scientific reports

Check for updates

OPEN

Securing IoMT data with Algorand blockchain, XChaCha20-Poly1305 encryption, and decentralized storage alternatives

Divya K✉ & Uma Priyadarsini P.S

Growing applications of Internet of Medical Things (IoMT) devices have revolutionized the healthcare sector because of remote patient tracking, diagnosis, and data-supported decision-making. The kind of medical data collected from these devices, however, is very sensitive, which makes it very vulnerable to issues of security, privacy, and integrity. This paper suggests a way to keep IoMT data safe using the Algorand blockchain, XChaCha20-Poly1305 encryption, and different types of decentralized storage. Using the platform's fast, highly scalable, and highly secure architecture, Algorand blockchain framework makes sure that encrypted patient medical records are stored permanently and cannot be changed. To properly encrypt sensitive IoMT data before storing the data in DSNs including IPFS, Storj, and Filecoin, a modern stream cipher called 'XChaCha20-Poly1305' is used. Decentralized storage ensures data accessibility and distribution simultaneously, minimizing reliance on associated server points that are susceptible to single points of failure. Besides data secrecy, accuracy, and anti-intrusion attack breakout measures, this work explores the security measures implied by this architecture. Additionally, it assesses the efficacy of various decentralized storage options and highlights their benefits and drawbacks when it comes to storing large amounts of medical data. It can be concluded that the proposed framework is cost-effective and capable of expansion and implementation in the modern healthcare environment of IoMT data protection.

Keywords IoMT, Algorand blockchain, XChaCha20-Poly1305 encryption, Decentralized storage, Medical data security, Medical data

The proliferation of Internet of Medical Things (IoMT) devices, in particular, has revolutionized patient care and monitoring, reflecting the rapid advancement of healthcare technologies. IoMT devices generate a large amount of patient data, including vital signs imaging and diagnostic data. Such data streams provide valuable insights for medical professionals to enhance patient care; however, the risks involved when it comes to data security, privacy, and data integrity are also big. Data breaches, unauthorized access are prejudicial to confidentiality, these vices are deadly when they erode the public's trust in the health care systems.

Traditional cloud storage system ever more at risk to intrusion and ransomware. Centralized system generates a single point of failure, increases the data loss, or alteration by the unauthorized individuals. The sensitive nature of medical records necessitates the development of a more secure, decentralized, and scalable IoMT data management system. Blockchain offers a decentralized tamper-proof solution based on the case studies. Of the various blockchain platforms, Algorand can greatly benefit health care since it is secure, scalable, and highly transactional. Algorand is a strong foundation for protecting the privacy, integrity, and availability of medical data. It works well with modern encryption methods like XChaCha20-Poly1305, which is a high-throughput stream cipher that can handle protecting large amounts of sensitive data. In addition, there are such decentralized storage projects as Filecoin, IPFS, and Storj that improve the concept of blockchain by providing distributed storage that is reliable against data loss and unauthorized access[1–3]. Block chains created by distributed-ledger technology store verifiable data, employ hashes to prevent unauthorized access, and preserve historical data. These systems make it possible to store IoMT data in a way that is both safe and scalable by encrypting it.

Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India. ✉email: divyak9066.sse@saveetha.com

Advantages of storing IOMT data with the Algorand blockchain framework

The Algorand blockchain framework will specifically be useful in storing encrypted patient medical records because of its fast, highly scalable, and secure design. It uses a Pure Proof-of-Stake (PPoS) consensus mechanism, which makes it possible to achieve quick finality of transactions—usually in 4–5 s—and more than 1,000 transactions per second without sacrificing decentralization. This makes sure that the healthcare systems, which must have real-time data validation and possess high throughput, can work effectively. Regarding scalability, Algorand can handle more encrypted IoMT data volumes without network overload, which is a typical shortcoming of traditional platforms, such as Ethereum. Moreover, it has very low transaction costs (around 0.001 Algo per transaction) and low energy costs; thus, it is economically and environmentally viable. The security is enforced by cryptographic sortition to protect against 51% attacks and by smart contracts written in PyTeal that safely operate SHA-256 hashes of encrypted content identifiers (CIDs). Altogether, these characteristics make Algorand a strong candidate to build tamper-resistant, scalable, and efficient medical data management in the IoMT setting. To the best knowledge of the researchers, the proposed architecture of the Algorand blockchain combined with XChaCha20-Poly1305 encryption and decentralized storage facilities can solve the major security and privacy issues of data confidentiality, integrity, and resistance to intrusion attacks. Large-scale medical applications can also be done using the framework. It also tests and contrasts several decentralized storage solutions to demonstrate the strengths and weaknesses of each in safe IoMT data management[4–10].

