scientific reports

Check for updates

OPEN

Opportunistic access control scheme for enhancing IoT-enabled healthcare security using blockchain and machine learning

Mohd Anjum[1], Naoufel Kraiem[2], Hong Min[3]✉, Ashit Kumar Dutta[4], Yousef Ibrahim Daradkeh[5] & Sana Shahab[6]

The healthcare industry, aided by technology, leverages the Internet of Things (IoT) paradigm to offer patient/user-related services that are ubiquitous and personalized. The authorized repository stores ubiquitous data for which access-level securities are granted. These security measures ensure that only authorized entities can access patient/user health information, preventing unauthorized entries and data downloads. However, recent sophisticated security and privacy attacks such as data breaches, data integrity issues, and data collusion have raised concerns in the healthcare industry. As healthcare data grows, conventional solutions often fail due to scalability concerns, causing inefficiencies and delays. This is especially true for multi-key authentication. Dependence on conventional access control systems leads to security flaws and authorization errors caused by static user behaviour models. This article introduces an Opportunistic Access Control Scheme (OACS) for leveraging access-level security. This approach is a defendable access control scheme in which the user permissions are based on their requirement and data. After accessing the healthcare record, a centralized IoT security augmentation and assessment is provided. The blockchain records determine and revoke the access grant based on previous access and delegation sequences. This scheme analyses the possible delegation methods for providing precise users with interrupt-free healthcare record access. The blockchain recommendations are analyzed using a trained learning paradigm to provide further access and denials. The proposed method reduces false rates by 11.74%, increases access rates by 13.1%, speeds up access and processing by 12.36% and 13.23%, respectively, and reduces failure rates by 9.94%. The OACS decreases false rates by 10.64%, processing time by 15.62%, and failure rates by 10.95%.

Keywords Access control, Blockchain, Electronic healthcare records, Healthcare, Internet of things, Random forest, Security

List of symbols

γ	Anonymous Entries
$e_n + u_n$	Health Care Center and Services
$\mathrm{Q_E}$	User Request
K_h	Blockchain-Based Healthcare Services
$\mathrm{G_R}$	Access Grant
$\mathrm{F_D}$	Defendable Services
$\mathrm{R_D}$	Healthcare Record
$\mathrm{J_C}$	Record Forwarding
p^t	Requirement of Patients

[1]Department of Computer Engineering, Aligarh Muslim University, Aligarh 202002, India. [2]College of Computer Science, King Khalid University, 61413 Abha, Saudi Arabia. [3]School of Computing, Gachon University, Seongnam 13120, Republic of Korea. [4]Department of Computer Science and Information Systems, College of Applied Sciences, AlMaarefa University, 13713 Ad Diriyah, Riyadh, Kingdom of Saudi Arabia. [5]Department of Computer Engineering and Information, College of Engineering in Wadi Alddawasir, Prince Sattam bin Abdulaziz University, 16273 Al-Kharj, Saudi Arabia. [6]Department of Business Administration, College of Business Administration, Princess Nourah Bint Abdulrahman University, PO Box 84428, 11671 Riyadh, Saudi Arabia. ✉email: hmin@gachon.ac.kr

α	Access Level States
H	Authorization for User Handling
m_i	Defendable Permission Level
o_n	Anonymous Detection
c_r	Appropriate Data to the End Users
d'	Access Control
w_0	Information Forwarded to Appropriate User
i_0	User Time
$f_d(\varnothing)$	Defendable Access Control
t'	Data Forwarded to Users Based on Relevance
S	Access Grant
Y	Secure Transmission of Data
l_a	The Augmentation Approach for the Access Grant
$\varnothing$	Blockchain Security
R	Recommends for the Training Data to Improve the Access Rate
s_m	Assessment
∂	Access Grant and Revokes
$\alpha(t_g)$	Training Data
P	Security Prediction
r_0	Computation Time
e_0	Error Data
$\gamma(d')$	Interrupt-Free Healthcare Record Access
f'	Failure Rate
Δ	State the Matching
n'	Decrease the Denial of Service
β	Failure in Networking Healthcare Data Transmission
v_k	Authorized Access Level

Internet of Things-enabled healthcare security concerns generally include unauthorized access to patient data, which could violate trust and confidentiality. More linked health gadgets and more individually identifiable health information mean it's more necessary than ever to anonymize and safeguard this data using blockchain technology. Due to performance difficulties like controlling system scalability as devices increase, essential health records may be unreachable for a lengthy period in an emergency. Integrating different IoT devices causes uneven security methods, making universal access control tougher. These issues require a balance between data management, adaptive access control, and security. Blockchain technology has the potential to completely change several business sectors, including financing, management of supply chains, and healthcare. Blockchain is fundamentally a distributed ledger that safely logs transactions across several computers or nodes and verifies them. Electronic health records (EHRs) can be stored and managed using a secure, unchangeable ledger that can be provided via blockchain. Blockchain preserves the integrity and confidentiality of health records by leveraging cryptographic hashes and decentralized patient data storage to restrict unauthorized access and modification. Not all nodes on the blockchain network will necessarily have a backup of the data once it is added to the blockchain, as the technology, while providing tamper-resistant features, does not guarantee that all nodes store identical copies of the data. With its autonomous and distributed ledger structure, blockchain technology offers data redundancy and security; nevertheless, it does not guarantee that every node retains a copy of every data. Blockchain's support of granular consent management can give people more power over their health data. Patients can securely grant or revoke access to their health records, protecting their privacy while allowing data sharing for study and individualized care.

Blockchain technology's decentralization means data is stored on a distributed node network, not a central server. This dispersal of data across nodes helps avoid single points of failure. The network's redundancy and consensus procedures ensure that it continues to function even in the event of a node or group failure, and the nodes work together to preserve access control rules. This collective approach ensures data security and system integrity, affirming the statement's correctness. IoT is a new technological paradigm expected to emerge as a dynamic global network of interacting devices and machines, incorporating many standards and technologies to enable sensing, identification, networking, connectivity, storage, computational, and other capabilities[1]. The development of IoT includes multiple intelligent sensory elements and wearable smart devices, which are crucial in various fields such as healthcare, mining, buildings, cities, agriculture, transportation, industries, and automated systems[2]. The healthcare industry has integrated IoT successfully due to advancements in information and communication technologies, resulting in self-replenishing services. Healthcare services using IoT can provide data for EHRs, but EHRs are not exclusively for IoT; they represent digital medical data accessible through various means, including traditional computer systems, web interfaces, and mobile apps. Smart devices offer seamless connectivity between users and EHR systems, enabling end-to-end access and retrieval of information. As a result, users retrieve the required information without any delays or interruptions.

Furthermore, smart devices also enhance information sharing as part of health monitoring and patient assessment[3]. IoT infrastructure transfers such communications to the medical and healthcare centres. The healthcare centre comprises the information technology infrastructure for storing, managing, exchanging, and analyzing data[4]. This infrastructure includes servers, databases, EHR systems, networking equipment, and security systems. IoT platform exploits cloud computing resources for analyzing, visualization, and projecting healthcare data[5]. Data handling varies based on the type and quantity of data accumulated or shared from user devices. Different types of data require different levels of processing and storage resources in IoT-based

healthcare services[6]. The raw data collected from various sources is processed and organized into EHR that can be easily identified, accessed, and retrieved. In this organization of data, timestamp-based augmentation and updates are often used for access. Therefore, a user query is processed and granted with an identified EHR through healthcare applications and cloud services[1,5].

Healthcare data contains sensitive user information, such as personal and medical records, that must be kept secure to ensure privacy. Unauthorized access and modifications to EHR raise concerns about the privacy and security of sensitive healthcare data and the accuracy of medical diagnoses and treatment plans[7]. Besides, active attacks compromise the confidentiality and integrity of healthcare data, exposing sensitive information[8]. Therefore, security demands are crucial to protect sensitive healthcare data from attacks, including unauthorized access, modification, and exposure. It is essential to ensure healthcare data's confidentiality, integrity, and availability to maintain privacy and prevent potential patient harm[9]. Healthcare organizations and service providers implement robust security measures such as access control, encryption, authentication, and monitoring to protect healthcare data from cyber threats[10]. IoT-based healthcare services use various security measures to protect sensitive healthcare data, including infrastructure and access-based security[11]. Infrastructure services rely on various security measures such as authentication, identity verification, and device connectivity-based security. At the same time, access-level security includes data authentication, trust modules, and integrity verification for meeting security demands[11]. These two security measures provide swift and reliable data and user privacy, reducing adversary impacts[12]. The security measures implemented through IoT vary in effectiveness and complexity, reflecting IoT security's ongoing and evolving nature.

Data authentication and validation provide access and analysis security by restricting unauthorized access and preventing tampering[13]. These measures ensure that only authorized users have access to the healthcare data and that the data is accurate and reliable for analysis. Regularly scheduled security updates and processing improve the reliability of data sharing and processing and help mitigate the impact of various attacks. Key-based authentication is a widely used security mechanism that involves using cryptographic keys to verify the authenticity of data and ensure secure communication between devices[14]. Trust models are also used to establish trust between different entities in an IoT ecosystem, such as between devices, applications, and users, to prevent unauthorized access and malicious attacks[15]. Therefore, IoT-based healthcare services provide a scalable and harmonized security measure that leverages authentication, validation, and trust models to ensure data and user privacy and prevent unauthorized access and modifications[16].

Sensitive healthcare information requires strong authentication and verification mechanisms to ensure privacy and prevent unauthorized access or retrieval. Anonymous access and unauthorized storage can compromise the integrity of EHR, leading to modifications or unavailability of the data that may result in the wrong diagnosis, delayed treatments, and other serious consequences[17]. Therefore, healthcare service providers implement privacy controls and access management to ensure concealed access and privacy controls for different users. This process ensures that only authorized individuals can access the data, maintaining data confidentiality. The user's access levels and permissions are defined based on the verification and platform recommendations[18]. A user's access levels and permissions can be updated based on various factors such as user behaviour, data content, and availability. Blockchain technology offers a promising solution to mitigate security risks associated with healthcare systems. Its decentralized and immutable nature provides a robust and secure platform for storing, managing, and sharing sensitive healthcare data[17]. The computational complexity of reaching consensus among nodes might increase latency and degrade throughput when handling numerous networked devices' massive volume of real-time transactions. Even while blockchain enhances data security, it must address scalability and efficiency issues to ensure successful performance in large-scale IoT scenarios.

Blockchain can store access control policies in a distributed, immutable, and transparent tamper-evident ledger, making it an ideal solution to mitigate security risks associated with unauthorized access, tampering, and data breaches in the healthcare industry[19]. This process allows for enforcing access control policies without relying on a centralized authority. Blockchain-based access control allows fine-grained access control over user permissions and delegations. Fine-grained access control provides a more detailed and precise way of controlling access to data and resources. It typically involves defining access permissions based on specific attributes or characteristics of the user, data, or context[20]. Breaking down access permissions into smaller, more specific units is called granular control, which involves defining access permissions on a per-object or per-action basis. This access control prevents false data injection and modification by restricting access to sensitive data and resources based on specific attributes, such as user role or location[21]. It also allows for more sophisticated security recommendations and authentication modifications, such as granting temporary access or requiring multi-factor authentication for high-risk actions. Blockchain technology allows the storing and processing users' credentials and device access levels securely and de-centrally[22]. Implementing an access control scheme allows access-level security and patient privacy in healthcare services that IoT enables. With blockchain technology, it is possible to precisely analyze past states and revoke access grants accordingly while granting authorized persons uninterrupted access based on delegation knowledge.

The OACS framework employs blockchain technology to govern consent and to design and enforce access control policies using smart contracts, as shown in Fig. 1.

(1) Creating a smart contract requires user authorization to access healthcare data. This contract specifies data access rules.
(2) The blockchain network receives all IoT-generated health data requests from healthcare providers and applications
(3) Smart contracts allow the blockchain network to verify user consent by matching requests to contract rules. It checks the request's legality using user roles, security levels, and past actions.

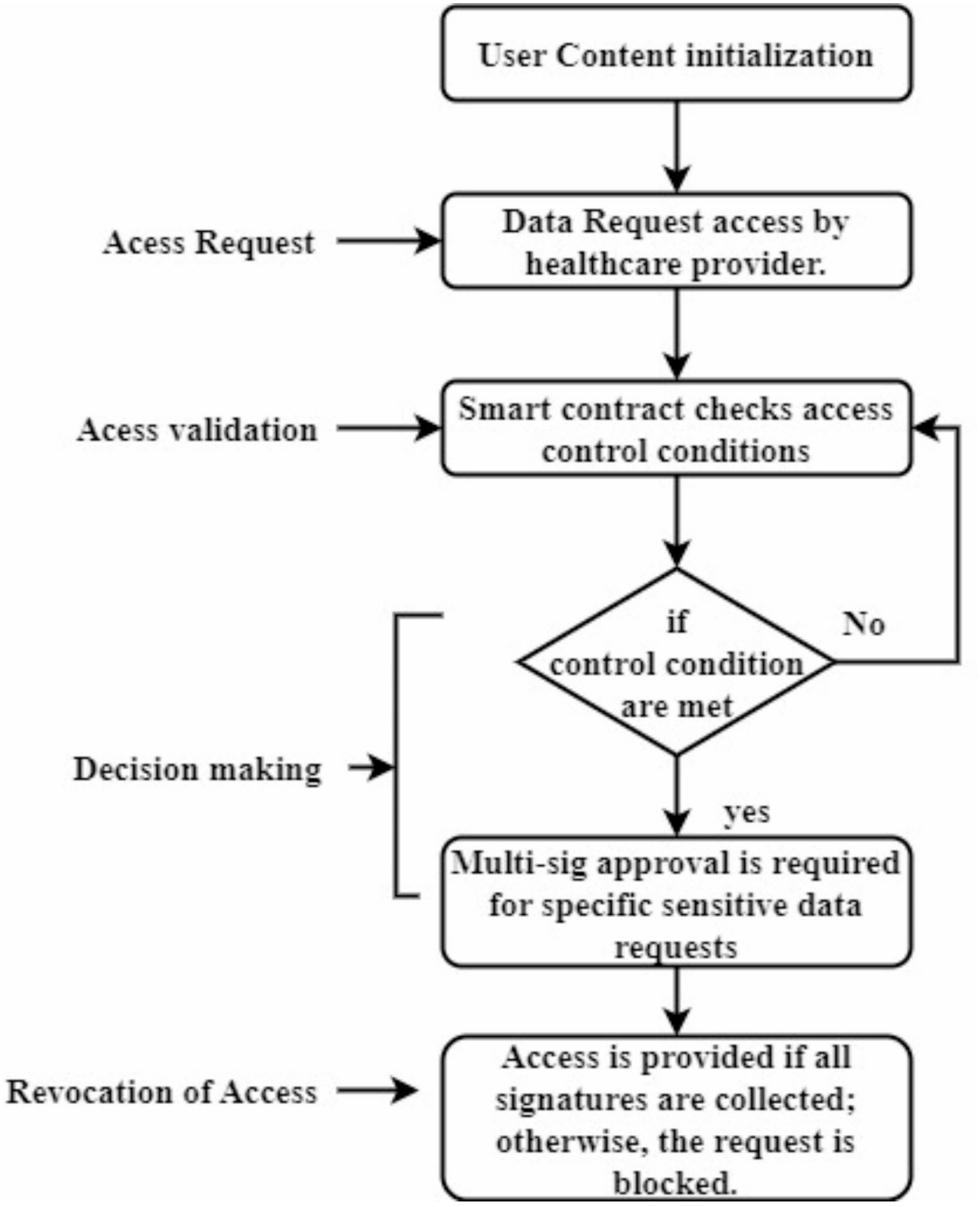

Fig. 1. Flow diagram of consent management.

