns. The experimental results demonstrated the system's resilience: without mitigation, the system was overwhelmed by a flood of requests, causing significant slowdowns and preventing access to patient data, highlighting its vulnerability to DoS attacks. However, with the implemented mitigation strategies, the system performed well under attack—rate limiting prevented any single user from flooding the system, while the IDS detected abnormal traffic, blocked malicious IP addresses, and kept the system operational with minimal downtime, ensuring continuous access to patient data for healthcare professionals. These results confirm that EHRGuard is resilient to DoS attacks when effective mitigation strategies are in place, ensuring the system remains available and functional even during high-traffic events.

In the Sybil Attack Evaluation, the focus was on assessing EHRGuard's ability to prevent malicious actors from creating fake identities or nodes within the network to manipulate the consensus process or alter patient records on the blockchain. A Sybil attack could compromise the integrity of the system by enabling attackers to modify critical medical data. To mitigate such attacks, EHRGuard employs a permissioned blockchain model, where only authorized participants—such as registered hospitals, doctors, and medical institutions—are allowed to join the network. Participants are verified during registration through multi-factor authentication and only verified healthcare professionals are permitted to engage in the consensus mechanism, ensuring that fake nodes cannot interfere with the blockchain. In the experimental results, a Sybil attack was simulated by introducing multiple fake nodes into the network: without mitigation, the fake nodes participated in the consensus process and were able to manipulate the validation of transactions, altering patient records on the blockchain. However, with the mitigation in place, the permissioned nature of the blockchain successfully prevented unauthorized nodes from joining the network, ensuring that only registered and verified participants could validate transactions, which protected patient data from tampering. The results demonstrate that EHRGuard's use of a permissioned blockchain is an effective safeguard against Sybil attacks, preserving the integrity of patient records by restricting network access to authenticated and authorized participants.

In the Replay Attack Evaluation, we assessed EHRGuard's resilience to an attack where an adversary intercepts and retransmits valid communication, such as transaction data, to deceive the system into accepting it as a legitimate request. In the context of healthcare, this could involve an attacker retransmitting valid patient data to manipulate or overwrite medical records. To mitigate this threat, EHRGuard employs timestamping and sequence numbering in all transactions. Each transaction includes a timestamp and a unique sequence number, ensuring that data cannot be replayed without detection. In the experimental results, the system was tested by capturing a valid transaction and retransmitting it to the server: without mitigation, the system accepted the replayed transaction, allowing the attacker to insert false data into the blockchain. However, with mitigation in place, the system recognized the replayed transaction by checking the timestamp and sequence number, promptly rejecting it and preventing unauthorized changes to patient records. The results demonstrate that transaction timestamps and sequence numbers are highly effective in protecting EHRGuard from replay attacks, ensuring that only legitimate transactions are accepted and recorded on the blockchain.

Performance analyses

This section evaluates the proposed EHRGuard system, beginning with an overview of the hardware platform, the "E-health sensor shield V2.0," followed by a visual analysis of the experimental results. The performance of EHRGuard is compared with two other systems, BIoTHR[21] and EHDHE[23], focusing on metrics such as latency, execution time, and throughput. Table 3 provides a summary of the stack technology used in the development of the proposed system.

Dataset

The dataset used for evaluating the EHRGuard model consists of patient vitals collected from IoMT sensors, including heart rate, blood pressure, oxygen levels, and glucose levels, along with associated diagnoses, prescriptions, and blockchain transaction hashes for secure data management. The data is recorded in real-time, enabling continuous patient monitoring and immediate detection of abnormal conditions such as hypertension, diabetes, and critical alerts. If abnormal readings are detected, alerts are triggered for medical intervention, while normal readings are securely stored in an off-chain database, with hashed references recorded on the blockchain to ensure integrity and immutability. Each patient record is linked to a Doctor ID for medical supervision, and prescribed medications are logged securely. This dataset demonstrates EHRGuard's capability to securely manage electronic health records using a combination of IoMT, blockchain, and real-time monitoring, ensuring data privacy, security, and efficient remote healthcare management. Table 4 resumes the dataset used for evaluating the EHRGuard.

Hardware platform

The E-Health Sensor Shield V2.0 is a hardware module specifically designed for Arduino-based projects, particularly those focused on e-health and medical monitoring. It serves as a versatile platform for integrating a wide range of sensors and devices to measure and monitor physiological parameters. The shield features connectors and interfaces for connecting various health sensors, such as those for measuring heart rate, oxygen saturation (SpO2), body temperature, and more, as illustrated in Fig. 5. In the proposed system, four types of health sensors are connected to the patient's body: a temperature sensor, a SpO2 sensor, a pulse rate sensor, and an EMG sensor. The shield enables the collection of real-time data from these sensors, which can then be processed and used to monitor an individual's health parameters. It supports both analog and digital connectivity, making it compatible with sensors of different output types. Additionally, the shield offers flexible power options, allowing users to configure power supply for both the sensors and the shield according to their project needs. In this system, a Raspberry Pi equipped with the E-Health Sensor Shield V2.0 functions as an IoT gateway, routing vital-sign data to a healthcare IoT server. The e-health sensor platform also provides an open-

Segment name	Component	Description
Healthcare medical blockchain network	CPU	Intel® Core™ i5-8250U CPU @1.80 GHz
	Operating System	Ubuntu 17.04
	IDE	Python and Django
	Programming Language	Python and Django, JavaScript
	Database	SQLite
	Memory	16GB
Healthcare IoT Server	Hardware	Intel® Core™ i5-8250U CPU @1.80 GHz
	Server	CoAP Server
	Library/Framework	Californium CoAP, Http URL Connection
	Programming Language	Python
	Operating System	Ubuntu Linux 18.04 LTS
Gateway	Hardware	Raspberry pi OS
	Server	Arduino Uno
	Libraries Used/Framework	HTTP URL Connection
Web application	Operating System	Windows 10
	Browser	Internet Explorer, Firefox, Chrome, Firefox
	Programming Language	HTML, CSS, JavaScript, Node.js
	Libraries Used/Framework	Notify.js, Californium CoAP, JQuery, Bootstrap
Off-chain database	Server	SQLite
	Operating System	Windows 10

Table 3. Development of the environment for the proposed system.