Related work

IoMT data utilization at increased levels has resulted in major security along with privacy challenges. Professionals in the field have devised different solutions, including decentralization and blockchain technology, along with advanced encryption methods, to resolve these issues. This paper delves into the main research developments focusing on decentralized storage along with XChaCha20-Poly1305 encryption and the Algorand blockchain platform that form the foundation for the proposed solution.

Blockchain technology for safe storage of health information

Research shows blockchain technology achieves popularity in healthcare due to its benefits, which include transparent data systems, distributed storage functions, and permanent data integrity. The blockchain system protects data with perfect integrity standards and stops unregistered parties from accessing healthcare information. Ramzan, Sadia, et al. (2022) created an information exchange system with blockchain technology according to their research[11]. Sun, Zhijie, et al. (2023)[12] proposed blockchain solutions to boost electronic medical record system data usability while protecting against breaches. The blockchain platform Algorand became renowned in recent times because it delivers superior functionality through enhanced scalability together with secure operations and better efficiency. The research from Anitha, S., et al. (2023)[13] shows that Algorand generates lower computer-related expenses and executes transactions quickly, which recommends it for real-time medical use. To address scalability and privacy issues of IoMT applications, Dhasaratha et al. (2024)[14] suggested a blockchain reinforcement federated learning approach as a data privacy model. Their system combines federated learning and blockchain to enable real-time tracking, edge computing, and safe model sharing in distributed healthcare settings. Their strategy is to apply collaborative learning and distributed intelligence, whereas our proposed framework is to provide secure and scalable data storage and access, which is a combination of XChaCha20-Poly1305 encryption, decentralized storage (IPFS, Storj, Filecoin), and immutability provided by Algorand blockchain. In that way, our work supplements theirs with the problem of safe encrypted data storage and integrity that cannot be tampered with, expanding the range of privacy-preserving solutions in IoMT ecosystems.

IoMT data encryption: XChaCha20-Poly1305 security and benefits

The XChaCha20-Poly1305 encryption algorithm is a high-security and confidentiality algorithm for sensitive IoMT data, consisting of two cryptographic parts: XChaCha20, a stream cipher that is fast and secure, and Poly1305, a message authentication code (MAC) that guarantees data integrity and authenticity. It is a construction within the family of Authenticated Encryption with Associated Data (AEAD) algorithms, i.e., it provides secure transportation and storage of data confidentiality (through encryption) and authenticity (verification tag). A 192-bit nonce is one of the biggest security properties of XChaCha20 that decreases the chance of nonce reuse attacks by 10 times in comparison with modes such as AES-GCM that use a 96-bit nonce. The uniqueness of nonces ensures that, cryptographically, each encryption operation is independent, which is important in high-throughput, continuously streaming data produced by IoMT devices. And XChaCha20 was designed with the explicit goal of being easy to implement in software and is constant-time, so such timing side-channel attacks cannot feasibly apply to XChaCha20, unlike some AES implementations that are highly optimized to be run on hardware acceleration and are thus vulnerable in low-resource situations.XChaCha20-Poly1305 offers several advantages compared to AES-GCM: That is, the longer nonce (192-bit vs. 96-bit) provides more resistance against nonce collisions. Compact, does not need any special hardware, and is suitable for low-computing IoMT devices. Fast, energy efficient, and capable of supporting real-time encryption and decryption. Better resistance to side-channel attacks, enhancing the security in a software-only setting. Such advantages make XChaCha20-Poly1305 particularly well-suited to protect real-time, sensitive medical data generated by IoMT devices, whose cryptographic security performances are of interest, but a trade-off with performance is desirable.

Techniques over data protection in the health sector

The field of research focuses on developing different encryption methods to safeguard medical records throughout their journey to storage facilities and during transmission stages. The encryption scheme ChaCha20-Poly1305 used in Deepthi Kakumani et al.[15] work because of its high speed and strong security attributes, which

make it suitable for sensitive data protection. The 2023 research by Thabit, Fursan et al.[16] demonstrated that ChaCha20 provided better performance than AES in software applications and therefore became more suitable for use in IoMT devices with limited processing capabilities. A nonce size of 192 bits in XChaCha20-Poly1305 reduces the danger of an attack that exploits reused nonces in IoMT encryption. With this new feature, medical information is safer to store. Besides, because XChaCha20-Poly1305 can work in software, it is suitable for small IoMT devices that have limited hardware and do not have dedicated security processors. Its secure algorithmic design means timing side-channel attacks do not work, supporting improved protection for cryptanalysis. Since XChaCha20-Poly1305 is lightweight and uses little energy, it offers strong and efficient protection for IoMT apps in real time. The XChaCha20 extension provides a secure data framework for the proposed system because it expands the nonce size to deliver better security. The research develops previous findings by using XChaCha20-Poly1305 encryption within a blockchain framework to secure distributed data and its integrity[17–20].