(4) A smart contract decision allows access if the request fits its conditions. The system can automatically revoke access when user actions or security needs change. Blockchain allows real-time tracking and consent adjustments by recording delegations and access.

Motivation

IoT-enabled healthcare poses major security risks, such as unauthorized access to sensitive patient data and data breaches due to the large number of interconnected devices, which motivated the OACS. The motivation behind

blockchain in healthcare is that data is stored and retrieved on the blockchain tamper-proof because of its secure and unchangeable storage method. Data integrity is improved, and the risk of data breaches is decreased because blockchain's decentralized structure ensures that data cannot be readily updated or manipulated. Therefore, the primary objective of this study is to ensure robust security measures, including maintenance of authentication, access control, data integrity, and concealed sessions. These measures are implemented dynamically and flexibly, depending on user behaviour, potential adversary impact, and the system's reliability. The absence of access control privileges for user information underscores the paramount challenge of preserving patient privacy in IoT-based healthcare systems[23].

Design goals and contributions

The following design goals are set to implement the proposed methodology:

(1) By introducing an OACS, access-level security and privacy of patients in IoT-enabled healthcare services can be provided.
(2) The incorporation of blockchain enables accurate analysis and revocation of access grants based on the previous state and provides uninterrupted access to authorized users based on delegation knowledge.
(3) Enhance the access control scheme and informed decisions using a trained learning paradigm
(4) Improved overall efficiency by evaluating false rate, failure, processing time, access rate, and time

The work's main novelty is combining the access control scheme with the blockchain concept to improve overall security. In addition, a learning paradigm is incorporated that provides the grants and revocation effectively. The contributions of this article in addressing the sensitive nature of healthcare data include the following:

(1) To design an effective access control scheme that grants appropriate user permissions for secure and dependable access to healthcare data.
(2) To augment complementary security for grant and revocation powered by blockchain with delegation knowledge
(3) To incorporate a trained learning paradigm to decide on access grants and revocation through iterated learning and random forest (RF) classification.
(4) The OACS outperformed typical access control methods in processing speed, false positive rate (FPR), and dynamic access request flexibility. These findings show that an OACS can secure healthcare IoT settings while streamlining processes, which could inform enhanced access management solutions.

Overall, this approach helps to ensure the confidentiality, integrity, and availability of sensitive healthcare data, which is crucial for maintaining the quality of care provided to patients. The rest of the paper is organized as follows. Section "Related works" analyzes the researchers' studies on the secured IoT health data monitoring process. Section "Proposed opportunistic access control scheme" proposes a blockchain-based IoT data transmission and access control process, and system efficiency is evaluated in Section "Performance analysis". Section "Conclusion" summarizes and concludes the work.

Related works

Modern technology in healthcare has led to significant advancements in how medical services are delivered to patients. Cloud computing, fog computing, and mobile-based healthcare systems are some technologies implemented in recent years to improve healthcare service delivery. However, the security and privacy of patients' sensitive information remain major concerns. Various access control models and security mechanisms based on blockchain have been proposed to address these concerns.

Li et al.[24] proposed a data aggregation scheme using blockchain technology for medical environments to secure patient privacy and provide more personalized healthcare services. Additionally, a group authentication mechanism was designed for multiple authorized users to access patients' health records and protect sensitive information with a group session key. With the advancements in information and telecommunication technologies, telecare has become integral to modern healthcare services. A telecare medical information system implemented in the wireless body area network (WBAN) offers the convenience of remote healthcare monitoring, enabling real-time data collection and analysis. However, these systems are prone to security threats, including eavesdropping, data tampering, and denial-of-service attacks.

The authors in[25] implemented a protocol that employed ciphertext-policy attribute-based encryption for access control and blockchain to guarantee data integrity. Access control models are necessary to verify legitimate user requests and prevent attacks. Similarly, healthcare systems have adopted traditional access control models such as role-based or attribute-based access control. While effective in managing permissions, these models often fail to adapt to dynamic contexts, such as emergency scenarios, making them susceptible to privilege escalation attacks. Singh et al.[26] proposed a trust-based access control model for the healthcare system that enhanced the accuracy and efficiency of the system by including a trust mechanism, trust model, and access control policies.

The growing need for wider access to healthcare data has prompted the development of healthcare information exchange between health authorities. The cloud paradigm is used as a solution but remains inefficient and vulnerable. To address this, researchers proposed EdgeMediChain (EMC), a secure and efficient data management framework that leveraged edge computing and blockchain to improve scalability, security, and privacy. As the proposed implementation is performed in simulation, the real-time implementation is very expensive to process[27].

In[28], the authors proposed a lightweight, secure access scheme (LSAS) that was robust and effective for protecting data security and privacy in cloud-based E-healthcare services. This scheme applied a secure access

technique using multiple keys derived through a key derivation function to ensure end-to-end information encryption and prohibit unauthorized access. However, employing a local database and low power wide area networks, the proposed approach is not economically viable, and security administration is more complex.

Zhang et al.[29] proposed an inference attack-resistant e-healthcare cloud system with two-layer encryption for fine-grained access control (TLE-FGAC) to address EHR data's security and privacy issues. The authors implemented a two-layer encryption scheme to efficiently and securely control access to EHR data while preserving the privacy of role attributes and access policies. They also suggested a blind data retrieving protocol that protected the EHR's access pattern of data attributes. It is crucial to evaluate the mechanism's applicability and flexibility in various healthcare contexts this proposed concept.

Fog computing, a distributed computing paradigm, has the potential to revolutionize the healthcare industry by bringing the power of cloud computing closer to the edge of the network, allowing for faster and more efficient processing of healthcare data. It is designed to support IoT and other applications that require real-time data processing, low-latency communications, and improved security and privacy. However, security risks are often not considered, and existing machine learning and blockchain approaches are inadequate for meeting the quality-of-service requirements of healthcare IoT. A novel solution integrating fog computing with blockchain is proposed to address this issue[30]. The proposed approach includes a fog computing-based three-tier architecture, an analytical model, a mathematical framework, and an advanced signature-based encryption algorithm for secure data transmission.

In[31], the authors presented a lightweight authentication and matrix-based key agreement scheme to ensure secure healthcare transmission in fog computing. The proposed scheme supported multi-party communication in fog computing and encrypted healthcare data using doubly-linked cyclic tables.

With the advancement of technology, healthcare providers can now gather and store large amounts of data. The healthcare industry has emerged as a potential area of big data application to improve patient diagnostic systems while preserving their privacy. Big data analytics is an effective approach to identifying patterns and trends that traditional methods may miss—however, big data comprises significant data privacy and security challenges. Therefore, a security framework for big data in healthcare based on the logistic equation, Hyperchaotic Equation, and DNA encoding was proposed[32]. A Lossless Computational Secret Image Sharing method was used to convert encrypted secret images into shares for distributed storage in cloud-based servers. Hyperchaotic and DNA encryption was used to improve overall security, and Pseudorandom Numbers generated by the Logistic Equation were XORed with the image sequence in two phases. The application of Secret Sharing generates completely noise-like cipher images that enhance the security of the cloud-based cryptosystem.

Study[33] designed a novel framework to integrate big data with privacy and security concerns to determine knowledge patterns for future decision-making in human immunodeficiency virus and Tuberculosis coinfection patients. The framework utilized unsupervised learning techniques in STATA and MATLAB 7.1 to develop patterns for the knowledge discovery process while maintaining data privacy and security.

In the era of health 4.0, mobile-based healthcare systems have emerged as healthcare services that utilize mobile devices such as smartphones, tablets, and wearable devices to provide healthcare services remotely. Hathaliya et al.[33] proposed an approach enabling patients to self-authenticate using their mobile and wearable devices, establishing a session key between owned devices. After mutual authentication, the cloud server verifies each user. An attribute-based signature scheme with attribute revocation was implemented to protect user identity privacy in a blockchain-based healthcare system[34]. This scheme used attributes to identify users and protect their identities. The attribute revocation was achieved using the KUNodes algorithm. The proposed method was unforgeable, collusion-resistant, and privacy-preserving and required relatively few pairing operations without relying on a central authority.

In[35], the authors also implemented BCHealth, an architecture based on blockchain technology, to address the data security and privacy challenges in smart healthcare applications. The proposed architecture allowed data owners to define their access policies over their healthcare data, and it was composed of two separate chains for storing access policies and data transactions.

Tolba et al.[36] applied predictive data analysis to improve data security features in modern healthcare systems. This approach prevented illegal access to sensitive information by selectively processing healthcare and grid data. The proposed method used transfer learning to analyze and match medical and grid data recurrently, classify loss, and predict accurate analysis data. The predictive data analysis method's intensive learning and training process can differentiate between authenticated and illegal access to healthcare data.

Liu et al.[37] Suggested blockchain and distributed ledger technology to improve biomedical security and privacy across healthcare applications. Since this involves managing and accessing a large amount of medical information, it makes it feasible for patients to use the information to support their care and provide strong consent systems for sharing data among various organizations and applications. Additionally, this sort of technology can maintain data to ensure reliability. The experimental study revealed that it could boost the ratios of sharing time and records by 8.077% and 7.03%, respectively. Additionally, it delivers a 20.11% faster response time than the alternative methods. The suggested solution limits computation and convergence time in the authentication situation by 10.26% and 12.31%, respectively.

Wu et al.[38] provided a blockchain-based intelligent healthcare network with granular privacy protection for trustworthy data sharing and transferring between various users. To provide attribute-based privacy protection in the transactional process, create a dynamic access control system that uses local differential privacy techniques with blockchain technology. The smart contracts address the needs of anonymous transactions, adaptive control access, matching, and the assessment of published data in an open network. The suggested privacy-preserved method can conduct dependable and stable transactions between EMR providers and requesters. The accuracy and utility of the data may be jeopardized by adding noise or randomization to protect privacy, which could lower the standard of evaluation and decision-making.

Rani et al.[39] described a framework that uses numerous pre-trained models and transferred learning to use blockchain for security. The suggested routing technique uses probability, believability rating, and node energy to route the data to its destination with the least network overhead and energy consumption. It isn't easy to reach a common understanding of norms, protocols, and data representations. The suggested routing routes the data to its destination with variables like likelihood, credibility rating, node energy, etc., to reduce network overhead and minimize energy usage. The findings demonstrate that the suggested method provides 92.24% classification accuracy.

Sapna et al.[40] discussed an efficient IoT interoperability model using a secure access control mechanism (ACM). Except for the downward flow direction, the mode of operation for a Routing Protocol designed for low-power and lossy networks is configured to the direction of multipoint-to-point traffic. In this configuration, the server receives data packets from the sensor nodes, which it then uses to calculate trust levels. To reduce packet loss by 0.43%, energy consumption by 0.4%, and average residual energy loss by 0.87 mJ, the suggested trust mechanism is based on privacy access control. The largest average residual energy loss occurs at node 30, which has the highest residual energy.

Zahid Ghaffar et al.[41] suggested the ML Attack Resilient and Low-Latency Authentication Scheme for AI-driven Patient Health Monitoring System. Concerns about privacy and security have made it difficult to design a mutual authentication and key agreement mechanism for RPHM that is both effective and safe. For RPHM systems powered by AI, dependable and low-latency connectivity is especially essential. The high delay rates and vulnerability to machine learning attacks are two of the many problems with many current authentication techniques. We address these concerns by introducing a low-latency authentication system for AI-driven RPHM resistant to machine learning attacks. The suggested method makes use of an ECC-based three-factor authentication system. To protect medical sensing equipment against assaults by machine learning, it uses an OPUF or one-time physical unclonable function. The robustness and durability of the scheme's security are shown by evaluations of its security in informal and formal settings. In addition, the scheme's performance is evaluated using several metrics, proving that it is better than comparable schemes and achieves a low latency rate.

Khalid Mahmood et al.[42] proposed a Cloud-Assisted, Secure, Cost-Effective Authenticated Solution for a Remote Wearable Health Monitoring System. The author explores informal security proof to demonstrate the security strength of the proposed approach against recognised security risks. A thorough evaluation of the suggested scheme's performance in conjunction with relevant protocols shows that it can cut communication costs by 40% and calculation expenses by 37%. In addition, the approach provides further security measures to avoid physical and desynchronisation threats.

Muhammad Asad Saleem et al.[43] recommended the Puncturable Pseudorandom Function for Provably a Secure Authentication Protocol for Mobile Clients in an IoT Environment. Two mobile clients may authenticate each other via the server using the proposed PSK-MC protocol. The security strength of the proposed protocol is determined via formal and informal evaluations. The random oracle model, which is often used, is used to illustrate the formal security analysis. In addition, a desktop computer is utilised to get experimental findings to evaluate computation cost, while a mobile device is used to conduct all the cryptographic operations used by the mobile client side. According to the results of the performance investigation, the protocol outperforms similar ones since it has the lowest communication and computing overhead.

Table 1 presents a comprehensive comparison of various models from the literature survey, highlighting key features, FPR, processing time, blockchain integration, and the strengths and weaknesses of each approach. This table offers a clear overview of the different models, showcasing their performance metrics and the extent to which they incorporate blockchain technology for enhanced security and policy enforcement.

Scalability, high latency, and static policy enforcement make healthcare IoT ACM unsuitable for dynamic contexts. Traditional access control measures are inflexible and unable to respond to changing user behaviours and urgent real-time demands, which might delay high-volume requests. Centralized access control solutions increase security risks and single points of failure. The OACS leverages blockchain and RF machine learning to provide a secure, scalable, and adaptable access control system. The blockchain element of the OACS ensures distributed, tamper-proof access request processing, while the machine learning part dynamically modifies permissions using real-time data and user behaviour. This dual strategy reduces latency scales and improves access control in healthcare IoT systems, bridging security and operational efficiency.

While these methods effectively establish security for IoT healthcare data, they fail to manage authentication and security while analyzing large amounts of data and hidden sections. The existing algorithms face many challenges, especially a lack of concentration related to authentication and security. Systems may be susceptible to unauthorized access if authentication procedures are weak or poorly built. It's crucial to anonymize personally identifying information when working with vast amounts of data to safeguard the privacy of individuals. When examining massive amounts of data, it is crucial to prioritize security and authentication. Organizations can improve their capacity to safeguard sensitive information and reduce risks by implementing strong security measures like access control measures and routinely evaluating and upgrading security rules. Rather, it focuses on huge data analysis of healthcare records. Some of the existing limitations are discussed here. The security administration becomes more complex, particularly with the multi-key-based authentication methods discussed in[28,31]. On the contrary, the contributions in[25] and[33] present a long time gap resulting from single and multi-server authentications. However, the focus is on improving the session duration while maintaining consistent access and authentication security. In this process, fine-grained access control[29], pairing operations[34], or flexible yet robust methods, as in[27], are required.