Patient ID	Timestamp	Heart rate (BPM)	Blood pressure (mmHg)	Oxygen level (%)	Glucose level (mg/dL)	Doctor ID	Diagnosis	Prescription	Blockchain hash
P001	2025-02-25 08:00	78	120/80	98	110	D001	Hypertension	MedA 50 mg	a1b2c3d4e5
P002	2025-02-25 08:05	85	130/85	96	140	D002	Diabetes type 2	MedB 10 mg	f6g7h8i9j0
P003	2025-02-25 08:10	92	125/78	99	100	D003	Normal	None	k1l2m3n4o5
P004	2025-02-25 08:15	72	118/75	97	95	D004	Normal	None	p6q7r8s9t0
P005	2025-02-25 08:20	100	145/90	94	180	D005	Diabetes type 1	Insulin 5u	u1v2w3 × 4y5
P006	2025-02-25 08:25	110	160/100	93	200	D006	Critical alert	Emergency Care	z6a7b8c9d0
P007	2025-02-25 08:30	90	132/82	98	105	D007	Normal	None	e1f2g3h4i5
P008	2025-02-25 08:35	65	110/70	97	90	D008	Low BP	MedC 20 mg	j6k7l8m9n0
P009	2025-02-25 08:40	88	135/88	95	130	D009	Hypertension	MedD 25 mg	o1p2q3r4s5
P010	2025-02-25 08:45	102	140/85	96	115	D010	Normal	None	t6u7v8w9 × 0
P011	2025-02-25 08:50	74	122/78	99	105	D011	Normal	None	y1z2a3b4c5
P012	2025-02-25 08:55	95	128/80	97	140	D012	Pre-diabetes	MedE 15 mg	d6e7f8g9h0
P013	2025-02-25 09:00	80	118/76	99	100	D013	Normal	None	i1j2k3l4m5
P014	2025-02-25 09:05	115	165/110	92	210	D014	Critical alert	Emergency Care	n6o7p8q9r0
P015	2025-02-25 09:10	98	140/90	95	130	D015	Hypertension	MedF 30 mg	s1t2u3v4w5
P016	2025-02-25 09:15	75	120/80	99	90	D016	Normal	None	x6y7z8a9b0
P017	2025-02-25 09:20	85	130/85	96	145	D017	Pre-diabetes	MedG 20 mg	c1d2e3f4g5
P018	2025-02-25 09:25	92	126/79	98	100	D018	Normal	None	h6i7j8k9l0
P019	2025-02-25 09:30	100	150/95	95	165	D019	Hypertension	MedH 40 mg	m1n2o3p4q5
P020	2025-02-25 09:35	110	160/105	92	220	D020	Critical alert	Emergency Care	r6s7t8u9v0

Table 4. IoMT patient data for EHRguard.

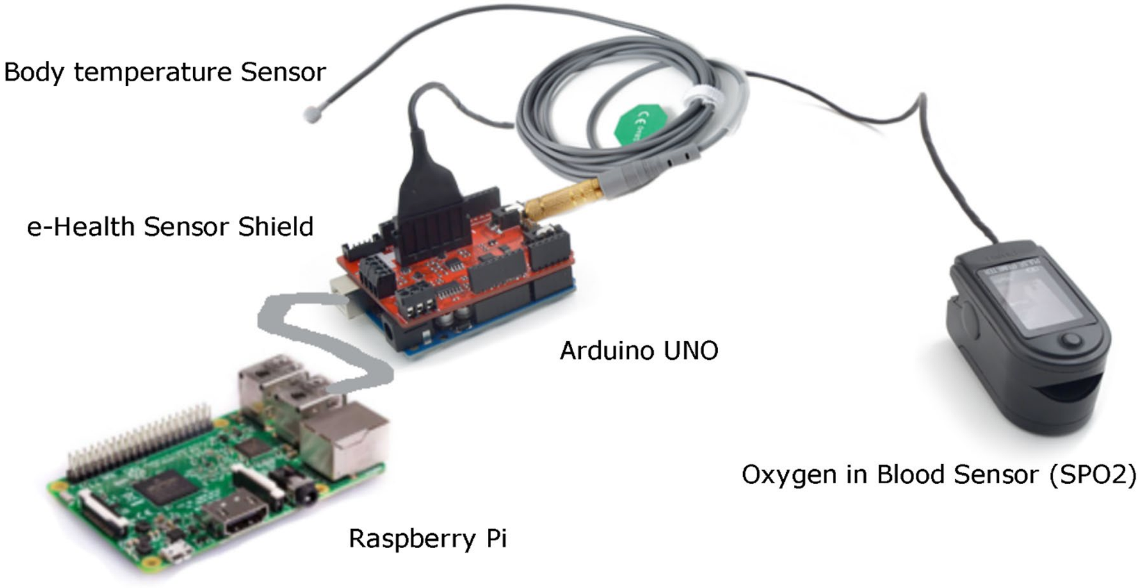


Fig. 5. E-health sensor shield V2.0.

source C++library for reading data from the sensors. For detailed information on using the shield, users should consult the manufacturer's product documentation and specifications[33].