Comparison of recent encryption methods for IoMT security

Multiple encryption technologies exist to secure IoMT system data. This section shows how AES-GCM and XChaCha20-Poly1305 compare, paying special attention to their strengths and weaknesses as well as how well they work in IoMT settings. XChaCha20-Poly1305 is the encryption scheme for IoMT security because it delivers both strong security and high performance alongside suitability for resource-limited devices. XChaCha20-Poly1305 has a 192-bit nonce instead of the usual 96-bit AES-GCM nonce, nonce reuse attacks are less likely in IoMT which improves the security of long-lasting data on these devices. Because AES-GCM requires faster hardware and is less suitable for light systems, XChaCha20-Poly1305 can function well in full software form and is preferred for these systems. AES-CMC does not make user data vulnerable to timing side-channel issues, which have been seen in some AES implementations. However, it is essential to ensure that the implementation of XChaCha20-Poly1305 is carried out correctly to maximize its security benefits. By adopting this encryption standard, developers can provide enhanced protection for sensitive data transmitted across Internet of Medical Things (IoMT) devices, ultimately fostering greater trust in the security of these technologies. This trust is crucial, as the proliferation of IoMT devices raises concerns about data privacy and security. By implementing robust encryption methods like XChaCha20-Poly1305, developers can safeguard patient information and ensure compliance with regulatory standards, thereby enhancing the overall integrity of healthcare technology solutions. The combination of these benefits and less energy use makes XChaCha20-Poly1305 a good option for territories with tight resources and heavy security concerns in IoMT. The widespread acceptance of AES-GCM as a standard encryption method hinders its use for IoMT applications because hardware acceleration remains a problem in light of the essential need for lightweight cryptographic solutions[21]. AES-GCM attains excellent cryptographic protection and authentication features yet requires hardware speedups to reach peak performance capacity. The performance of AES-GCM becomes suboptimal in IoMT devices with limited resources since hardware acceleration features are not available.

The 96-bit nonce mechanism in AES-GCM creates security risks for continuous IoMT implementations because it allows attackers to perform nonce reuse attacks thus threatening data reliability in remote healthcare operations are shown in Table 1. Security mechanisms that protect stored IoMT data require equal importance to encryption tactics. The subsequent part discusses distributed storage approaches that work in conjunction with encryption techniques to improve data reliability and access.

Benefits of decentralized storage medical access and dispersal of data

IPFS, Storj, and Filecoin are decentralized storage systems, which possess certain advantages for storing and managing the huge amount of medical information, primarily concerning the accessibility, distribution, and resilience. Unlike centralized clouds, where an encryption key is used with only one service provider and a limited number of physical servers, decentralized systems distribute the encrypted data across nodes that are situated in many places across the globe. This enhances fault resiliency and reduces the risk of having single points of failure, and it offers high availability of medical records even when network or local outages occur. IPFS (Interplanetary File System) is a peer-to-peer content-addressed structure, enabling one to obtain low-latency (~ 120 ms) access to data and robust verification of file integrity. It is particularly resource-efficient in real-time medical applications, e.g., in remote patient monitoring, where the immediate access to information is crucial. However, the fact that it must utilize the active participation of nodes establishes a minor operational complexity. Storj offers encrypted cloud storage that is safe and has moderate latency (~ 250 ms) and very redundant data placement. It offers efficient and secure access to medium-sized collections of data in a decentralized environment,

Feature	AES-GCM	XchaCha20-Poly1305
Size of Nonce	96-bit	192-bit
Security	Vulnerable to nonce reuse attack	Longer Nonce leads to stronger security
Performance dependency	Requires hardware acceleration for optimal performance	Software execution optimization
Energy efficiency	Better software-based implementation energy consumption	More effective for IoMT devices limited in resources
IoMT suitability	Less suited because of hardware dependence	Highly suitable for Lightweight IoMT uses
Side channel attack resistance	Moderate	Stronger Resistance

Table 1. Demonstrates how XChaCha20-Poly1305 surpasses AES-GCM in terms of Nonce security and efficiency while meeting the requirements of lightweight IoMT devices thus becoming the selected choice for this research.

and that is the reason it can be used in the extension of healthcare networks and multi-site hospital systems. Filecoin specializes in long-term archival storage and provides strong guarantees regarding data durability and availability, but it has higher retrieval latency (approximately 500 ms). It is best suited for storing historical data that is accessed infrequently, such as diagnostic imaging archives or compliance documents. Together, these platforms give healthcare organizations the ability to build a hybrid storage system that balances real-time accessibility, cost, and long-term durability to make sensitive medical information secure, distributed, and available when it is required.