This plan's novel work suggests an enhanced access control system as a smart contract in blockchain. However, the access control strategy put out by this proposal restricts the kinds of access people can have with the recommended approach and is defined based on the delegation factors. This approach uses access control

Model	Key features	FPR	Processing Time (ms)	Blockchain Integration	Strength	Weakness
BCHealth-Privacy[19]	Access control with attribute revocation	0.0715	479	High (Blockchain + Attribute Control)	Efficient health data exchange, High data integrity through blockchain	Complexity in maintaining multiple authentication keys and reliance on edge computing may lead to bottlenecks
Trust-Based Access Control[26]	Trust mechanism, security for healthcare systems	0.0745	603	Moderate (Trust-based)	Implements trust-based mechanisms, Strong security measures	This can lead to false positives/ negatives in access decisions, Complexity in managing trust relationships
Moderate (Trust-based)[27]	Efficient health data exchange, edge-augmented	0.0673	537	High (Blockchain with Edge)	Combines edge computing with blockchain, Enhances data access speed	Moderate processing time under heavy loads May face challenges in multi-key authentication
LSAS-Secure[28]	Multi-party key agreement, matrix-based keys	0.0523	563	High (Matrix-Based Security)	Lightweight and efficient for mobile environments.	Vulnerable to unauthorized access if keys are leaked,
TLE-FGAC[29]	Fine-grained access control, EHR privacy	0.0931	768.09	Moderate (Two-layer Encryption)	Fine-grained access control, Strong data privacy protections	High latency due to sequential processing, Limited scalability for large user bases
Fog-BI[30]	IoT security for healthcare, low latency	0.0584	490.57	High (Blockchain with Fog)	Quick access decision-making	Limited adaptability to changing access patterns
BC Health[35]	Decentralized, attribute-based access policies	0.0471	450	High (Blockchain-based Access)	Decentralized management of permissions, Robust against tampering	Potential scalability issues with increased nodes, Higher latency in achieving consensus
OACS (Proposed)	Dynamic consent management, RF, smart contracts	0.0321	382.50	High (Blockchain + RF)	Enhanced Security, Dynamic and adaptive access control	Dependency on data quality

Table 1. Comparative analysis of models from Literature Survey.

contact based on blockchain. It predicts authorization using an RF scheme compared to the previously proposed ones, which lacked management in session duration while preserving constant access and authentication security and a waste of time in handling single and multiple servers. These drawbacks motivate the introduction of an OACS using blockchain that emphasizes user validation for secure access.

Proposed opportunistic access control scheme

System architecture

IoT-based healthcare systems utilize service forwarding to the appropriate patient. This deployment of an IoT environment enables ubiquitous and convenient patient access to related services. The ubiquitous data is stored in an authorized repository to determine access to secure users. In the healthcare industry, IoT detects the data; based on this, the service is provided on time. The computation time is decreased, and the patients handle the relevant information. The storing of relevant and irrelevant data is done on the repository; from this approach, the access level states the user's health. This study proposes a fully decentralized authentication strategy leveraging blockchain to address the shortcomings of the present centralized authentication solutions. A distributed network of computing devices powers a blockchain called nodes.

Using the term opportunistic suggests that the proposed system may prioritize adaptability and flexibility in access domains, potentially by introducing some level of false positives or false negatives in certain situations. Such a metric is analyzed to accommodate dynamic or changing conditions and adapt to them. Incorporating blockchain technology is part of an effort to enhance transparency, traceability, and accountability in access decisions.

Every node keeps an archive of blockchain technology containing encrypted data on patient records. Thanks to this decentralized storage, data availability is improved as there is no single point of failure. Blockchain creates a safe ACM using cryptographic methods. Smart contracts, autonomous, rule-based contracts, can control who has access to patient records. Only parties with permission to see or alter the patient data can do so, thanks to smart contracts' enforcement of access control restrictions. The proposed scheme's process is illustrated in Fig. 2.

The proposed scheme performs user validation, access control, and decision-making using the blockchain paradigm. The assessment is based on the previous user information, such as access and revocation. Based on this information, blockchain provides users with access to delegations. User validation relies on identity verification and denial history (Fig. 2). The order or sequence in which permissions for access are assigned to various individuals inside a system is called the delegation sequence. According to historical data and user requirements, the delegation sequence enables the system to keep track of access privileges and make educated judgments about giving or denying access. Data security is ensured for the number of services and determines the relevant processing. The relevant service is evaluated for the access control scheme. The user permission is used to delegate the defendable access control scheme. The authorized repository defines the concord patient in the healthcare industry. All nodes on the blockchain network will not have a backup of the data once it is put in the blockchain because the technology is not tamper-proof. The security and privacy of medical records are considerably enhanced if an attacker interferes with the data in some nodes since the erroneous data will be found and corrected by other nodes.

Healthcare IoT data access management is the goal of the OACS, which combines machine learning for adaptive decision-making with blockchain for secure access control. At its heart, the OACS is a distributed

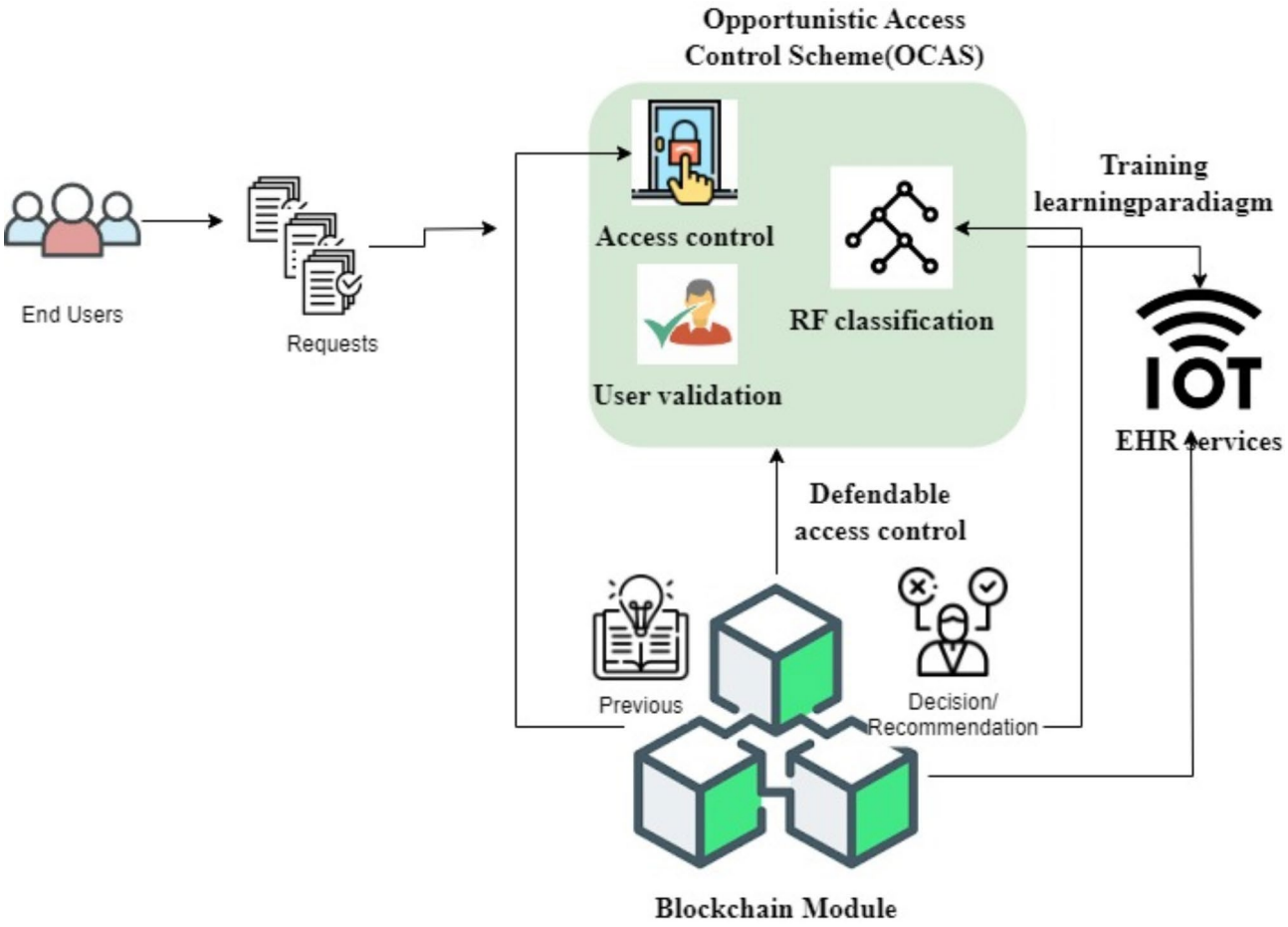

Fig. 2. The proposed Opportunistic Access Control Scheme.

ledger system that records all transactions, including those involving access requests (approved or denied). Smart contracts automate the process of enforcing policies related to access control. With each access request, the smart contract verifies the user's identity and verifies the data permissions and predefined restrictions. Because these smart contracts are unchangeable once deployed, they add another safeguard by ensuring the rules for access control are consistent and trustworthy.

Along with blockchain technology, the OACS also uses RF techniques for machine learning to assess access requests. The system utilises considerations such as user role, data sensitivity, access context, frequency of prior accesses, and request geolocation for classification. Access requests are categorized as valid or suspicious based on these factors. The system may adjust to its users' evolving demands and behaviours by processing past data using the RF algorithm. One way the algorithm can help prevent unauthorized access is by detecting suspicious patterns of requests (such as those coming from an unexpected location) and then implementing extra authentication processes.

The OACS takes the following steps in response to an access request:

(1) An initial step in the validation process is for the system to compare the user's credentials and previous actions with those stored on the blockchain.
(2) The OACS checks the blockchain for their delegation history, including previous attempts, permissions, and revocations, to verify that the user has the right authorisation for the resource they are requesting.
(3) For the final decision, the RF algorithm looks at the request through the lens of past access trends and behavioural analysis. This assessment determines whether the request is approved or denied by the OACS.
(4) After reaching a decision, it is added to the blockchain as a new transaction, ensuring that the access request record cannot be altered.

Utilizing methods like sharding to divide the blockchain and reduce processing costs for each node and off-chain storage for non-critical data, the OACS tackles possible scalability difficulties, especially in high-traffic IoT applications. This makes it ideal for widespread healthcare IoT deployments since it keeps the system responsive even under heavy strain.

Unauthorized people can attempt to get physical access to IoT devices that support them. To do this, one can tamper with the devices, directly extract data from memory, or connect to the network to intercept or modify data

transfers. The access level is kept secure by blocking unauthorized entrances and data downloads. Data security is guaranteed for various services, and the appropriate processing is chosen. The pertinent service is assessed in light of the access control plan. The defendable access control scheme is delegated via user authorization. In the healthcare sector, the authorized repository specifies the concord patient. The examples are: Blockchain offers a tamper-proof and unchangeable storage solution for medical documents called an authorized repository. Here, blockchain can store patient data, ensuring that once the information is recorded, it cannot be changed without the network's participants' consent. It preserves data integrity and stops unidentified people from tampering with the records. Blockchain relies on decentralized consensus methods, in which several network users verify and concur on the blockchain's current state. With the help of this consensus model, healthcare records are protected against unilateral modification or manipulation, increasing the security against unauthorized access.

Here, similar information matches the current and the previous state and examines the authorized repository. The data repository provides access grants to the patient and maintains security. Blockchain is a ledger that includes healthcare data collection and provides similar information to the end-users. To determine the legitimacy of a healthcare provider's access to patient records during an emergency, Eq. (1) represents the circumstances when access requests are being considered. User credentials, historical access patterns, and data sensitivity are defined; they are used to improve the healthcare IoT system's security by re-evaluating permissions when an anomaly in access patterns is detected.

$$\gamma = \left(\frac{1}{e_n + u_n}\right) * \sum_{g_r}^{e_0} (m_i + r_0) * \left[\left(\frac{r_d\,(q_e) \Big/ e_n}{w_0 + t'}\right) + (k_h * m_i)\right] + j_c \tag{1}$$

As shown in Eq. (1), where e_n denotes the number of active entities, u_n is the number of unauthorized users, e_0 denotes the number of evaluated requests, $m_i$represents the access request metric, r_0 denotes the constant factor related to an access request, $\mathrm{q_e}$ denotes user request, $\mathrm{k_h}$ indicates blockchain-based healthcare services, γ represents anonymous entries, $\mathrm{g_r}$ signifies access grant, r_d symbolizes healthcare record holds, $w_0$is the information Forwarded to the appropriate user, f_d implies defendable services, j_c denotes record forwarding. The anonymous entries and data download define the access level for the number of services. Here, the computation determines the repository and examines the related services on time. An access control scheme for security analysis is employed, and it is stored in an authorized contract with a blockchain by identifying the user request and access grant for the initiated transaction flow was stored in a current state and then based on delegation knowledge and identifies the anonymity user request and then revoke it. Assuring consensus and preventing unauthorized changes, the distributed network of blockchain nodes collectively maintains the ledger and authenticates transactions. Security analysis was performed using the abovementioned procedures.

The computation process utilizes the recent IoT for ubiquitous and concord patients/users. A similar service is forwarded to the end-user by defining anonymity in the network. In IoT, the repository stores the collection of information and leverages the access level for security. The security level is maintained for anonymous entries and data downloads. For every iteration step, the analysis is carried out for the anonymous entries and data download.

The system manages access grants using blockchain technology. Based on prior access and delegation sequences, access grants are determined from blockchain records and can be revoked. The service handling deploys the augmentation and evaluation to refer to the access allowed to the end-users and is used to decide the blockchain. The requirement is assessed here, and blockchain provides security using Eq. (3). The decision is made for the deployable blockchain security and defendable access control followed by the security, and it is referred to in Eq. (4). This RF classification tree is used to classify the access, give and revoke suggestions given by blockchain, and forward the information on time. Equation (6) is used by the blockchain suggestion to analyze this scheme's training stage of processing data and investigates the blockchain recommendation's access-level security to ensure security. The security setting is appropriate for the range of services and widespread information sharing by accessing Eq. (13).

The detection process states the authorized service and forwards it to the defendable access control. This paper introduces an OACS for leveraging access-level security and the defendable access control scheme. The access-control scheme determines the related services, provides the authorized repository, and deploys ubiquitous information. The information forwarding is used to determine the healthcare record and estimate the defendable service to the end-users. Blockchain for the healthcare system is used to utilize the related services, and it is represented as k_h. The number of users who request the requirement q_e in Eq. (2a) to the healthcare centre, $\{u_0, u_1, \ldots\ u_n\}$ and services are defined as $\{e_0, e_1, \ldots\ e_n\}$.

Here, analysis defines the anonymous entries to access the authorized record from IoT, referred to as γ . The access is granted to the end-users based on the relevant information, and it is denoted as g_r described using Eq. (2b). The healthcare centre handles the requests/requirements of the patients p^t, and matching is performed with the current and previous state, which provides the result. Here, the permission m_i is granted to the patient to ensure the security level. The healthcare record holds the collection of information regarding the patients, and it is represented as r_d. In this approach, access control is used to determine the defendable services, and it is denoted as f_d. The access control defines the blockchain for better record forwarding, and it is termed as j_c. Thus, the information w_0 is forwarded to the appropriate user on time i_0. From this analysis approach, the examination for access level is formulated in the following Eq. (2). This equation calculates the access efficacy score (α), which indicates the likelihood of approval based on several parameters. Credentials, request significance, prior access trends, and present request context are considered. The score helps improve decision-making by revealing the access request's legitimacy.

$$\alpha = (u_0 + m_i) * \left(\frac{H + c_r}{\prod_{g_r} (S * r_d)} \right) + (q_e * u_0) \tag{2}$$

Query effectiveness (q_e) measures access request efficacy based on the time and resources involved. This equation considers timing, resource sensitivity, and other criteria to decide if an access request is appropriate.

$$q_e = t' * w_0(g_r + o_n) \tag{2a}$$

This equation estimates the group of resources (g_r) associated with the access request by including data sensitivity (f_d), present request context (c_r), and access request metric (m_i). Quantification helps prioritize access requests by resource utilization to handle sensitive data correctly.

$$g_r = (f_d + c_r) * m_i \tag{2b}$$

This equation evaluates the request context (c_r) using query effectiveness (q_e), a historical adjustment factor (k_h), and any necessary deviation or adjustment ($d\prime$). This equation uses the request's context to determine if access is good in the current situation.

$$c_r = (q_e + k_h) - d\prime \tag{2c}$$

In Eq. (2), the access level states the anonymous entries and data download. Here, the examination provides the authorization and deploys the security. The access control determines the defendable permission and examines the blockchain. The requirement provides IoT security augmentation and assessment for healthcare record access. The augmentation determines the access grant and provides the requirement, and it is represented as $\left(\frac{H + c_r}{\prod_{g_r} (S * r_d)} \right)$.