Throughput

Evaluating the throughput of the proposed system using JMeter is essential for assessing its performance under varying loads. Throughput, measured in KB/sec, indicates the system's efficiency in handling user requests and data transfer rates. Figure 6 compares the throughput of our proposed system with BIoTHR and EHDHE, demonstrating a significant improvement in throughput rate. This enhancement highlights the system's superior capability in facilitating faster and more efficient data transmission, which directly contributes to improved

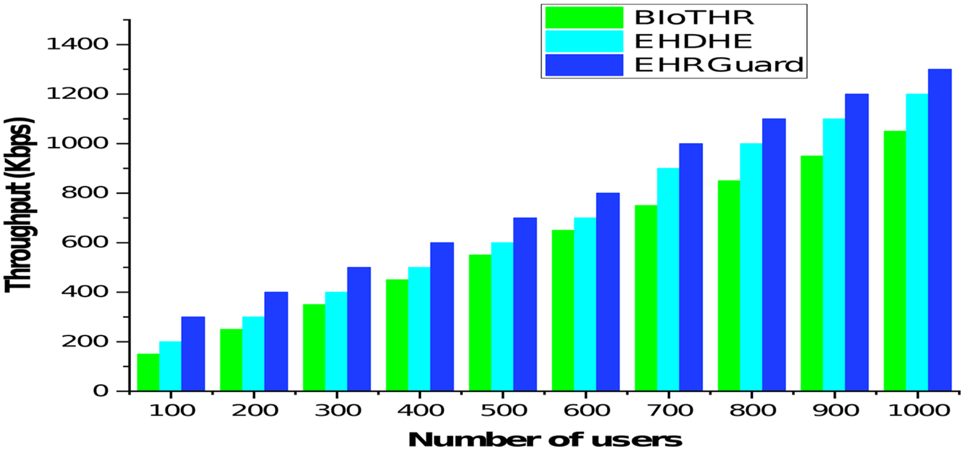


Fig. 6. Throughput of the proposed framework.

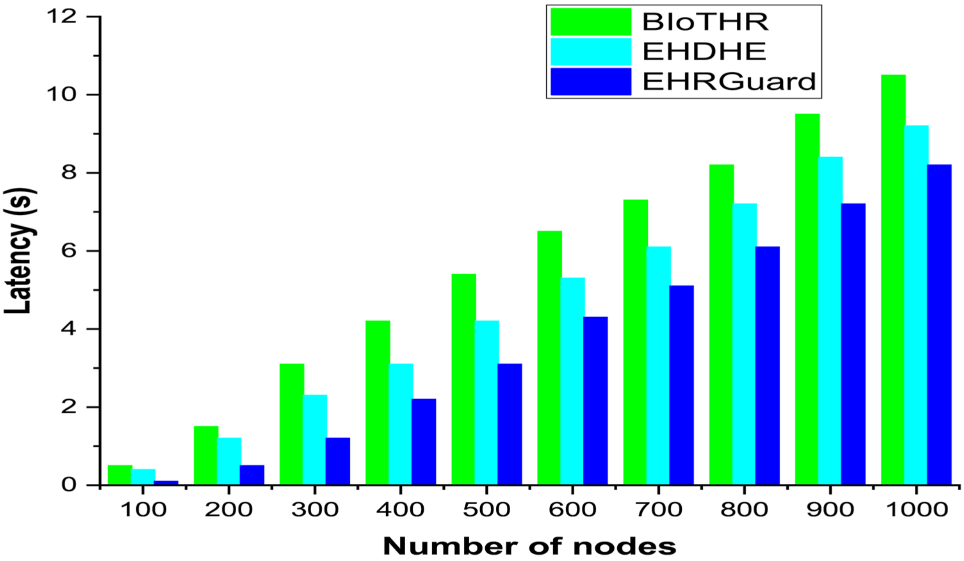


Fig. 7. Latency of the proposed system.

overall system performance and a better user experience. The results validate the effectiveness of the proposed system in managing high data loads and ensuring seamless operation in real-world healthcare scenarios.

Latency of the proposed system

In the proposed EHRGuard system, latency is a critical factor, especially in healthcare environments where timely access to patient records is essential for effective patient care. The system's latency is influenced by several factors, including network latency, consensus mechanisms, block size, and transaction throughput. To evaluate the system's performance, we measured the average latency using JMeter, a widely-used tool for performance testing. During the evaluation, we simulated varying numbers of users and measured latency in seconds. The results, illustrated in Fig. 7, compare the latency performance of our system with benchmark models such as BIoTHR and EHDHE. The proposed framework demonstrates significantly lower latency compared to these benchmarks, highlighting its efficiency and robustness. This reduction in latency ensures faster and more reliable access to patient records, enhancing the system's overall effectiveness and supporting timely decision-making in healthcare settings.

Computation cost

The computation cost, which reflects the resources required to execute tasks within a system or algorithm, is a critical factor in evaluating the efficiency of our proposed EHRGuard system. It encompasses various components, including user authentication, data retrieval, sensor data processing, blockchain integration, and data storage. Through extensive experimentation, our EHRGuard model has demonstrated superior cost-efficiency compared to benchmark systems like BIoTHR and EHDHE. As illustrated in Fig. 8, EHRGuard

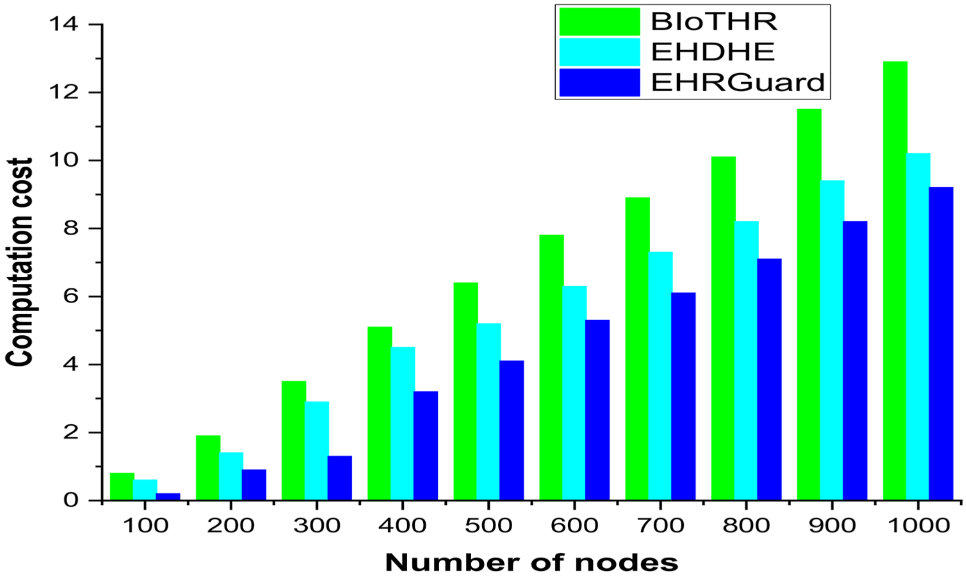


Fig. 8. Computation cost of the proposed system.