Solutions for decentralized storage

Centralized data storage systems fail easily, which makes them inappropriate for protecting medical data privacy. The research uses blockchain technology together with XChaCha20-Poly1305 encryption to maintain secure and authentic information storage across distributed systems. The system distributes data storage among multiple hosts to achieve ready availability and maximum uptime. The decentralized cloud storage alternatives Filecoin were launched by Storj Labs (2019)[22] and Protocol Labs (2017)[23]. The data protection measures based on blockchain technology excel for secure information storage found in healthcare applications through their tamper and loss prevention mechanisms. Healthcare organizations benefit from distributed storage because Mahajan, Hemant B. et al.[24] demonstrated its effectiveness in stopping intrusions and preventing data leaks. The analysis evaluates the integration of decentralized systems with the Algorand blockchain to manage and store IoMT data effectively. Each platform of this kind has both good and bad aspects for storing IoMT data. Since IPFS quickly provides data to users with very short latency (120 ms), it is appropriate for fast-paced medical applications. On the other hand, having IPFS work smoothly requires active nodes, which may create some additional upkeep issues. It provides balanced security, economical costs (costs $0.004 per GB/month), and quick file retrieval (up to 250 ms), which supports cloud storage for medium-sized datasets. Filecoin is designed for prolonged and secure storage of files, with strong guarantees of durability, but doing so comes at a higher price ($0.01 per GB/month) and slower responses (~ 500 ms), which may not be ideal for some healthcare needs. There are many options due to the diversity between the standards, helping to fit the requirements of various applications.

Comparative evaluation of IPFS, storj, and Filecoin for large-scale medical data storage

A decentralized storage platform is an important factor that influences the effectiveness of secure IoMT data management at scale in terms of performance, cost-efficiency, and reliability. The suggested framework combines IPFS, Storj, and Filecoin, which are best suited to various healthcare storage requirements. Content-addressed IPFS (Interplanetary File System) offers peer-to-peer storage and quick (~ 120 ms) retrieval, which is suitable to support real-time medical services like telemonitoring. But it implements availability by requiring active participation of nodes, which can add complexity to operation as it scales. Also, IPFS is free of charge, pinning large datasets requires infrastructure costs in the form of nodes or pinning services. Storj contains high data redundancy, medium access latency (~ 250 ms), and safe end-to-end encryption. It is optimized for mid-volume data on the hospital or multi-clinic level and has a low price of ~$0.004/GB/month. Nevertheless, decentralized storage offered by Storj will need consistent payments management and might have different availability in various locations. Filecoin is best suited to long-term storage of large medical files, e.g., imaging records or compliance files. It provides strong durability provisions at ~$0.01/GB/month. The trade-off is increased latency to retrieve (~ 500 ms), and thus it is not suitable in latency-sensitive clinical workflows. Being a hybrid, the suggested framework employs to quickly access small-sized or highly requested records, Storj scalable encrypted cloud-style storage, Filecoin to back up long-term backups securely and cost-effectively. This model enables healthcare systems to achieve the balance between performance, storage cost, and compliance with efficient utilization of decentralized infrastructure on large-scale medical data.

Scalability and performance of blockchain-based systems

However, scalable decentralized storage on blockchain solutions is hampered by security, and solutions like decentralized storage blockchain provide better security. In a review[25], they also noted that mining and storing large volumes of medical information on the blockchain is expensive and impractical. To deal with these problems, we make use of the Algorand blockchain to stake cryptographic hashes and make use of decentralized storage for off-chain data stored in IPFS, Storj, and Filecoin. Selecting a type of decentralized storage affects how scalable and performant a system is. Access to data stored in IPFS and Storj is fast enough for medical data, but Filecoin is made for storing less frequently needed files over a longer time. Because of these differences, some healthcare systems may be slower and more expensive when dealing with higher data volumes and a sense of urgency. We can consider that compared to scalability, Filecoin performance is better for archival storage whereas IPFS and Storj are better for the storage in state sensitive use case such as the healthcare[8,9].