Here, the requirement defines anonymous and data download and estimates the defendable access control. The assessment determines permission access for the requested users. The request is granted based on the healthcare record and deploys the authorization H for the user service handling. The service handling is examined to determine the appropriate information exchange between the users in IoT. Here, examination α is performed for the requirement, and permission is granted to the users based on the anonymous o_n detection. The control is provided to forward the appropriate data to the end users, and it is represented as c_r and calculated using Eq. (2c). Figure 3 presents the user access grant procedure.

This access grant procedure is defined by two conditions, namely verification success and failure. Access level and user delegations are defined based on the available information. A failed verification (user) is revoked of current access, and the new request is denied (refer to Fig. 3). Blockchain security states the augmentation and assessment and defines the access grant. Thus, the data is forwarded to the users based on relevance, and it is represented as $t\prime$. The defendable access control transfers the information to the appropriate user, and it is denoted as f_d. The delegate service is handled by the end-users, and it is based on the access control and is denoted as $d\prime$. Equation (3) performs the data forwarding based on the requirement and data delegated for defendable access control. From the access-level approach, an OACS is used for security maintenance and examines the user permission for the requirement for the data. IoT security is used to define the user permission delegated for service forwarding.

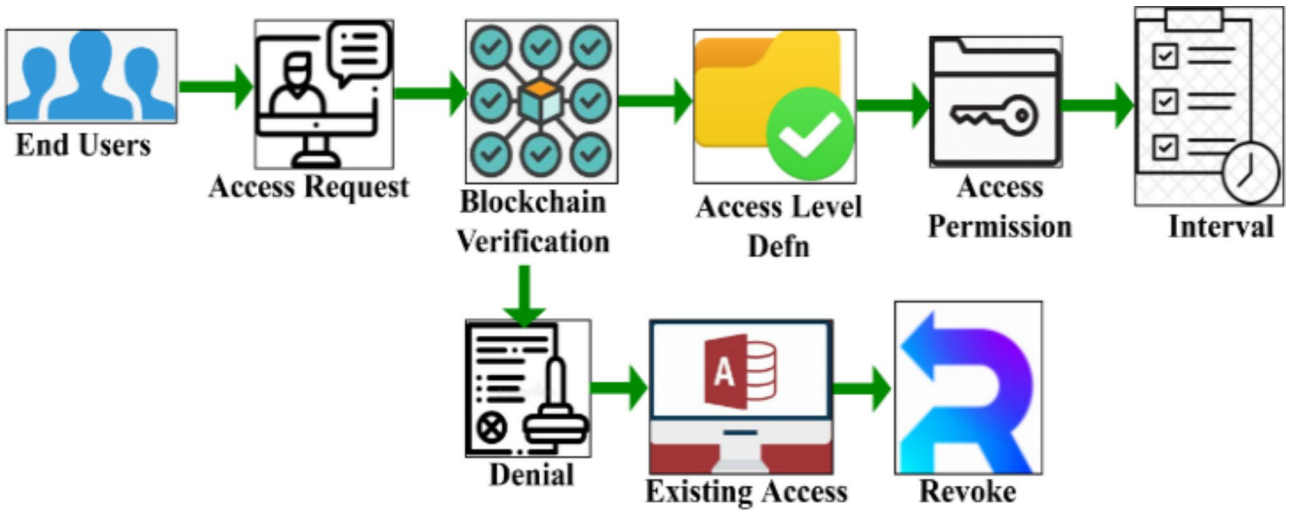

Fig. 3. Access grant procedure.

The defendable access control scheme defines the user permission delegated based on the requirement and data. The anonymous entries and data downloads are used to estimate the access to the secure users. The service handling is used to determine the blockchain and deploys the augmentation and assessment to refer to the access S granted to the end-users. Here, the evaluation is carried out for the requirement, and the blockchain is deployed for security.

Several aspects of forwarding processes require mathematical formulae by accounting for the parameters like user request on time for a particular requirement is verified by authorization and permission given for authorized users to access the information in the secured environment as represented in Eq. (3):

$$f_d(\varnothing) = \prod_{m_i}^{u_0} (w_0 + S) * \left(Y + \frac{H}{c_r}\right) - \left[\left(t' * k_h\right) * \ (q_e - i_0)\right] + d\prime \tag{3}$$

The defendable access control f_d is calculated in response to blockchain security $\varnothing$ by analyzing the authorization H the information w_0 is forwarded on time i_0 only when the permission m_i is granted to the patient u_0 to ensure the security level and the blockchain augmentation to refer to the access S granted to the end-users. Considering the blockchain for the healthcare system to utilize the related services, it is represented as k_h the data is forwarded to the users based on relevance, and it is represented as $t\prime$. User requirement request is given as q_e followed by analyzing the delegated service, which is handled by the end-users; it is based on access control and is denoted as $d\prime$.

Access is granted to the secure Y transmission of data from one end to the other. The anonymous detection is detected, and the secure transmission is deployed for the requested user. The determination is done for the defendable access control and deployment of blockchain security, which is termed as $\varnothing$. The computation is performed for the requirement, and it is based on the time, and it is formulated as $[(t' * k_h) * (q_e - i_0)]$. Thus, the delegation, requirement, and data forwarding are examined in Eq. (3), and the security is provided using Eq. (4).

$$Y = \frac{1}{e_n} * \sum_{w_0} \left[(c_r + H) * \left(\gamma + \frac{k_h * l_a}{m_i}\right)\right] + (q_e * r_d) - \varnothing \tag{4}$$

The security is maintained to prevent anonymous entries and data downloads, and the blockchain is deployed for assessment and augmentation. The computation is based on the access grant and provides the recommendation approach. The recommendation is performed for the healthcare record and states the access control for the number of services and users in IoT. The OACS is used in the healthcare blockchain and permits delegated service handling. The defendable service provides permission for the access control level and estimates the security. For the iteration step, the healthcare record is used to state the augmentation for the assessment and provide security. Security is ensured for the blockchain to handle the record.

Blockchain is used to refer to the augmentation approach for the access grant l_a to the number of users in IoT. The examination states the access grant by providing permission, and it is represented as $\left(\gamma + \frac{k_h * l_a}{m_i}\right)$. Thus, the security level is balanced throughout the computation step for the number of services. Machine learning techniques such as RF can be used to determine access grants and revoke them based on the blockchain.

Random forest classification technique

IoT-based healthcare systems employ RF because they excel with mixed numerical categorical and high-dimensional data, making them suitable for flexible user access demands. In environments with frequent user behaviour changes, ensemble learning reduces over fitting. Feature relevance metrics from RF help us understand access choice criteria.

To train the data, it is necessary to gather access logs from the healthcare IoT environment, which record both authorized and unauthorized attempts to enter the system. Next, the dataset is prepared to deal with missing values and normalize features. Then, it is separated into training and testing sets to evaluate the model on unseen data. The classifier is trained to generalize and make correct predictions on future requests by learning patterns associated with successful access requests using the RF method.

Feature selection

Information like user role, data sensitivity, historical access habits, and contextual factors like time and place are key to access control decisions. Features are selected to detect these factors. Both recursive feature removal and the RF model's feature relevance ranking reduce the number of features that affect classifier prediction performance. This keeps the model efficient and understandable without over fitting.

Optimisation of classifier parameters

Parameter tuning adjusts the RF classifier's hyper parameters, including the number of trees, maximum depth, and minimum samples for splitting nodes. To ensure the model works optimally on the validation set, grid search and cross-validation are used to evaluate parameter combinations. The security framework's effectiveness improves by tweaking the classifier's distinction between allowed and unauthorized access attempts.

The OACS uses RF because it handles high-dimensional data well and prevents overfitting with ensemble learning. RF's many decision trees improve anticipated performance and provide reliable access request evaluations. This precision is essential for real-time access control in IoT contexts because it permits quick and informed user rights decisions based on context and behaviour. The system's capacity to quickly process massive datasets ensures low latency and adaptability, essential for meeting healthcare applications' evolving needs.

Here, the computation states the blockchain for security. The permission is granted to the requested user and deploys the augmentation and assessment for the varying services. The security level is performed for the defendable service forwarding concerning requirements and data. The access grant and revocation are classified from this RF tree. Equation (5) considers many parameters to determine access control decisions (∂) for granting or denying access. A weighted assessment of past access grants, data sensitivity, unauthorized users, request context, and historical access trends are considered. This complete study can make healthcare systems supported by IoT secure and flexible ACM, enabling informed decision-making. Based on this, a decision is made for the defendable access control, shown in Eq. (5).

$$\partial = \begin{cases} \sum \varnothing \left(f_d * d'\right) + u_n * \left(\frac{c_r}{\frac{g_r}{(\gamma + R)}}\right) + k_h, \ Access\ grant \\ \left(\frac{\prod_{s_m} p^t}{k_h + k_0}\right) * (Y + \alpha) + \sum_{t'} \left(d' * t'\right), \ Revoke \end{cases} \tag{5}$$

The classification is performed for the varying services and determines the authorization. The authorization is given to the patients to handle the service and examine the anonymous entries and data download. The computation is based on the delegation, and the defendable service is forwarded to the end-users. This processing leads to access control and recommends R for the training data to improve the access rate. The above equation differentiates the access grant and revokes the operation for the relevant service forwarding. The first derivation indicates the access grant for the data analysis equated in Eq. (1). In this approach, the recommendation is performed for the access grant to the number of users, and it is represented as $\left(\frac{c_r}{\frac{g_r}{(\gamma + R)}}\right)$. Here, both the assessment s_m and augmentation is centralized in this IoT environment.

The second derivation represents the revoke; if any unwanted access alert is examined in IoT infrastructure, the revoke operation is performed. It is executed if an access denial occurs during the time-of-service request and forwarding. In this approach, the security level is maintained for the patients and the blockchain for the augmentation k_0. In this case, the authorization is balanced for the varying users, estimates the matching with the previous state, and provides the result on time. Figure 4 presents the classification illustration.

Sequential time observations are recorded for different access intervals in the permission-granting sequence. This sequence is observed for different classification instances for providing permission. The training is performed to verify the sequential access/grant for the users through classification (refer to Fig. 4). Thus, the

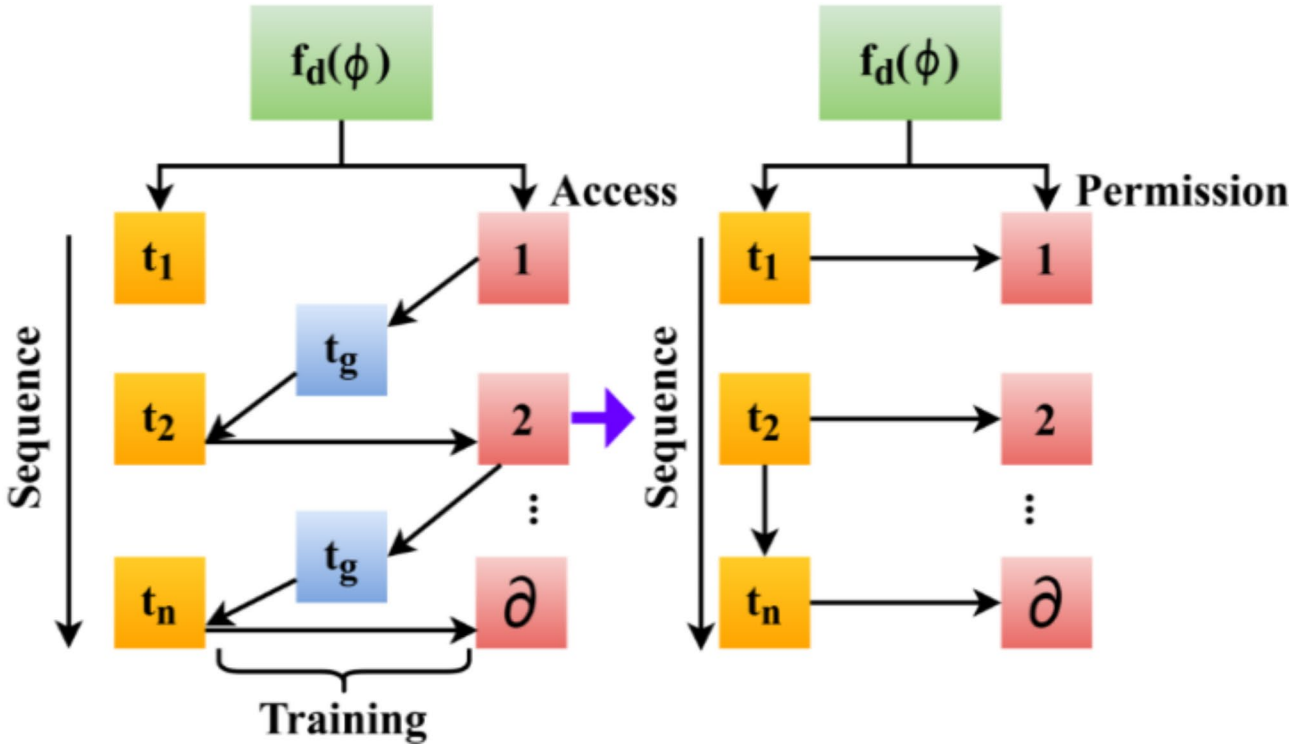

Fig. 4. RF classification illustration.

classification model is performed in this RF method for the access grant and revokes, denoted as ∂ . Equation (6) performs the training data to enhance the detection of anonymous entries and data downloads.

$$\alpha\ (t_g) = \begin{cases} \left(\frac{e_0}{\prod_{r_d}(R*d\prime)}\right) + [(k_h*t\prime) + (w_0 * d\prime)] - r_0 \\ d' = (u_0 + m_i) * s_m \\ s_m = (e_0 + o_n) * (k_h + f_d) \\ f_d = (Y + w_0) * q_e \end{cases} \tag{6}$$

The training data is done by performing matching that deploys the blockchain for reliable security. Here, security determines the service forwarding and performs the recommendation.

The error data determines a better prediction model and determines the access granted to the users. The access is granted to the appropriate user by deploying the access control. The access control states the augmentation and assessment for a reliable result. The evaluation is carried out for the different service handling and provides the access grant to the relevant users. The previous state defines the training data t_g for the different sets of services, and it is represented as r_0. Thus, the training data determines the authorization for the service handling and provides security. The prediction is evaluated based on the RF classification and deploys the concord patient/user-related service. In Table 2, the failure % for different user requests is tabulated.

Failure is computed for different granted requests, regardless of their pending status. In this case, the failure is estimated ∂ using the training data.

Blockchain for access control mechanism

With blockchain technology, there is no longer any need to depend on a single authority for access control, as it offers a decentralized structure that eliminates this danger. Data integrity is ensured by the immutability of access control choices and procedures stored on the blockchain. The complete auditability and traceability of all transactions (access demand, authorization, refusal) are recorded on the blockchain. It is difficult for unauthorized individuals to manipulate access control since blockchain employs sophisticated encryption methods to secure data. At first, blockchain compiles information about access requests, such as the user's role, the data type requested, the time of access, the location, the security of the device, and access trends of the past. With the use of access control history data, an RF model can be trained. Each data point comes with the above attributes and the matching access decision. Extract the pertinent features and feed them into the trained RF model whenever a new access request is submitted. The model can determine if the access request should be approved or denied by analysing the features provided. Ensure everyone can see the model's reasoning and choice on the blockchain. An intelligent contract on the blockchain enforces the decision to give or refuse access.

Utilizing blockchain technology, the system oversees the granting of access. Access grants can be revoked and determined from blockchain records based on earlier access and delegation sequences. When deciding on a blockchain, the service in charge of deployment evaluates and enhances the end-user access policies. Assessing the demand and utilizing the blockchain for security are both done here. Security is the decision-making process followed by defendable access control and deployable blockchain. To further guarantee security, blockchain also suggests analyzing the training stage of data processing for this scheme and looking at the access-level security of the blockchain recommendation. Various services and extensive data exchange are compatible with the current security configuration.