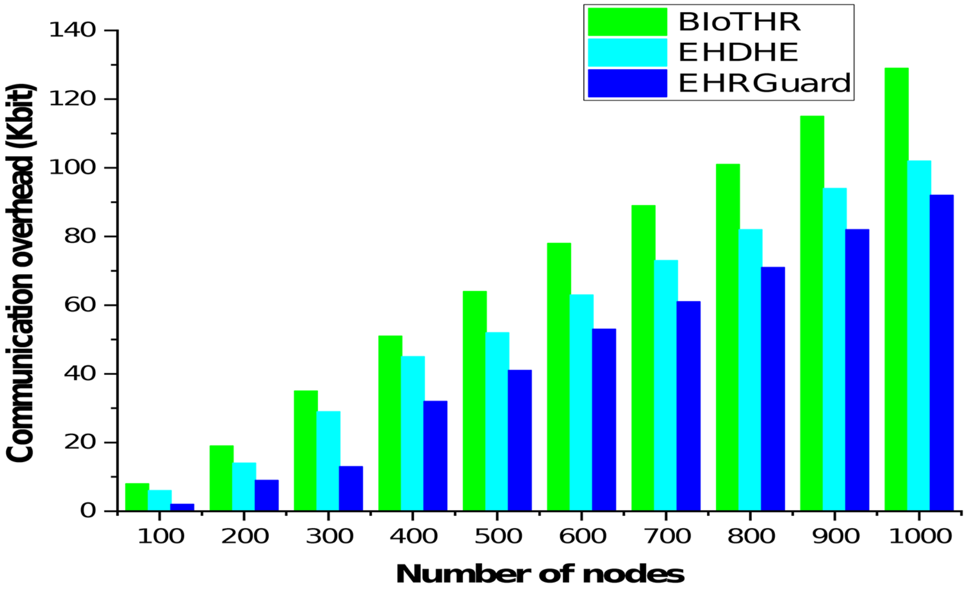


Fig. 9. The communication overhead of the proposed system.

achieves a total computation cost of approximately 7 s for 1000 smart nodes, representing a 38% reduction compared to BIoTHR and a 24% reduction compared to EHDHE. These results highlight EHRGuard's ability to significantly minimize computation costs while maintaining scalability, ensuring efficient resource utilization and enhanced performance in healthcare applications. This cost-effectiveness makes EHRGuard a robust and practical solution for real-world implementation.

Communication overhead

Communication overhead, which refers to the additional resources and latency incurred by a system due to communication-related activities such as data transmission, messaging, and transactions between components or nodes within a blockchain network, is a critical factor in system performance. In our analysis, as depicted in Fig. 9, the proposed scheme demonstrates significantly greater efficiency in managing communication overhead compared to BIoTHR and EHDHE. This improved efficiency indicates that our system utilizes communication resources more effectively, reducing unnecessary delays and optimizing resource allocation. By minimizing communication overhead, the proposed system enhances overall performance, ensuring smoother and more reliable operations within the blockchain network, particularly in healthcare applications where timely and efficient data exchange is paramount.

Computational time analysis

In this section, we analyze the computational efficiency of the EHRGuard system by evaluating the time required for key operations involved in managing patient health data. The analysis focuses on four core processes: data encryption, blockchain transaction processing, consensus mechanism execution (Proof of Work), and real-time alert generation. Given the critical nature of healthcare applications, ensuring both security and performance is paramount for the system's feasibility in real-world settings. We define the following parameters for measuring the computational time of each operation:

- T_enc: Data encryption is performed to ensure that patient health records are securely stored and transmitted. The time required for encryption can be calculated as:

$$T_{enc} = \frac{\sum{}_{i=1}^{n} T_{enc,i}}{n}$$

Where:
$T_{enc,i}$: is the time for encrypting the iii-th patient's data.
n: is the total number of patients.

- T_tx: The processing of a blockchain transaction involves creating a new block, hashing, and appending it to the blockchain. The computational time for blockchain transactions is given by:

$T_{tx} = T_{block\_creation} + T_{hashing} + T_{block\_append}$
Where:
$T_{block\_creation}$: is the time to create the new block.
$T_{hashing}$: is the time taken to generate the hash of the block.
T_{block_append}: is the time to append the block to the blockchain.

- T_pow: The Proof of Work mechanism ensures the integrity of the blockchain by requiring nodes to solve a computational puzzle before adding a block. The time for consensus mechanism execution can be represented as:

$$T_{pow} = \frac{T_{solve}}{N}$$

Where:
T_{solve}: is the time to solve the computational puzzle.
N: is the number of nodes in the blockchain network.

- T_alert: When sensor data falls outside the predefined thresholds (e.g., abnormal heart rate or blood pressure), real-time alerts are generated for healthcare professionals. The time for alert generation is calculated as:

$$T_{alert} = \frac{T_{detection} + T_{notification}}{2}$$

Where:
$T_{detection}$: is the time taken to detect abnormal readings from the sensor data.
$T_{notification}$: is the time taken to notify healthcare professionals via the alert system.

- T_db: To ensure the system can retrieve patient data efficiently for analysis or monitoring, the time for fetching patient records from the off-chain database is evaluated:

$$T_{db} = \frac{\sum{}_{i=1}^{n} T_{db,i}}{n}$$

Where:
$T_{db,i}$: is the time to retrieve the *i*-th patient's data from the database.

Table 5 presents the computational time analysis of key operations in the EHRGuard system, showcasing its efficiency in managing patient health data. The data encryption operation takes an average of 150 ms, ensuring fast and secure handling of patient information. Blockchain transaction processing requires 250 ms on average, reflecting the time needed to create, hash, and store a new block in the blockchain for maintaining data integrity. The Proof of Work (PoW) consensus mechanism, essential for blockchain security, averages 500 ms, introducing some latency due to its computational complexity. Real-time alert generation for abnormal sensor readings takes just 80 ms on average, ensuring timely notifications for healthcare professionals. Lastly, data retrieval from the off-chain database averages 60 ms, enabling quick access to patient records. Overall, the system demonstrates efficient performance, balancing security, real-time monitoring, and data integrity with minimal delays, making EHRGuard suitable for real-time healthcare applications.

Operation	Average time (ms)	Maximum time (ms)	Minimum time (ms)	Description
Data encryption	150	200	120	Time taken to encrypt patient health data before storage in the database.
Blockchain transaction Processing	250	350	200	Time required for creating a new block, hashing, and recording in the blockchain.
Consensus mechanism (PoW)	500	600	450	Time taken for the network nodes to solve the computational puzzle in the Proof of Work mechanism.
Real-time alert generation	80	120	60	Time required to detect abnormal sensor readings and send alerts to healthcare professionals.
Data retrieval from off-chain database	60	100	50	Time to fetch patient data from the off-chain database for review or analysis.

Table 5. Computational time for key operations in EHRguard.

References	A	B	C	D	E	F	G	H	I	J	K	L	M
[19]	High	N	N	Y	Y	N	High	Y	Y	Y	N	Y	High
[20]	Low	Y	N	Y	Y	Y	Medium	Y	N	Y	Y	Y	Medium
[21]	High	Y	Y	Y	Y	Y	High	Y	Y	Y	N	Y	Medium
[22]	High	Y	Y	Y	Y	Y	High	Y	Y	Y	N	N	Medium
[23]	Medium	N	Y	N	Y	Y	Medium	Y	Y	N	Y	Y	High
[24]	High	Y	N	Y	Y	N	High	N	Y	N	Y	N	High
[25]	Medium	Y	N	Y	N	Y	High	Y	N	Y	N	Y	Medium
[26]	High	N	Y	N	Y	N	High	Y	N	Y	N	Y	Medium
EHRGuard	High	Y	Y	Y	Y	Y	Low	Y	Y	Y	Y	Y	Low

Table 6. Comparative evaluation of the designed system with the other existing methods. *A* immutability, *B* access control, *C* use of sensors, *D* integrity, *E* confidentiality, *F* service reliability, *G* communication overhead, *H* availability, *I* privacy, *J* traceability, *K* scalability, *L* Interoperability, *M* cost, *Y* present, *N* not present.

Comparative analysis

The comparison of the proposed EHRGuard system with existing systems is summarized in Table 6, underscores its superiority in addressing crucial parameters related to privacy, security, and overall functionality. This comprehensive evaluation reveals significant advancements and performance enhancements over current systems, solidifying the proposed method as a robust solution for modern healthcare challenges. The key parameters considered in the comparison include immutability, access control, and use of sensors, integrity, availability, confidentiality, privacy, traceability, scalability, service reliability, communication overhead, interoperability, and cost. The proposed EHRGuard system excels in these aspects, demonstrating its capacity to meet and exceed the expectations set by current systems. The system's immutability ensures the integrity and permanence of health records, mitigating the risk of unauthorized alterations. Robust access control mechanisms guarantee that only authorized individuals have appropriate levels of data access, bolstering confidentiality and privacy. The incorporation of sensors enhances the system's capabilities for remote patient monitoring, facilitating proactive healthcare interventions. Moreover, the system exhibits high availability, ensuring uninterrupted access to critical healthcare data. Privacy and confidentiality are prioritized, addressing concerns associated with the sensitive nature of health information. Traceability features enable a transparent audit trail, fostering accountability and compliance. The system's scalability ensures adaptability to varying demands, while its reliability in service delivery instills confidence in users. Notably, the proposed system minimizes communication overhead, promoting efficient data exchange. Interoperability considerations allow seamless integration with existing healthcare infrastructures, fostering a cohesive healthcare ecosystem. Finally, the cost-effectiveness of the proposed system positions it as a practical and sustainable solution for healthcare institutions. In conclusion, the experimental results and functionalities showcased by the proposed EHRGuard system substantiate its capacity to not only address but surpass the privacy and security constraints present in current systems. The innovative approach of remotely monitoring patients while securely sharing healthcare data marks a significant advancement, aligning with the evolving landscape of modern healthcare practices. The proposed method emerges as a pioneering solution, poised to elevate the standards of healthcare data management and patient care.

Use cases and real-time applications of the EHRguard system

The EHRGuard system plays a pivotal role in transforming healthcare delivery by leveraging the integration of IoMT sensors, blockchain technology, and off-chain databases. One of the primary applications of this system is in remote patient monitoring, especially for patients with chronic conditions like diabetes, hypertension, or heart disease. For instance, a diabetic patient is equipped with continuous glucose monitoring sensors that track glucose levels in real time. These readings are transmitted wirelessly to a Raspberry Pi gateway, which forwards the data to the EHRGuard system. The system analyzes the data, and if an abnormal spike or drop in glucose levels is detected, a real-time alert is sent to the patient's healthcare provider, ensuring timely intervention and preventing severe complications. In the case of heart disease management, patients are equipped with heart rate monitors, and any irregularity in heart rate, detected by the sensors, triggers an automatic alert for immediate medical attention.

In emergency medical scenarios, the EHRGuard system facilitates swift decision-making and action. For example, a patient arriving at an emergency room (ER) with chest pain could have their vitals continuously monitored through IoMT devices, and their health data, including medical history and past diagnoses, is immediately available to the ER team. This enables healthcare providers to make quick, well-informed decisions about the necessary treatment plan. If the patient's readings indicate signs of a potential heart attack or other critical condition, the system generates alerts that notify the attending physicians and nurses in real-time, streamlining the emergency response and improving patient outcomes. The data recorded from this interaction is also securely stored on the blockchain, creating a transparent and tamper-proof record of the patient's treatment during the emergency.

Telemedicine consultations also benefit from the capabilities of EHRGuard. For instance, a patient consulting with a physician remotely could share their health data through the system. The doctor, with secure access to the patient's medical records and real-time sensor data (e.g., blood pressure, heart rate, oxygen levels), can make a comprehensive diagnosis even without an in-person visit. If the patient's health data shows abnormal readings, the system automatically flags these for the physician's attention. This capability enhances the accuracy and safety of remote healthcare, especially for patients in rural or underserved areas.