Every node in the network is vital in an OACS or other blockchain-based access control system because it manages state transitions associated with user permissions and access requests. Common tasks include representing states, transitioning between states, verifying user credentials against stored states, determining whether access should be provided based on current permissions and delegation history, and updating the state to reflect changes in permissions.

In the consensus mechanism, nodes talk to each other until they agree on the status of the current permissions. That way, nobody can alter the record of user permissions without authorization, and all the nodes will have the same record. Every time someone asks for access and the blockchain decides to approve or deny that request, it's recorded as a transaction. As a result, an auditable, immutable log is created.

The OACS class creates a blockchain for access requests and an index for user permissions. Request Access checks a user's blockchain delegation history for validity. It considers the user's credentials and past behaviour to determine resource access. If so, it grants or forbids access. Grant Access and deny Access record every choice as a blockchain transaction.

User Requests	Granted	Revoked	Failure (%)
20	18	0	0
40	36	3	0
60	52	5	1.8
80	74	7	2.5
100	91	9	3.9
120	109	10	3.4

Table 2. Failure % for user requests.

Inputs:

userID: Identifier for the requesting user.

resourceID: Identifier for the requested resource.

Outputs:

Access granted or denied message.

Procedure

1. **Initialize** (user id, resource id)

   Blockchain = []

   User Permissions = {}

2. **Request** Access (user ID, resource ID)

   if validate User(user ID)

   Delegation History = query Blockchain (user ID, resource ID)

   if check Access(user ID, resource ID, delegation History)

   Grant Access (user ID, resource ID)

   else

   Deny Access (user ID, resource ID)

3. Grant Access (user ID, resource ID)
4. Log Transaction (user ID, resource ID, "grant")
5. Deny Access (user ID, resource ID)
6. Log Transaction (user ID, resource ID, "deny")

End

Algorithm 1. Pseudocode of blockchain-based access control.

The training is based on previous blockchain information and prediction; prediction is discussed in the following section.

Security prediction

The security prediction is performed based on matching the previous state and provides a reliable result. Here, the recommendation is made for the blockchain to ensure security. The permission is forwarded concerning the relevant information handling to the end-user in IoT. The utilization of the recent IoT for ubiquitous and concord patients is examined in the healthcare industry. Access-level security is determined to grant permission to access the services. Concerning this prediction, the upcoming anonymous entries are avoided, and the efficient access rate is explored. Equation (7) is used to predict the varying services, and here, matching is done with the previous state.

$$P = \left(\frac{S * H}{(w_0 + k_h) \Big/ g_r} \right) + \prod_{d\prime}^{l_a} (r_d * \varnothing) + \left[\left(\frac{k_0 - R}{c_r} \right) * (f_d - e_n) \right] - r_0 \tag{7}$$

The prediction is performed by examining the service's current and previous state in the healthcare industry. Here, the evaluation is done by deploying the defendable access control and providing permission for the delegate services.

The end-user requests the particular services, so the healthcare industry performs the mapping. This mapping matches the current and previous data states and forwards the relevant data to the end user. In this stage, the recommendation is made for access control and augmentation, and it is formulated as $\left[\left(\frac{k_0 - R}{c_r} \right) * (f_d - e_n) \right]$. Here, the defendable process examines the security between the users and the devices. The analysis of anonymous entries and data downloads states the permission provided to the user. The computation time is included to perform the particular task and, from this prediction, is examined, and it is denoted as P. The delegation scheme deploys interrupt-free healthcare record access, as shown in Eq. (8).

$$\gamma\left(d'\right) = (j_c{*}e_0) + \left[\left(\frac{\sum_{m_i}(u_0 + t\prime)}{H + q_e}\right){*}k_h\right] + (k_0{*}s_m) + o_n(\gamma) \tag{8}$$

In Eq. (8), the interrupt-free healthcare record access determines the access grant for the end users. The evaluation is carried out for the varying service handling, examines the augmentation and assessment, and deploys the delegated. The previous state performs the matching, and from this approach, permission is granted to revoke the services. Here, the recommendation is made to provide access control and deploy the defendable access control. The evaluation is done by deploying the access to the end user and determining the blockchain record based on the previous state and delegation sequences. The access control is forwarded to the secure user in the network and balances the security for the access level.

The analysis is done by determining the delegation scheme, examining the access control, and providing the authorization, and it is denoted as j_c. The data forwarding is done securely in the centralized IoT augmentation and assessment, providing post-to-healthcare record access. The evaluation is done by deploying the permission to the repository and estimating the reliable processing for the delegation scheme. This delegation scheme includes the augmentation and assessment for healthcare record access in IoT. Thus, authorization is performed for the varying services in the environment. In this evaluation, the interrupt-free healthcare record access is determined, and from this blockchain, the recommendation is formulated in Eq. (9).

$$k_h(R) = (c_r + t\prime) * \left(\frac{H * e_n}{\sum_{g_r}(d' + e_0)}\right) + [q_e(m_i) * o_n] + \left(\frac{j_c + w_0}{\partial / S}\right) \tag{9}$$

The blockchain recommendation analyzes this scheme's training state of data processing using Eq. (6). The performance is used to state the authorization of service forwarding from one state to another. Figure 5 presents the recommendation process.

The recommendation process relies on matching updates after the request processing. In this process, the classified intervals are used for decision-making. Blockchain records are used for information updates and access to information storage. This is replicated in the services provided by the healthcare industry for retaining service-level security (refer to Fig. 5). In the healthcare industry, computation leads to examining the security and balances throughout the iteration steps. In the IoT healthcare industry, service delegation is performed to determine the security and access grant. The access grant to the user states the augmentation and assessment. It is a pre-defined term that holds the number of user access, and from this, the service is forwarded to the appropriate user by matching. From this, forwarding is done based on the classification method, and it is represented as $\left(\frac{j_c + w_0}{\partial / S}\right)$. The determination of access and denial is formulated in Eq. (10), which examines Eq. (5), which indicates the classification model.

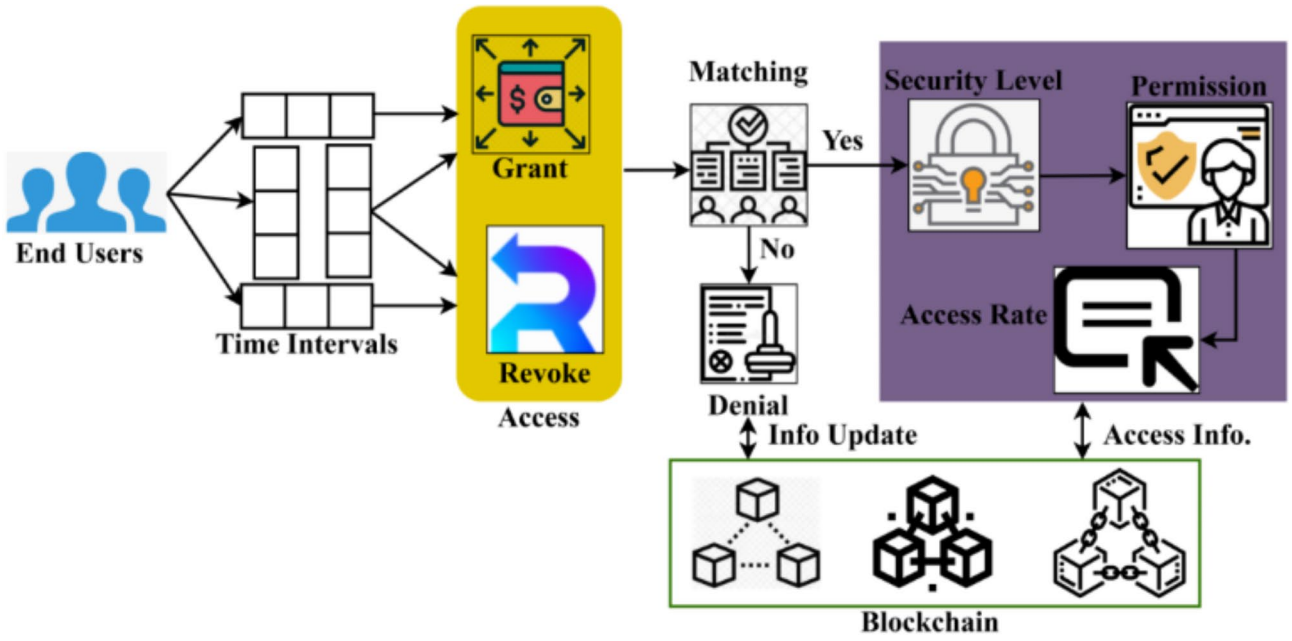

Fig. 5. Blockchain recommendation process.

$$\emptyset\left(S,n'\right)=\begin{cases}\left(Y+q_e\right)*\sum_{r_0}\left(e_0+w_0\right)+\left(\frac{e_0-f'/v_k}{k_h}\right)\\ f'=\left(l_a{}^*c_r\right)+r_0\\ r_0=P+\left(\Delta\left(c'\right)*m_i\right)\\ m_i=r_0\left(e_0\right)*t'+w_0\end{cases}\tag{10}$$

The determination is carried out for the access and denial in service forwarding. From this approach, blockchain is used to define user permission. Concerning user permission, anonymous entries and data downloads are used to state the security. The security of the user and the devices in IoT is balanced. Here, the computation matches the current and the previous state and provides the result. The derivation is performed based on the user's requirement and grants access on time. The access control and granting permission to use the service is termed from the authorization. The service authorization leads to examining the augmentation and assessment of the upcoming data handling in the healthcare centre. Table 3 presents the request examination for different delegation factors.

The examination factor is high if the matching is high, whereas complexity is less. If the matching is high, it reduces the denial ratio, and hence the examination is high. The examinations are performed based on P and interrupt free access delegations. Therefore, the access rate is high, reducing the denial, as shown in Table 3.

Access and denial are performed concerning the failure in the process, and it is termed as $f\prime$. The denial is made by determining the matching process with the requirement and defining the delegation for access control. The prediction is made by determining the previous state of action and deploying the revoke and access grant. The access grant is used to state the matching Δ and decrease the denial of service, and it is denoted as $n\prime$. Thus, determining access control and denial is performed by decreasing the failure in networking healthcare data transmission. Equation (11) evaluates the access rate and shows better improvement.

$$\beta\ =k_h\left(Y\right)*\left(\partial\ +\frac{l_a}{o_n}\right)+\left(e_n+u_n\right)q_e-r_0\tag{11}$$

The access rate is enhanced in this approach by decreasing the failure and defining the defendable access control scheme. The delegation of service determines the authorization by concerning the service to the requested user on time. The computation time is reduced in this processing, and permission is provided to secure users from this state. The security level is maintained for the varying users and the services based on the requirement, and it is equated as $\left(e_n+u_n\right)q_e$. The evaluation β is done to prevent anonymous entry into IoT and access to improper records. The matching process is derived in Eq. (12), which indicates the prediction model for the current and previous processing state.

$$\Delta\ =d'\ \left(e_0\right)*\left(f_d+\frac{S*l_a}{t_g}\right)+\left[\sum\ \left(v_k*c'\right)-r_0\right]+P\tag{12}$$

The matching is performed with the previous access and delegation sequences for the number of services. The evaluation is used to deploy the anonymous detection and provides the evaluation for the access control. The access control determines the dependable services and provides the recommendation process. The recommendation defines the permission for the current and the previous state and provides the result based on the matching. For every computation step, matching examines the defendable access control. In this case, the access grant and revoke are used to determine the blockchain for security. Equation (13) performs access-level security to decrease the false rate.

$$S\left(\alpha\right)=\frac{1}{u_n+e_n}*q_e\left[\left(w_0+u_0\right)+t_g*\left(P+\Delta\right)\right]+g_r\left(e_0+H\left(u_0\right)\right)\tag{13}$$

The above equation explores access-level security in the blockchain recommendation to ensure security. The security level is balanced for the varying services and ubiquitous information sharing. The defendable access control determines the augmentation and assessment. The computation deploys the authorized access level to the secure user to maintain the related service forwarding. In this state, the false rate decreases for the varying services users request. It is achieved using an OACS and RF classification to address the issues and ensure security. Machine learning deploys training data in the IoT-based healthcare industry and transmits relevant services to patients with less computation time.

Delegation Factor	Matching Factor	Complexity (ms)	Denial (%)	Examination
0.2	0.44	56.3	11.39	0.61
0.4	0.52	45.27	9.61	0.78
0.6	0.69	39.26	8.45	0.81
0.8	0.85	21.48	6.39	0.95
1	0.91	17.81	4.1	1

Table 3. Examination for delegation factor.

Figure 6a analyzes the access grant and request examination factors under different training instances. As the training instances vary, the learning is instigated based on classification. This identifies the grant and revokes cases for requests in the succeeding intervals. Therefore, the examination is performed for previous intervals and stored in the blockchain for further delegation. This improves the access rate for the examined requests, preventing interruptions. Based on the stored information, the interrupt-causing requests are identified. The identified users are denied new service provisioning, and the current requests are revoked. This ensures secure and liable healthcare data sharing between the devices under different training instances, as shown in Fig. 6b.

Performance analysis

The proposed scheme's performance has been empirically analyzed and evaluated using the OMNeT + + simulator[44]. To simulate ACM, blockchain integration, consensus algorithms, etc., the authors must develop custom models and modules or leverage third-party libraries/frameworks designed for simulating blockchain systems. The purpose of developing network simulators, OMNeT + + provides a framework and library for C + + simulations that are extendable, modular, and component-based. To demonstrate how the network members would interact and sync information, this study uses an OMNeT + + simulation to build the simplest version of the OACS. It then shows how interrupt-free healthcare record access to precise users would work. OMNeT + + provides a graphical runtime environment, an integrated development environment (IDE) based on Eclipse, and many more tools. Among the many available extensions are those that facilitate real-time simulation, network emulation, database integration, and System C integration. Researchers worldwide have contributed many simulation models and model frameworks to OMNeT + + throughout its availability.

Many different parts of a blockchain system, including nodes, transactions, consensus techniques, and protocols for network communication, can be modelled in OMNeT++. The proposed model utilizes the INET framework.

INET framework: One of the most well-known simulation libraries for the OMNeT + + discrete-event modelling environment is the INET framework. This framework simulates communication networks, especially ones that use blockchain technology. With IoT healthcare services as an example, there are several benefits to using the INET framework in blockchain-related simulations. The well-known modular design of OMNeT + + is the foundation upon which INET is based. We can expand and personalize simulations to incorporate particular blockchain protocols and healthcare IoT-related scenarios. Complex systems like blockchain networks, OMNeT++, and INET offer strong visualization and debugging capabilities crucial for understanding their behaviour. For healthcare IoT blockchain solutions to work, there must be enough capacity to handle many devices and users. As a result of INET, blockchain applications may be tested for scalability and performance under varying network loads and situations. The fault endurance of blockchain systems must be evaluated. To ensure the blockchain is resilient, INET can mimic network outages, node crashes, and other failure scenarios.

The experiment contains 23 user equipment generating 130 requests. The data is collected from the Best Electronic Health Record Datasets, Databases & APIs[45]. Four healthcare data servers with 61,067 user data records (replicated) are used in this scenario. The access interval is set to 10 so that minimum failures are targeted. This basic consideration is applied in simulator[46] to develop the introduced system. The performance metrics false and access rate, access and processing time, and failures are considered for analysis. The methods TLE-FGAC[29], EMC[27], and LSAS[28] from the related works section are augmented for a comparative analysis. Table 4 provides a detailed overview of the experimental setup.

Based on the implemented access control scheme, classification based on RF is utilized to identify failure and analyze MTBF.

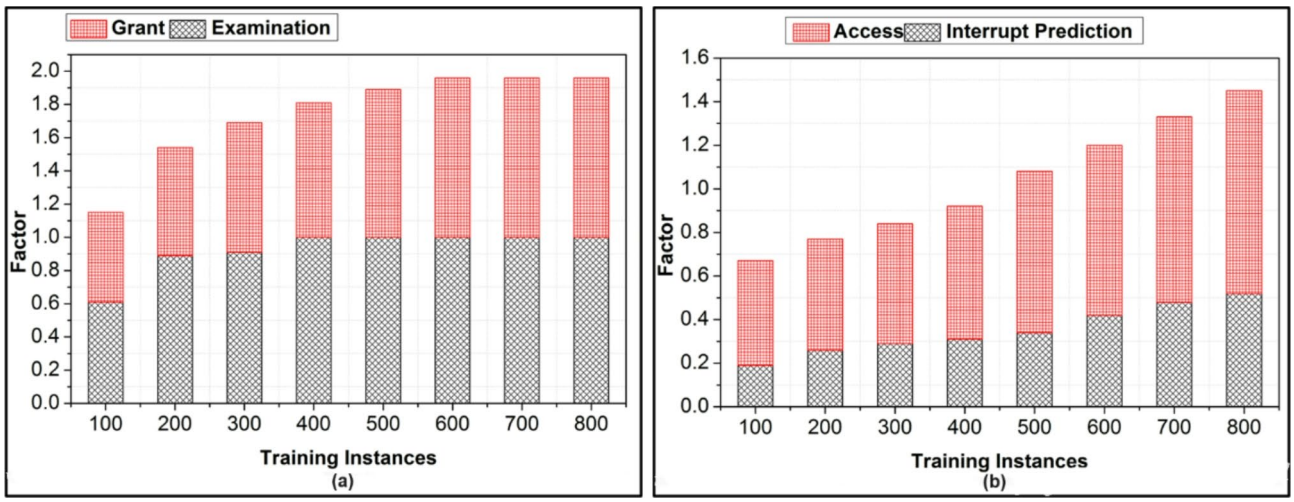

Fig. 6. (**a**) Grant and examination factor analysis (**b**) Access and interrupt factor analysis.

Component	Specification
Processor	Intel Core i7
Memory (RAM)	32 GB
Storage	500 GB SSD
Power Supply	650 W
Network Interface	Wi-Fi 6
Operating System	Windows 11
Simulator	OMNeT + + 6.0.1
Programming Language	Python 3.8+
Transaction Rate	10–100 transactions per second
Network Topology	Star topology for IoT device communication
Simulation Duration	1000 s
Network Configuration	Wireless Body Area Network (WBAN) with 100 nodes

Table 4. Experimental setup and configuration for performance analysis.

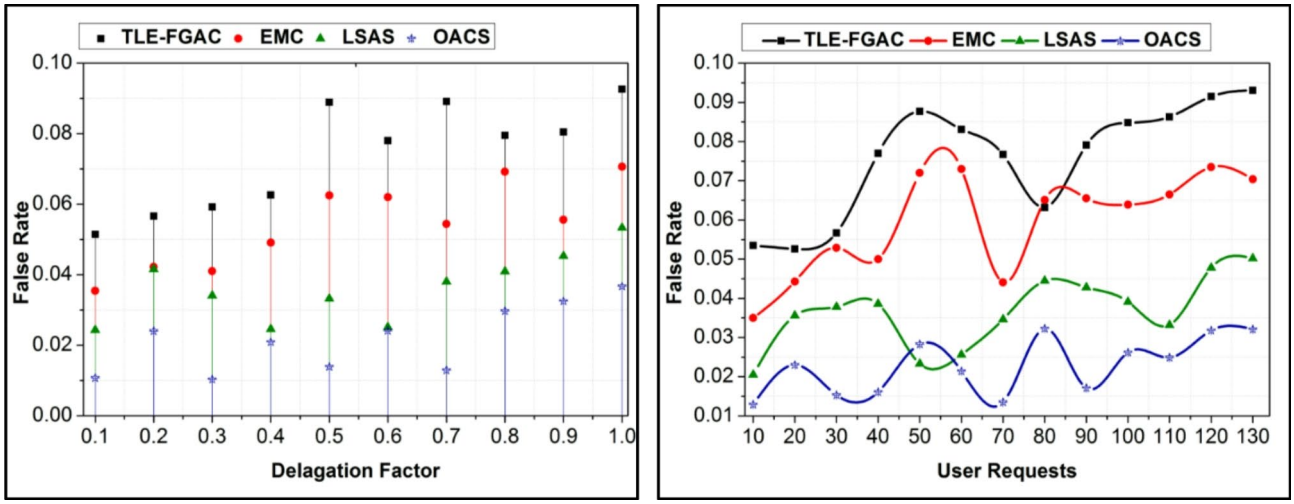

Fig. 7. False rate analysis.

False rate

$$FR = (Failed\ Access\ Requests)/(Total\ Access\ Requests) \times 100 \tag{14}$$

A system's FPR in Eq. (14) is the percentage of valid access requests that are mistakenly rejected. Figure 7 presents the false rate analysis for the delegation factor and user requests with the existing methods. The proposed scheme initiates an anonymous entry check before delegating access permissions. This is performed using user identity and previous history stored in the blockchain. The further processes are validated based on two assessments, namely ∂ and $\gamma\ (d')$. Therefore, the adversary inclusion and false request processing are denied in the Y administration, reducing the false rate, as shown in Fig. 7.

Access rate

$$AR = \frac{Sucessfull\ Access\ Requests}{Total\ Access\ Requests} \times\ 100 \tag{15}$$

The access rate is defined in Eq. (15). The proposed scheme achieves a high access rate for different requests. The processing is first analyzed for $(m_i + r_0)$ preventing anonymity. This information is matched with the available blockchain information for identifying Y and $\varnothing\ (S, n')$. Access delegation and revocation are consistently performed based on $(u_0 + m_i)$ and $(Y + w_0)$. Therefore, the prediction for unavailability and secure access is determined. Based on this P, the healthcare records are mapped with the requests. This enhances the continuity between users and application services without denial. Contrarily, $\gamma\ (d')$ analysis identifies certain false or unattended requests mitigated by the communication sessions. Retaining the service sessions, the user requests are fed to different sessions, providing access to healthcare data. Based on the access rate, further allocations are planned with t_n and its pursuing sequence. This improves the request handling rate, and access is improved

without denials. The matching process further scrutinizes the request count to retain the security level, and hence $S(\alpha)$ is unanimous for all the requests. Therefore, the access rate is improved for different user requests, as presented in Fig. 8.

Access time

$$AT = T_{response} - T_{request} \tag{16}$$

As shown in Eq. (16), where $T_{response}$ is the timestamp at which the system gives a response (approval or denial) after finishing processing the request for access and $T_{request}$ denotes the timestamp when the user initiates the access requests. A comparative analysis of access time (AT) for different user requests is presented in Fig. 9. AT is predicted based on incoming and pursuing resource delegations. AT equation refers to the system's processing time and response to an access request. At different intervals, the anonymity is mitigated at the initial step, confining the wait time for different requests. In pursuing access requests, ∂ is validated in $(d' * t')$ Intervals, preventing the revocation of timed requests. The process is pursued in different training instances, and the information $\gamma\ (d')$ and $o_n(\gamma)$ is used for validating different requests. The recommendation process is pursued at different intervals through access and denial classification. Classification learning relies on training data to predict instances of failure. Such instances are mitigated using training data, and hence, $f_d(\varnothing)$ is granted. This ensures concurrent and seamless request processing, preventing augmented queues. The proposed scheme validates interrupt-free access to retain multiple security instances and prevent failures. The failure-detained intervals improve the request processing rate, reducing the time needed to process the request. Besides, the sequential classification reduces the false requests; hence, the pursuing request is handled without additional wait time. This reduces multiple requests' AT, improving the proposed scheme's performance.

Processing time

$$Access\ Processing\ Time = Time\ of\ Access\ Response - Time\ of\ Access\ Request \tag{17}$$

Therefore, the processing time is confined to the previous intervals until t_n as in Eq. (17). Figure 10 compares the request processing time based on the delegation factor and user requests with the existing methods. The proposed scheme mitigates anonymous requests from the users at the initial stage. This prevents time for processing illegitimate requests, so the α process is uninterrupted. At this stage, the healthcare data allocation

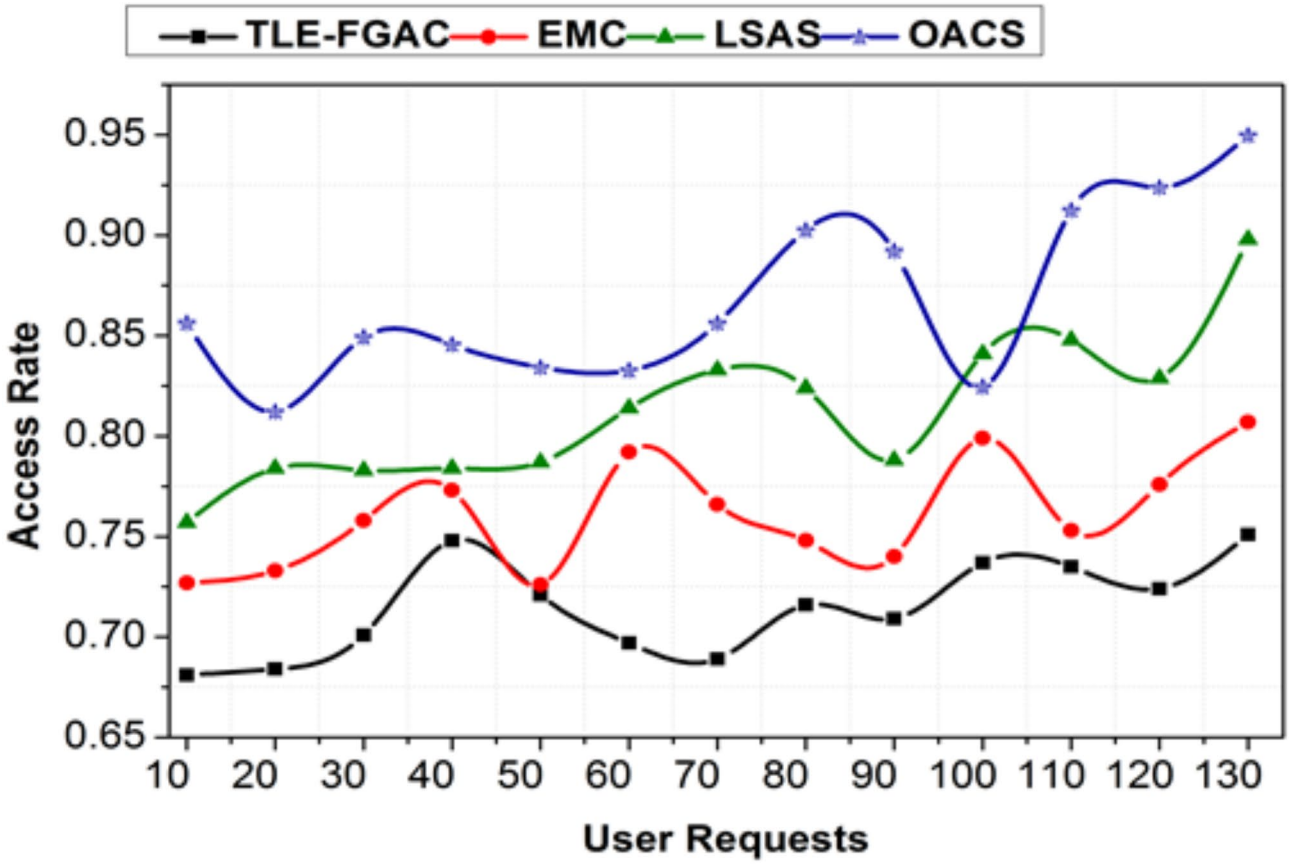

Fig. 8. Access rate analysis.

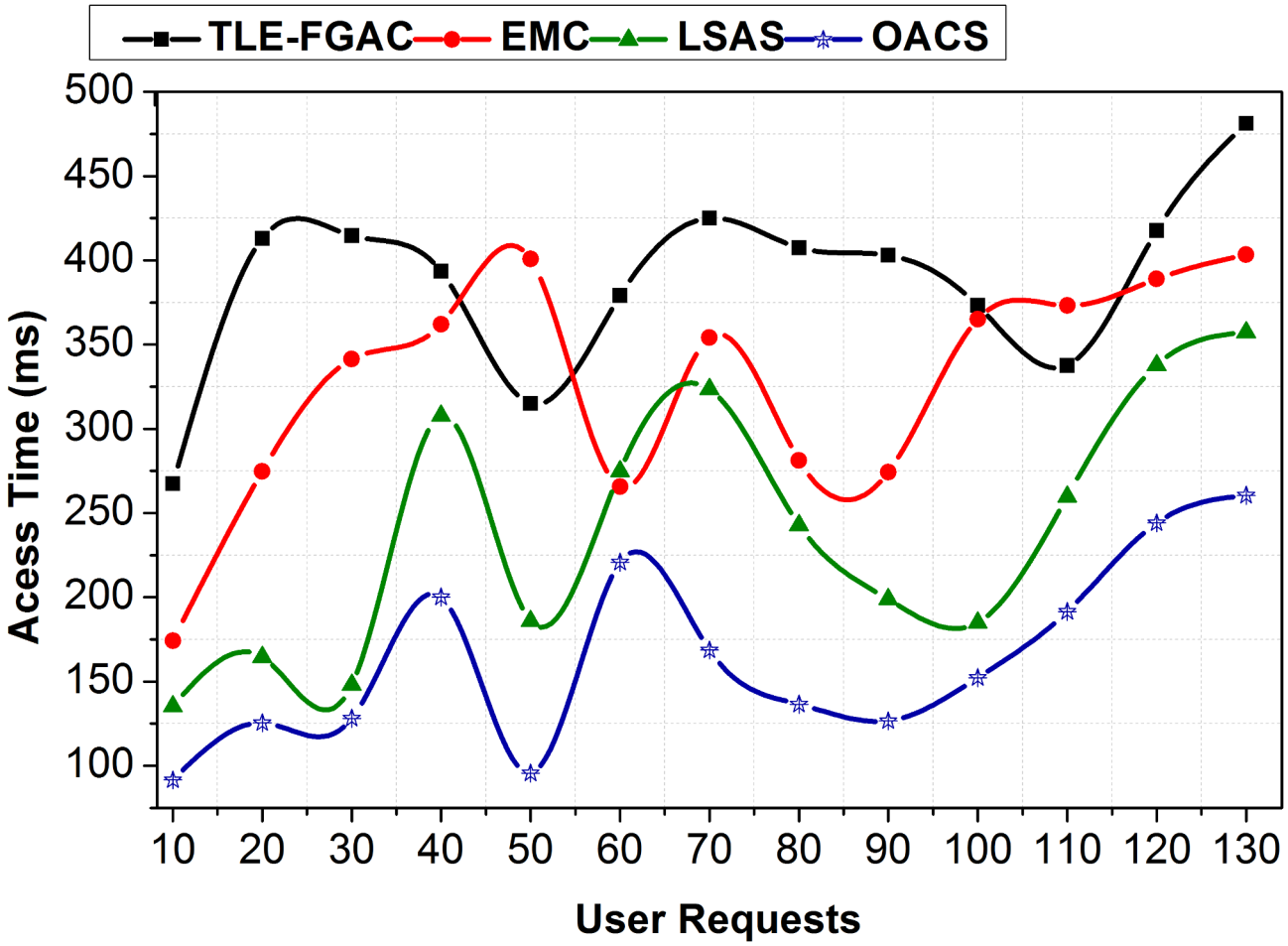

Fig. 9. Access time analysis.