The system also plays a critical role in medication adherence monitoring. For example, a patient prescribed medication for hypertension may forget to take their medicine or may not follow the recommended schedule. With IoMT-enabled devices like blood pressure monitors, EHRGuard tracks the patient's readings over time and can automatically detect patterns that suggest non-adherence to the prescribed medication regimen. The system will notify the healthcare provider, who can then intervene by advising the patient or adjusting the prescription if necessary. This proactive approach ensures better treatment compliance and improved patient outcomes.

In medical research, EHRGuard supports the collection of anonymized health data for studies by securely storing and recording patient information in a blockchain ledger. Researchers can access this data, ensuring it remains authentic and tamper-proof. For example, researchers studying the effectiveness of a new drug can track and analyze data from a large number of patients participating in clinical trials. The blockchain ensures that the integrity of the data is preserved, and the anonymization of sensitive patient information ensures privacy. Additionally, the system's flexibility allows researchers to aggregate data across multiple hospitals and clinics, making it possible to conduct large-scale studies without compromising data security or patient privacy.

Emergency response systems are another important area where EHRGuard proves useful. Suppose an elderly patient with a history of respiratory conditions experiences difficulty breathing while at home. The system, continuously monitoring the patient's vital signs, detects the change in oxygen levels and immediately sends an alert to emergency responders and the patient's primary care provider. This allows for quick intervention and reduces the chances of the situation escalating into a medical emergency.

Finally, the patient consent and data privacy management feature of EHRGuard allows patients to control their health data. Before any health record is added to the system, patients must give explicit consent, which is stored on the blockchain, ensuring that any subsequent access or modification of their data is logged and can be reviewed for transparency. This is especially crucial for telemedicine, where patients need confidence that their data is protected, and that they have control over who can access it.

Through these real-time applications, EHRGuard not only improves the quality of healthcare but also ensures that patient data remains secure, transparent, and accessible only to authorized individuals. The integration of IoMT devices, blockchain, and off-chain databases allows the system to bridge the gap between secure data management and effective patient care, offering a comprehensive solution for modern healthcare challenges.

Scalability analysis for EHRguard in large-scale medical environments

The scalability of the EHRGuard system is essential for its successful implementation in a global healthcare network where multiple devices and users generate large volumes of data. To ensure the system performs efficiently, even with a massive surge in users and devices, several strategies have been incorporated into the system design. These strategies focus on maintaining high performance, low latency, and system stability while supporting large-scale deployments in real-time healthcare applications.

Load balancing and distributed architecture

In large-scale environments, load balancing becomes essential to prevent bottlenecks and ensure that the system can handle a large influx of data without compromising its responsiveness. EHRGuard employs a distributed architecture that is designed to scale horizontally across multiple servers. Load balancing techniques are utilized to distribute the computational and storage load evenly across the network, reducing the risk of overloading individual nodes and ensuring that the system continues to provide fast, responsive access to patient data. In this distributed setup, multiple healthcare institutions, hospitals, and even individual practitioners can connect to the system simultaneously. The decentralized approach of the permissioned blockchain further enhances this architecture by enabling a distributed consensus mechanism. Blockchain nodes, including full nodes in hospitals and light nodes on mobile devices, participate in the consensus process to validate transactions and maintain the integrity of the data, ensuring the system scales with the increasing number of devices and healthcare providers.

Hybrid blockchain-off-chain storage model

One of the key components of EHRGuard's scalability lies in the hybrid storage model that combines both blockchain and off-chain databases. Blockchain provides the secure, tamper-resistant storage of critical transaction data, such as patient health records and sensor readings. However, storing large volumes of raw sensor data on the blockchain is inefficient and costly. Therefore, a hybrid approach is employed where high-volume data, such as IoMT sensor data and medical imaging, are stored in off-chain databases, while only the essential hashes, metadata, and transaction logs are recorded on the blockchain. The off-chain database can scale independently from the blockchain, allowing for rapid data retrieval and efficient management of large data sets without overwhelming the blockchain's storage capacity. With this architecture, as the number of devices and sensors increases, the off-chain database can expand dynamically to accommodate the surge in data, ensuring that the performance of the overall system remains unaffected.

Edge computing and cloud integration

To further enhance scalability and reduce latency, EHRGuard integrates edge computing with cloud storage solutions. Edge computing nodes are strategically placed closer to the devices, such as IoMT sensors, allowing for real-time data processing at the edge. This approach reduces the amount of raw data that needs to be transmitted to the central server or cloud, minimizing network congestion and speeding up decision-making for healthcare providers. Additionally, real-time sensor data analysis can be performed locally, triggering alerts, when necessary, thus improving the overall responsiveness of the system. Cloud computing complements edge computing by providing scalable storage and computational resources. As the volume of data generated by patients and healthcare devices increases, the system can seamlessly scale by utilizing cloud infrastructure to store and process large amounts of data. The cloud platform can accommodate the growing data storage needs while ensuring that the performance of the system is not compromised.

Distributed consensus and blockchain network scaling

As the number of devices and users increases, ensuring that the blockchain network remains scalable is vital. EHRGuard leverages a permissioned blockchain, where only authorized participants are allowed to validate transactions and participate in the consensus process. This mechanism improves performance compared to public blockchains, as the number of nodes in the network is restricted to trusted parties, reducing the computational load. To further enhance scalability, EHRGuard uses an optimized consensus algorithm tailored for healthcare applications. This algorithm reduces the time required for transaction validation, ensuring that the system can handle a high transaction throughput while maintaining the integrity and immutability of the data. By using a lightweight, permissioned blockchain, the system ensures that even as the network grows, the consensus process remains efficient and the blockchain's storage and processing requirements are kept within practical limits.

Dynamic resource allocation and cloud-based elasticity

The dynamic nature of healthcare systems, where the number of connected devices and users fluctuates, requires dynamic resource allocation. EHRGuard leverages cloud-based elasticity to scale the system's resources up or down based on demand. For instance, during periods of high activity, such as large-scale health emergencies or seasonal healthcare needs, the cloud infrastructure automatically allocates more computational power and storage capacity to handle the increased load. Similarly, during low-traffic periods, the system can scale down resources, optimizing costs and maintaining system efficiency. This dynamic resource allocation ensures that EHRGuard is able to accommodate fluctuations in healthcare demand, ensuring the system is both cost-effective and responsive to real-time needs.

Optimized data validation and storage protocols

As the number of devices and users grows, it becomes increasingly important to optimize data validation and storage protocols. EHRGuard uses efficient hashing algorithms and data compression techniques to minimize the data footprint on the blockchain. This ensures that the blockchain does not become bloated as more transactions are recorded. The validation process is optimized to ensure that only necessary data is included on the blockchain, while larger datasets are stored off-chain, making the system more scalable. In addition, the use of sharding techniques in the blockchain network allows for parallel processing of transactions, reducing bottlenecks and improving the speed and efficiency of the consensus mechanism. By partitioning the blockchain network into smaller, manageable units, sharding enhances the system's ability to scale horizontally while maintaining high levels of security.

Fault tolerance and high availability

Scalability is not just about handling larger amounts of data and more users; it also involves ensuring system reliability in the face of potential failures. EHRGuard incorporates fault-tolerant mechanisms and high-availability strategies to ensure the system remains operational even if certain components fail. Redundant nodes, automated failover systems, and real-time monitoring tools are in place to ensure that if a node or server becomes unavailable, data can still be accessed from another node without disruption. The decentralized nature of the blockchain network further strengthens fault tolerance, as data is not stored in a single location, and every participating node maintains a copy of the blockchain. This ensures that even in the event of network partitioning or server downtime, the system remains operational, and that patient data is always accessible.

Conclusions

In conclusion, the integration of blockchain technology into Electronic Health Records (EHRs) for smart hospitals represents a transformative advancement in addressing the critical challenges of privacy and security in healthcare data management. Traditional EHR systems, with their inherent vulnerabilities and risks, have necessitated the exploration of innovative solutions, and blockchain technology has emerged as a powerful tool in this domain. By leveraging blockchain's core principles of decentralization, immutability, transparency, and consensus, the proposed system provides a robust framework for securing sensitive health information. Cryptographic techniques and smart contracts further enhance the system by enabling secure storage, retrieval, and granular access control, effectively preventing unauthorized data manipulation or access. The fusion of blockchain and EHRs marks a paradigm shift toward a more patient-centric, interoperable, and secure healthcare ecosystem. Patients gain greater control over their health data, assured by the tamper-resistant and transparent nature of blockchain-ledger storage. Healthcare providers benefit from streamlined data sharing, which improves care coordination and supports more informed decision-making. Case studies and real-world use cases highlight the practical successes of blockchain in healthcare, demonstrating its effectiveness in mitigating data breaches, enhancing interoperability, and ensuring compliance with privacy regulations. However, challenges such as scalability, regulatory compliance, and the need for standardized frameworks remain. Addressing these challenges requires a collaborative effort from stakeholders, including healthcare providers, technology developers, and policymakers, to establish guidelines and standards that facilitate the seamless integration of blockchain into healthcare infrastructures. Despite these hurdles, the potential of blockchain to revolutionize healthcare data management is undeniable, paving the way for a more secure, efficient, and patient-focused future in healthcare.

Data availability

The datasets used during the current study are available from the corresponding author on reasonable request.

Received: 11 February 2025; Accepted: 21 March 2025
Published online: 10 April 2025