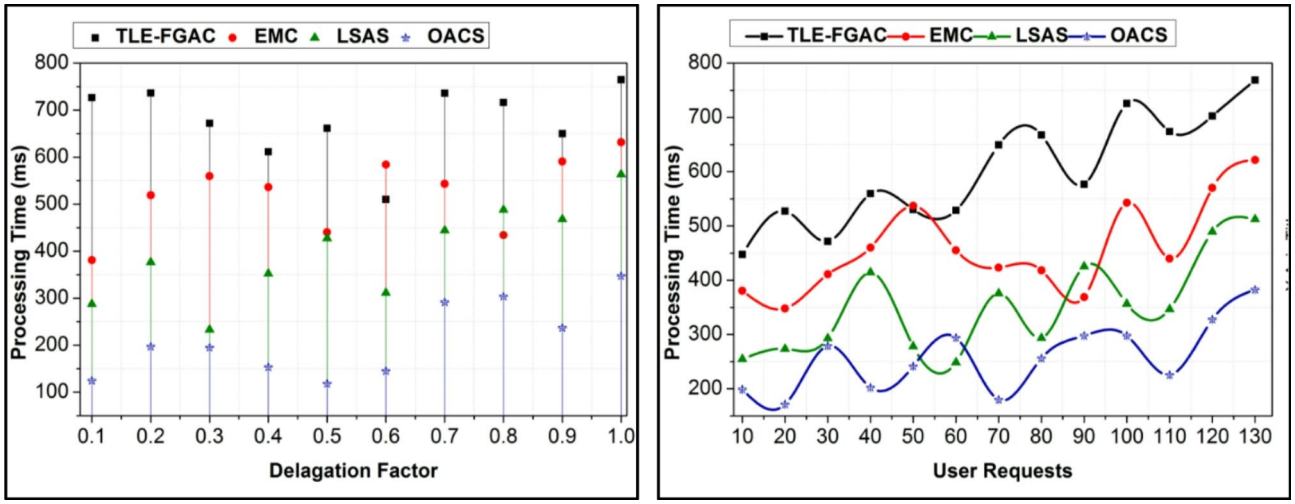

Fig. 10. Processing time analysis.

is sequential and does not require additional validation. The classification learning identifies ∂ for which the sequence is modified, and hence, interrupt-free access is provided. In multiple scenarios, the training data is used for access or denial estimation, preventing unnecessary data access. $\left(\frac{j_c+w_0}{\partial / S}\right)$ estimation ensures high-level access security for all the scrutinized requests. As the requests enter the security administration process, the consequent request is processed without additional delay. In this process, delegation is improved without additional time. The pending requests are validated based on the blockchain recommendation, as guided through Δ processes.

Failures

A comparative analysis of healthcare data access failures is presented in Fig. 11. The dense user requests increase the processing and data allocation rate regardless of different intervals. In this process, classification learning differentiates the access grant and revocation based on P. This computation aids $\gamma\ (d'\ )$ fewer recommendations for preventing access failures. From the other end, the delegation is specific over $\varnothing\ (S, n'\ )$ such that the matching instances alone deviate for further processing. Therefore, the delegations are performed for different intervals based on user requests and access rates. The proposed scheme identifies anonymity based on $f_d\ (\varnothing\ )$ and further training is ensured using classification data. This classification distinguishes the permission grant and revoking instances for which the failures are identified. The identified failing instances are categorized under anonymous access or P process, reducing permissions. Therefore, the access rate is high, preventing unnecessary denial. The proposed scheme achieves less failure by providing seamless and classified access permissions. Failure analysis with 4 existing algorithms, including ACM-low-power and lossy networks[40], confirms the superiority of the proposed OACS by providing 16 failure node count on delegation factor and 14 for each request, as depicted in Fig. 11.

Mean time between failures analysis

$$MTBF\,(\%)\ =\ Total\ Operational\ Time\ /\ Failures\ count. \tag{18}$$

Equation (18) shows the mean time between failure analysis. The system's performance needs to be evaluated for accessing IoT healthcare services. A measurement is the mean time between two consecutive system failures in identifying the anonymous access by distinguishing the permission grant and revoking instances for user access or the Mean Time between Failures $(MTBF)$. Quantifying the system's capacity to function continuously without experiencing malfunctions shows its dependability.

Keeping track of the system's total operational time during user request initiation and transaction of files indicates the entire time the system has been up and running without experiencing problems in computing $(MTBF)$. It is possible to determine $(MTBF)$ to assess the system's dependability quantitatively. While a lower MTBF value signifies a less reliable technology with more frequent failures, a higher $(MTBF)$ value denotes a system with longer gaps between failures, which improves the system's performance. A comparative analysis of $(MTBF)$ is presented in Fig. 12.

Time to detect replay attacks

One of the key performance indicators that can demonstrate the effectiveness of the OACS's blockchain-based access control system in preventing replay attacks is the Time to Detect Replay Attacks (TDR). A replay attack occurs when an attacker attempts to reuse a legitimate data transmission, and TDR measures how quickly the

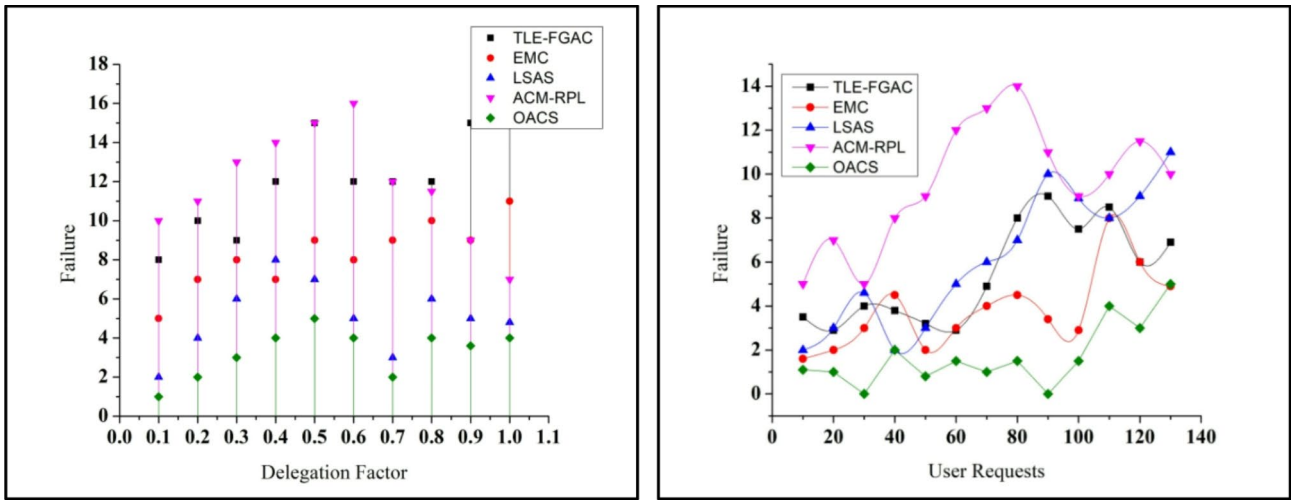

Fig. 11. Failure analysis.

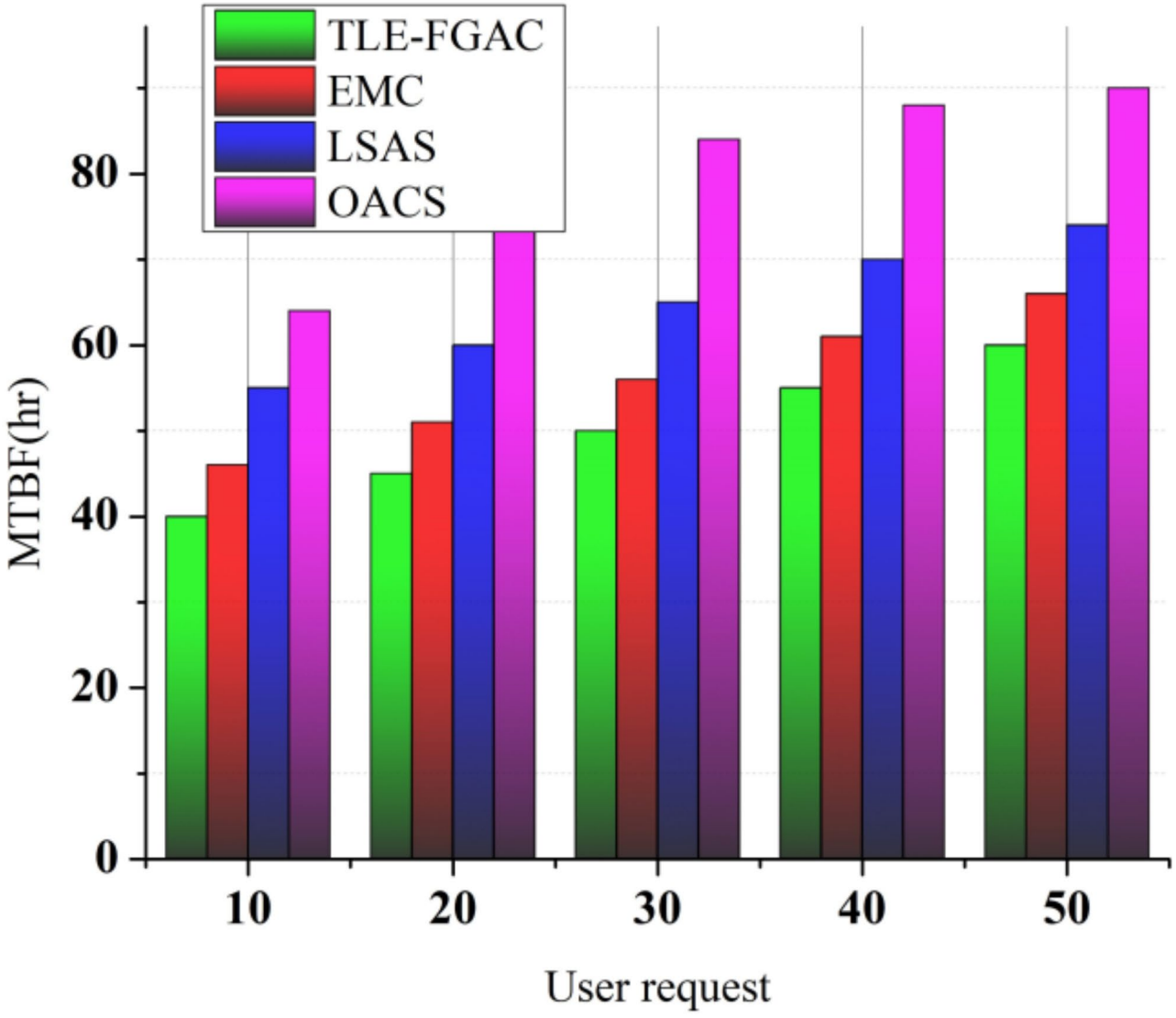

Fig. 12. System performance based on $(MTBF)$.

Method	TDR (Sec)
TLE-FGAC	1.1
EMC	0.9
LSAS	1.2
OACS	0.25

Table 5. Time to detect replay attacks.

system can identify and prevent such attempts. TDR for various methods is compared in Table 5. Compared to conventional access control models, which require 1.1 s for TDR, the OACS demonstrated an average detection time of 0.25 s in simulations using the blockchain's decentralized verification mechanism. This faster detection is attributed to the immutable nature of the blockchain, which timestamps every access request, preventing unauthorized retransmission of data. The reduced detection time significantly limits the vulnerability duration, effectively mitigating replay attacks.

Latency

Latency, a key OACS indicator, measures healthcare IoT access request processing time. Using blockchain and smart contracts to automate access control options greatly reduces validation and response times, as shown in Table 6. With the OACS's decentralized ledger, many network nodes record and validate each access attempt,

No of Users	TLE-FGAC(s)	EMC(s)	LSAS(s)	OACS(s)
100	329.54	280	255.43	150.43
200	423.53	378.65	359	204.21
300	523.53	486.5	432.54	259.43
400	694	634.53	596.53	364.30
500	894.3	725.4	649	412.31

Table 6. Latency under varying loads.

No of Users	TLE-FGAC (req/sec)	EMC (req/sec)	LSAS (req/sec)	OACS (req/sec)
100	33	35	40	66
200	56	58	60	89
300	78	85	98	143
400	95	105	163	178
500	124	156	186	220

Table 7. Throughput under varying loads.

Methods	TLE-FGAC	EMC	LSAS	OACS
False Rate	0.0931	0.0704	0.0502	0.0321
Access Rate	0.7510	0.8070	0.8980	0.9498
Access Time (ms)	481.19	403.37	357.35	260.507
Processing Time (ms)	768.9	621.68	512.36	382.498
Failure	17	12	8	5

Table 8. Comparative analysis results for average user requests.

unlike traditional models that use central servers. This setup speeds up authentication and authorization by avoiding centralized processing bottlenecks. The OACS has lower latency than TLE-FGAC, EMC, and LSAS as user numbers increase. OACS has 250 ms latency for 100 users, while TLE-FGAC, EMC, and LSAS have 600–550 ms, which shows that OACS is best for instantaneous healthcare applications. The OACS's RF algorithm improves latency by making decisions based on prior access patterns. The model optimizes latency by learning from new access requests in real time. Thus, the OACS provides a scalable solution to meet expanding access needs without losing speed or efficiency and maintains lower latency under varying user loads. The suggested model emphasizes the OACS's latency improvements, demonstrating its ability to handle high-demand healthcare contexts with fast reaction times and powerful processing capabilities.

Throughput

$$Throughput = \frac{Total\ sucessful\ Access\ requests}{Total\ Processing\ Time} \tag{19}$$

Compared to more traditional approaches, the OACS has an impressive throughput capability, meaning it can process more requests per second, as shown in Table 7. For example, the OACS keeps its throughput at 20 requests per second with 200 users, while traditional systems struggle to keep up with 8 requests per second. This distinction emphasizes how efficiently the OACS handles several concurrent access requests without noticeably lowering performance. The use of blockchain technology allows for more efficient processing and faster handling of access requests. In healthcare contexts, where quick data access is vital for patient care, these throughput figures highlight the OACS's potential to grow efficiently in scenarios with many concurrent users. The suggested model emphasizes the OACS's throughput improvements, demonstrating its ability to handle high-demand healthcare contexts with fast reaction times and powerful processing capabilities.

Comparative evaluation

Tables 8 and 9 present the comparative analysis of average user requests and delegation factors.

The proposed scheme achieves an 11.74% less false rate, 13.1% higher access rate, 12.36% less access time, 13.23% less processing time, and 9.94% less failure. Also, the OACS achieves a 10.64% less false rate, 15.62% less processing time, and 10.95% fewer failures.

The OACS analyses input variables like the delegation factor and user requests, which strongly impact access control results. Users' ability to delegate access permissions affects the system's responsiveness and flexibility,

Methods	TLE-FGAC	EMC	LSAS	OACS
False Rate	0.0926	0.0706	0.0533	0.0367
Processing Time (ms)	764.72	631.71	563.35	347.058
Failure	17	11	7	4

Table 9. Comparative analysis results for average delegation factor.

allowing authorized users to handle access in real time. The OACS has greater access rates in systems with high user interaction and clear delegation laws because its machine-learning component can dynamically alter permissions based on access patterns. The OACS can improve decision-making in settings with extensive and relevant historical data by providing quick and secure access to sensitive information and lowering the risk of unauthorized access. The OACS is flexible and performs well in healthcare IoT contexts.

Blockchain provides a safe platform for recording transactions and controlling access requests by guaranteeing data integrity, transparency, and immutability. As part of the machine learning strategy, Random Forest allows the system to analyze and forecast access patterns in real-time, making context-aware decisions and adjusting to changing user behaviours and network circumstances. This adaptive decision-making power is vital in healthcare, where strict security requirements must be balanced with the need for real-time access to medical data.