References

1. Deepa, V. V. et al. Smart embedded health monitoring system and secure electronic health record (EHR) transactions using blockchain technology. *Soft Comput.* **27**, 12741–12756. https://doi.org/10.1007/s00500-023-08893-4 (2023).
2. Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V. & Kim, S. W. The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. *IEEE Commun. Surveys Tutor.* **22**, 1121–1167. https://doi.org/10.1109/COMST.2020.2973314 (2020).
3. Liu, Q., Mkongwa, K. G. & Zhang, C. Performance issues in wireless body area networks for the healthcare application: a survey and future prospects. *SN Appl. Sci.* **3**, 155. https://doi.org/10.1007/s42452-020-04058-2 (2021).
4. Leila, E., Othman, S. B. & Sakli, H. An Internet of Robotic Things System for combating coronavirus disease pandemic (COVID-19). *2020 20th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*. Monastir, Tunisia, 333–337. https://doi.org/10.1109/STA50679.2020.9329310 (2020).
5. Nagpal, D. et al. Automatic detection of diabetic hypertensive retinopathy in fundus images using transfer learning. *Appl. Sci.* **13**, 4695. https://doi.org/10.3390/app13084695 (2023).
6. Mukherjee, A. et al. Internet of health things (IoHT) for personalized health care using integrated edge-fog-cloud network. *J. Ambient Intell. Hum. Comput.* **12**, 943–959. https://doi.org/10.1007/s12652-020-02113-9 (2021).
7. Khan, M. A., Quasim, M. T., Alghamdi, N. S. & Khan, M. Y. A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data. *IEEE Access.* **8**, 52018–52027. https://doi.org/10.1109/ACCESS.2020.2980739 (2020).
8. Faris, A., Almalki, B. O. & Soufiene EPPDA: An Efficient and Privacy-Preserving Data Aggregation Scheme with Authentication and Authorization for IoT-Based Healthcare Applications. *Wirel. Commun. Mob. Comput.* **5594159**, 18. https://doi.org/10.1155/2021/5594159 (2021).
9. Othman, S. B., Bahattab, A. A., Trad, A. & Youssef, H. LSDA: Lightweight Secure Data Aggregation Scheme in Healthcare using IoT. *10th International Conference on Information Systems and Technologies*. Lecce, Italy, Tunisia. https://doi.org/10.1145/3447568.3448530 (2019).
10. Tao, F., Wang, X. & Liu, C. Secure data collaborative computing scheme based on blockchain. *Secur. Commun. Netw.* **6630291**, 9. https://doi.org/10.1155/2021/6630291 (2021).
11. Qin, C. et al. and Effective Construction Scheme for Blockchain Networks. *Secur. Commun. Netw.* **8881881**, 20. https://doi.org/10.1155/2020/8881881 (2020).
12. Othman, S. B. et al. Confidentiality and integrity for data aggregation in WSN using homomorphic encryption. *Wirel. Pers. Commun.* **80**, 867–889. https://doi.org/10.1007/s11277-014-2061-z (2015).
13. Chinnasamy, P. et al. Smart Contract-Enabled secure sharing of health data for a mobile Cloud-Based E-Health system. *Appl. Sci.* **13** (6), 3970. https://doi.org/10.3390/app13063970 (2023).
14. Chinnasamy, P. & Deepalakshmi, P. HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. *J. Ambient Intell. Hum. Comput.* **13**, 1001–1019. https://doi.org/10.1007/s12652-021-02942-2 (2022).
15. Chinnasamy, P. et al. Integrating intelligent breach detection system into 6 g enabled smart Grid-Based cyber physical systems. *Wirel. Pers. Commun.* https://doi.org/10.1007/s11277-024-11192-2 (2024).
16. Zhao, R., Zhou, A. & Article Kezhi Mao. Automatic detection of cyberbullying on social networks based on bullying features. In *Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN '16)*. Association for Computing Machinery. New York, NY, USA, 1–6. https://doi.org/10.1145/2833312.2849567 (2016).
17. Guo, C., Tian, P. & Choo, K. K. R. Enabling Privacy-Assured Fog-Based data aggregation in E-Healthcare systems. in *IEEE Trans. Industr. Inf.*, **17**, 1948–1957. https://doi.org/10.1109/TII.2020.2995228 (2021).
18. Soufiene Ben Othman, A. A., Bahattab, A., Trad & Youssef, H. RESDA: Robust and Efficient Secure Data Aggregation Scheme in Healthcare using the IoT. *International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*. Tunis, Tunisia, 209–213. https://doi.org/10.1109/IINTEC48298.2019.9112125 (2019).
19. Jamil, F., Ahmad, S., Iqbal, N. & Kim, D. H. Towards a remote monitoring of patient vital signs based on IoT-Based blockchain integrity management platforms in smart hospitals. *Sensors* **20**, 2195. https://doi.org/10.3390/s20082195 (2020).
20. Abou-Nassar, E. M. et al. DITrust chain: towards blockchain-based trustmodels for sustainable healthcare IoT systems. *IEEE Access.* **8**, 111223–111238. https://doi.org/10.1109/ACCESS.2020.2999468 (2020).
21. Ray, P. P., Chowhan, B., Kumar, N. & Almogren, A. BIoTHR: electronic health record servicing scheme in IoT-blockchain ecosystem. *IEEE Internet Things J.* **4662**, 1–10872. https://doi.org/10.1109/jiot.2021.3050703 (2021).
22. Samuel, O. et al. An anonymous IoT-based E-health monitoring system using blockchain technology. *IEEE Syst. J.* **17**, 1–12. https://doi.org/10.1109/JSYST.2022.3170406 (2022).
23. Pratima Sharma, S., Namasudra, R. G., Crespo, J., Parra-Fuente, M. C. & Trivedi, E. H. D. H. E. Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Inf. Sci.* **629**, 703–718. https://doi.org/10.1016/j.ins.2023.01.148 (2023).

24. Sezer, B. B., Turkmen, H. & Nuriyev, U. PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks. *Internet Things*. **22**, 2542–6605. https://doi.org/10.1016/j.iot.2023.100781 (2023).
25. Gohar, A. N., Abdelmawgoud, S. A. & Farhan, M. S. A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. *IEEE Access.* **10** (September), 92137–92157. https://doi.org/10.1109/ACCESS.2022.3202902 (2022).
26. Nguyen, D. C., Pathirana, P. N., Ding, M. & Seneviratne, A. BEdgeHealth: a decentralized architecture for edge-based IoMT networks using blockchain. *IEEE Internet Things J.* **8** (14), 11743–11757. https://doi.org/10.1109/JIOT.2021.3058953 (2021).
27. Vittorio Capocasale, D., Gotta, G. & Perboli Comparative analysis of permissioned blockchain frameworks for industrial applications. *Blockchain Res. Appl.* **4** (1), 100113. https://doi.org/10.1016/j.bcra.2022.100113 (2023).
28. Tsang, Y. P. et al. On-Chain and Off-Chain data management for Blockchain-Internet of things: A Multi-Agent deep reinforcement learning approach. *J. Grid Comput.* **22**, 16. https://doi.org/10.1007/s10723-023-09739-x (2024).
29. Yongjun Ren, Z., Lv, N. N., Xiong & Jin Wang HCNCT: A Cross-chain interaction scheme for the Blockchain-based metaverse. *ACM Trans. Multimedia Comput. Commun. Appl.* **20**, 23. https://doi.org/10.1145/3594542 (2024).
30. Ren, Y. et al. Multiple cloud storage mechanism based on blockchain in smart homes. *Future Generation Comput. Syst.* **115**, 304–313. https://doi.org/10.1016/j.future.2020.09.019 (2021).
31. Ren, Y. J., Leng, Y., Cheng, Y. P. & Wang, J. Secure data storage based on blockchain and coding in edge computing. *Math. Biosci. Eng.* **16**(4):1874–1892.https://doi.org/10.3934/mbe.2019091. (2019).
32. Moritz Wendl, M. H., Doan, R., Sassen & Part, A. The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. *J. Environ. Manag.* **326**, 0301–4797. https://doi.org/10.1016/j.jenvman.2022.116530. (2023).
33. Sahraoui, H. et al. Design and implementation of a medical platform for real-time and remote ECG monitoring using digimesh wireless sensor network technology. *Res. Biomed. Eng.* **39**, 959–976. https://doi.org/10.1007/s42600-023-00319- (2023).

Acknowledgments

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. 251202].

Author contributions

All authors contributed equally to the conceptualization, formal analysis, investigation, methodology, and writing and editing of the original draft. All authors have read and agreed to the published version of the manuscript.

Funding

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU251202].

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to S.B.O. or M.G.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.