The latency study shows that the scheme can handle real-time queries in healthcare IoT settings, where delays might jeopardize important healthcare choices. Rates of false positives show how well the access control mechanism identifies valid users compared to possible attackers, which affects the scheme's dependability. By comparing processing times, this study can see that OACS can efficiently process high-frequency access requests on a broad scale. Using multi-key authentication adds another degree of security by lowering the probability of unauthorized access and increasing resistance to several attack vectors by necessitating many types of verification before allowing access. Incorporating context-aware checks makes the system even more resilient. These checks make the access control mechanism more dynamic and responsive by evaluating the user's role, device type, and AT, among other factors. Thanks to these upgrades, OACS can now easily adapt to the complicated and ever-changing healthcare IoT settings, even when various scenarios call for varying degrees of access and security.

To better handle massive datasets and frequent access requests, sharding divides the blockchain into smaller, more manageable pieces, enabling parallel processing of transactions and drastically lowering the burden on individual nodes. To overcome blockchain's storage limits, off-chain storage moves massive healthcare data sets, including patient records and sensor logs, to an external location while retaining necessary information on-chain. This keeps the blockchain lightweight. The Random Forest model is essential for access control because it examines requests using context and past patterns, including user behaviour and the request time. This paradigm allows sharding to be easily identified and allocated, and off-chain storage can be managed effectively, resulting in fewer unwanted data retrievals.

Security analysis

Improving IoT healthcare services' security, dependability, and scalability can be as simple as integrating an RF method with a blockchain that relies on an access control scheme. Some of its advantages were robustness, precise forecasting, and the ability to handle complex data. User role, request context, and previous access history are some criteria for training RF to decide whether to allow or deny access. They can flag abnormal access behaviours as potential security breaches.

The security analysis may differ from formal security analysis because it focuses on behavioural patterns and practical performance metrics like throughput, AT and FPR rather than mathematical proofs of security properties. Formal security analyses typically outline desired security outcomes (like availability, confidentiality, or integrity) and test the system's compliance using adversary models, model checking, or security games under predetermined conditions. Formal studies require additional cryptographic or theoretical proofs, but this work uses simulations and practical evaluations to demonstrate the OACS's operational effectiveness.

RF model integration with the OACS is crucial to access control decision management. The OACS framework's RF model uses critical features to inform decisions about access control in healthcare IoT settings. The specifics of feature selection are based on the user Role, which establishes permissions according to the user's position. Medical records are classified using data sensitivity criteria. Details about the request, including the context in which the data is accessed. Requests, rejections, and past access revocations are detailed in the access history. Factors influencing access permissions include the requestor's location. The level of security provided by the device being utilized for access. The security and compliance needs of healthcare settings are the primary considerations when selecting these features. RF model uses weights assigned by past data to each feature, which factor into the model's ultimate decision.

The training data comprises healthcare system access logs, including both approved and refused attempts. This data includes details regarding access patterns, past actions, and patterns of emergency access requests compared to routine access.

These varied datasets are used to train the RF to detect unusual requests and normal access behaviours. The model learns from authorized and unauthorized attempts using a decision tree-based technique to generalize patterns in access requests.

The model uses these methods to avoid over fitting and adapt to new access patterns:

(1) Retraining the RF model with new access data is regular. Retraining ensures the model can adapt to new user roles, security threats, and healthcare IoT device kinds.
(2) Ensemble learning with many decision trees prevents the RF from becoming too dependent on one path. Train each tree on a randomly selected sample of data to reduce bias and ensure the model covers all access scenarios.
(3) To handle dynamic access requests, the system monitors new ones and compares them to trends. The model can prevent illegal access by identifying questionable activity for further inspection, such as a request outside work hours. New patterns allow the model to update its categorization criteria in real-time constantly.
(4) The OACS's RF model may provide flexible and dependable access control without over fitting to old or infrequent access patterns using these methods.

The security level is executed to address needs and data for defendable service forwarding. RF tree is used to classify the access grant and revocation. We decide on the defendable access control based on Eq. (5). Authorization is determined by classifying the various services. Patients have permission to use the service, view the anonymous submissions and download data. IoT healthcare services employ an RF model for access request classification rather than interacting with users directly. This means that different aspects of each access request are considered to decide whether to approve or reject the request. The analysis is carried out for the secure sharing of service to the appropriate user in IoT, and based on this, relevant service is determined. The anonymous entries and data download are defined, and the access-level security is stated.

Conclusion

The research presented an OACS, which uses a mix of blockchain and machine learning techniques to efficiently and securely improve healthcare IoT system performance and safety. Utilising blockchain and machine learning, the OACS improves security and access management. Scalability and latency are issues, especially with frequent access requests. The system employs RF to avoid latency by making real-time access decisions based on user behaviour and access history. Although consensus delays may occur, blockchain technology ensures safe and tamper-proof state changes. Enhancing blockchain consensus processes, storing frequently requested data, and parallel processing can reduce high-frequency access requests and maintain system responsiveness during heavy loads. Compared to more conventional access control forms, the primary results show that the OACS considerably reduces processing times and false-positive rates. The system allows users access to resources according to their requirements while ensuring their safety through analytics on user behaviour and dynamic delegation histories. These findings have important real-world consequences; the OACS provides a solid foundation for controlling who has access to private healthcare records, which speeds up responses to patients' demands while keeping their information secure. The proposed technique achieves an 11.74% lower false rate, 13.1% higher access rate, 12.36% faster access, 13.23% faster processing, and a 9.94% lower failure rate. The OACS also reduces the false rate by 10.64%, the processing time by 15.62%, and the failure rate by 10.95%. The suggested remedy, though, does have its restrictions. As the number of devices and users grows, the reliance on simulated performance measures could not adequately portray the intricacies of real-world IoT environments. Additionally, the scalability of the blockchain component could provide issues. Furthermore, constant retraining and adaptation to changing access patterns are required since machine learning models can overfit past data. To overcome these limitations, future studies should evaluate the OACS's performance in various healthcare contexts through rigorous real-world testing. It is possible to increase the system's resilience by looking into different machine-learning approaches and ways to make the blockchain more scalable.

Data availability

Data is publicly available at EHR Data: Find Electronic Health Records & Datasets | Datarade, (n.d.). https://datarade.ai/data-categories/electronic-health-record-ehr-data.

Received: 2 September 2024; Accepted: 17 February 2025
Published online: 04 March 2025

References

1. ElRahman, S. A. & Alluhaidan, A. S. Blockchain technology and IoT-edge framework for sharing healthcare services. *Soft Comput.* **25**, 13753–13777 (2021).
2. Ullah, A. et al. Secure healthcare data aggregation and transmission in IoT—a survey. *IEEE Access.* **9**, 16849–16865 (2021).
3. Arul, R. et al. IoT-enabled healthcare systems using block chain-dependent adaptable services. *Pers. Ubiquitous Comput.* **28**, 43–57 (2024).
4. Alserhani, F. M. Integrating deep learning and metaheuristics algorithms for blockchain-based reassurance data management in the detection of malicious IoT nodes. Peer-to-peer netw. *Appl* https://doi.org/10.1007/s12083-024-01786-9 (2024).
5. Li, W. et al. A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system. *Mob. Netw. Appl.* **26**, 234–252 (2021).
6. Pradhan, B., Bhattacharyya, S. & Pal, K. IoT-based applications in healthcare devices. *J. Healthc. Eng.* (2021). (2021).
7. Almaghrabi, N. S. & Bugis, B. A. Patient confidentiality of electronic health records: A recent review of the Saudi literature. *Dr Sulaiman Al Habib Med. J.* **4**, 126–135 (2022).
8. Keshta, I. & Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inf. J.* **22**, 177–183 (2021).
9. Zarour, M. et al. Ensuring data integrity of healthcare information in the era of digital health. *Healthc. Technol. Lett.* **8**, 66–77 (2021).
10. He, Y., Aliyu, A., Evans, M. & Luo, C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *J. Med. Internet Res.* **23**, 1–18 (2021).
11. Rupanetti, D. & Kaabouch, N. Combining edge computing-assisted internet of things security with artificial intelligence: Applications, challenges, and opportunities. *Appl. Sci.* **14** (2024). https://doi.org/10.3390/app14167104

12. Butpheng, C., Yeh, K. H. & Xiong, H. Security and privacy in IoT-cloud-based e-health systems-A comprehensive review. *Symmetry (Basel)*. **12**, 1–35 (2020).
13. Andreas, A. et al. Towards an optimized security approach to IoT devices with confidential healthcare data exchange. *Multimed. Tools Appl.* **80**, 31435–31449 (2021).
14. Benil, T. & Jasper, J. Cloud based security on outsourcing using blockchain in E-health systems. *Comput. Netw.* **178**, 107344 (2020).
15. Alghofaili, Y. & Rassam, M. A. A Trust Management Model for IoT devices and services based on the Multi-criteria decision-making approach and deep long short-term memory technique. *Sensors* **22**, 634 (2022).
16. Tariq, N., Qamar, A., Asim, M. & Khan, F. A. Blockchain and smart healthcare security: A survey. *Procedia Comput. Sci.* **175**, 615–620 (2020).
17. Edemacu, K., Jang, B. & Kim, J. W. Collaborative Ehealth privacy and security: An Access control with attribute revocation based on OBDD Access structure. *IEEE J. Biomed. Heal Inf.* **24**, 2960–2972 (2020).
18. Jin, H., Luo, Y., Li, P. & Mathew, J. A. Review of secure and privacy-preserving medical data sharing. *IEEE Access.* **7**, 61656–61669 (2019).
19. Sharma, A. & Kaur, P. Tamper-proof multitenant data storage using blockchain. *Peer-to-peer Netw. Appl.* https://doi.org/10.1007/s12083-022-01410-8 (2022).
20. Abou-Nassar, E. M. et al. DITrust Chain: Towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE Access.* **8**, 111223–111238 (2020).
21. Tall, A. M. & Zou, C. C. A framework for attribute-based access control in processing big data with multiple sensitivities. *Appl. Sci.* **13**, (2023).
22. Xu, J. et al. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system. *Futur. Gener. Comput. Syst.* **108**, 1287–1296 (2020).
23. Nasr Esfahani, M., Shahgholi Ghahfarokhi, B. & Etemadi Borujeni, S. End-to-end privacy preserving scheme for IoT-based healthcare systems. *Wirel. Netw.* **27**, 4009–4037 (2021).
24. Li, C. T., Shih, D. H., Wang, C. C., Chen, C. L. & Lee, C. C. A blockchain based data aggregation and group authentication scheme for electronic medical system. *IEEE Access.* **8**, 173904–173917 (2020).
25. Son, S. et al. Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain. *IEEE Access.* **8**, 192177–192191 (2020).
26. Singh, A. & Chatterjee, K. Trust based access control model for securing electronic healthcare system. *J. Ambient Intell. Humaniz. Comput.* **10**, 4547–4565 (2019).
27. Akkaoui, R., Hei, X., Cheng, W. & EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange. *IEEE Access.* **8**, 113467–113486 (2020).
28. Masud, M., Gaba, G. S., Choudhary, K., Alroobaea, R. & Hossain, M. S. A robust and lightweight secure access scheme for cloud based E-healthcare services. *Peer-to-Peer Netw. Appl.* **14**, 3043–3057 (2021).
29. Zhang, W., Lin, Y., Wu, J. & Zhou, T. Inference attack-resistant E-healthcare cloud system with fine-grained access control. *IEEE Trans. Serv. Comput.* **14**, 167–178 (2021).
30. Shukla, S., Thakur, S., Hussain, S., Breslin, J. G. & Jameel, S. M. Identification and authentication in Healthcare Internet-of-things using Integrated Fog Computing based Blockchain Model. *Internet Things (Netherlands)*. **15**, 100422 (2021).
31. Shen, J., Yang, H., Wang, A., Zhou, T. & Wang, C. Lightweight authentication and matrix-based key agreement scheme for healthcare in fog computing. *Peer-to-Peer Netw. Appl.* **12**, 924–933 (2019).
32. Sarosh, P., Parah, S. A., Bhat, G. M. & Muhammad, K. A security management framework for big data in smart healthcare. *Big Data Res.* **25**, 100225 (2021).
33. Hathaliya, J. J., Tanwar, S. & Evans, R. Securing electronic healthcare records: A mobile-based biometric authentication approach. *J. Inf. Secur. Appl.* **53**, 102528 (2020).
34. Su, Q., Zhang, R., Xue, R. & Li, P. Revocable attribute-based signature for Blockchain-based Healthcare System. *IEEE Access.* **8**, 127884–127896 (2020).
35. Mohammad Hossein, K., Esmaeili, M. E., Dargahi, T., Khonsari, A. & Conti, M. BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. *Comput. Commun.* **180**, 31–47 (2021).
36. Tolba, A. & Al-Makhadmeh, Z. Predictive data analysis approach for securing medical data in smart grid healthcare systems. *Futur. Gener. Comput. Syst.* **117**, 87–96 (2021).
37. Liu, H., Crespo, R. G. & Martínez, O. S. Enhancing privacy and data security across healthcare applications using Blockchain and distributed ledger concepts. *Healthc* **8**, (2020).
38. Wu, G., Wang, S., Ning, Z. & Zhu, B. Privacy-preserved Electronic Medical Record exchanging and sharing: A blockchain-based Smart Healthcare System. *IEEE J. Biomed. Heal Inf.* **26**, 1917–1927 (2022).
39. Rani, P., Kaur, P., Jain, V., Shokeen, J. & Nain, S. Blockchain-based IoT enabled health monitoring system. *J. Supercomput.* **78**, 17284–17308 (2022).
40. Sapna, G. S. & Revanna, S. D. An efficient internet of things interoperability model using Secure Access Control mechanism. *Int. J. Intell. Eng. Syst.* **16**, 41–56 (2023).
41. Ghaffar, Z. et al. A machine learning attack resilient and low-latency authentication Scheme for AI-Driven Patient Health Monitoring System. *IEEE Commun. Stand. Mag.* **8**, 36–42 (2024).
42. Mahmood, K. et al. Cloud-assisted secure and cost-effective authenticated solution for Remote Wearable Health Monitoring System. *IEEE Trans. Netw. Sci. Eng.* **10**, 2710–2718 (2023).
43. Saleem, M. A. et al. Provably secure authentication protocol for Mobile clients in IoT environment using puncturable pseudorandom function. *IEEE Internet Things J.* **8**, 16613–16622 (2021).
44. OMNeT + + Discrete Event Simulator. https://omnetpp.org/.
45. EHR Data. Find Electronic Health Records & Datasets | Datarade. https://datarade.ai/data-categories/electronic-health-record-ehr-data
46. Ullah, I., Sohail Khan, M. & Kim, D. IoT services and virtual objects management in hyperconnected things network. *Mob. Inf. Syst.* (2018). (2018).

Acknowledgements

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through a large group Research Project under grant number RGP2/421/45. This work was supported by the Researchers Supporting Project Number (MHIRSP2024005) at Almaarefa University, Riyadh, Saudi Arabia. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2025/R/1446). This research was supported by the Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R259), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author contributions

Mohd Anjum: Conceptualization, Methodology, Software, Writing - Original Draft, Writing - Review & EditingNaoufel Kraiem: Methodology, Validation, Formal analysis, Resources, Writing - Review & Editing, Visualization, Funding acquisitionHong Min: Conceptualization, Methodology, Resources, Writing - Original Draft, Writing - Review & Editing, Funding acquisitionYousef Ibrahim Daradkeh: Methodology, Validation, Formal analysis, Resources, Data Curation, Funding acquisitionAshit Kumar Dutta: Methodology, Resources, Writing - Review & Editing, Visualization, Funding acquisitionSana Shahab: Conceptualization, Methodology, Software, Data Curation, Writing - Original Draft, Writing - Review & Editing, Visualization, Funding acquisition.

Funding

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No.2021R1F1A1055408).

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to H.M.

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.