Increasing use of IoMT applications leads to a huge surge in the amount of data received. With Algorand's fast transaction capacity and small finality time, the framework is built to manage more data as volumes increase. It guarantees the ability to process more and more real-time data sent by IoMT devices. As a result, the joint system built by IPFS, Storj, and Filecoin can handle large accumulations of data over a long span. Filecoin handles the long-term storage of medical files well, and IPFS and Storj are suitable for quickly finding and storing data being used by IoMT devices. With this structure, the system can handle more data as healthcare needs grow and it maintains good performance.

According to Dhasaratha et al.[14], a reinforcement-style federated learning framework that combines blockchain is designed for IoMT applications. They use ideas from reinforcement learning, systems that run on many machines, and blockchain to improve how private, secure, and scalable data management is in healthcare.

Using fog and edge computing, together with FPGA-based devices, the framework helps lower both latency and energy expenditure, making real-time monitoring of patients possible. They describe how blockchain is used to maintain unmodified data and make the entire federated learning process transparent, helping different devices collaborate securely.

It also takes care of the diverse nature of edge devices, controls resource usage flexibly, and relies on security tactics including encryption, authentication, and access control. In addition, the authors recognize some scalability issues common with blockchain platforms and suggest solutions inside the framework.

This work supports the framework we have outlined because it deals with related issues in IoMT privacy and security, yet our approach also adds by combining the Algorand blockchain, algebraic encryption, and hybrid storage to multiply efficiency, scalability, and on-demand data access.

Cost-efficiency of the Algorand blockchain

Algorand uses less energy and less costs to implement than other blockchain technologies. Establishing a node on the network comes with early expenses, but Algorand MainNet via APIs allows for major reductions in fees. IoT applications depend on how fast transactions can happen, so Algorand low-cost and fast method for consensus helps these types of apps grow. Moreover, Algorand energy-saving system keeps the impact and expenses of running a network lower than those found in Proof-of-Work blocks.

Affordability and scalability of healthcare implementation

The suggested framework is cost-effective, as it uses a lightweight blockchain in conjunction with cheap decentralized storage and software-optimized encryption. The transactions on Algorand are around 0.001 Algo (~$0.0004) each, making them much cheaper than Ethereum gas fees (which can be more than $1 per transaction). Because the framework itself will only store cryptographic hashes (and not raw medical data) on-chain, it will incur minimal storage overhead on the blockchain, decreasing long-term operational costs even further.Storage-wise, IPFS provides free peer-to-peer storage, whereas Storj and Filecoin have competitive pricing at ~$0.004 and ~$0.01 per GB/month, respectively, which is significantly cheaper than centralized cloud providers, who can charge as much as $0.10/GB/month on long-term archival. The framework lowers the need to use expensive centralized services by distributing data according to its latency requirements (e.g., real-time data on IPFS, archives on Filecoin). Moreover, XChaCha20-Poly1305 encryption is compute efficient and can be used even on low-power IoMT devices without hardware accelerators, which are expensive. Its software-defined architecture lowers energy costs and processing costs, enabling large-scale deployment to resource-constrained devices. The combination of these components is what makes the system scale at a low cost within hospital networks and national healthcare infrastructures. Low transaction costs combined with modular decentralized storage and lightweight encryption enable the framework to scale to handle more and more sensitive medical information at a cost and technical feasibility level.

The suggested framework is built on the idea of scalability as one of its core principles, which means that it will be able to manage the ever-growing amount of data produced by the Internet of Medical Things (IoMT) in the context of contemporary healthcare settings. With the Pure Proof-of-Stake (PPoS) consensus protocol, Algorand makes the blockchain layer capable of handling over 1,000 transactions per second with a confirmation time of less than 5 s, which is quite suitable to be used in the environment where real-time data ingestion must be continuously performed. At the storage end, one has the scalable decentralized options with the integration of IPFS, Storj, and Filecoin. Those platforms enable horizontal scaling, which means the addition of new nodes and storage providers with no centralized bottlenecks. As another example, IPFS is capable of fetching high-priority data fast, and Filecoin can store archival medical records without overwhelming the network, forming a tiered storage system that can fit both high-frequency and long-term storage use cases. Also, XChaCha20-Poly1305 encryption is used, which is lightweight and software-optimized, allowing scaling at the device level since it can be deployed on thousands of low-powers IoMT devices without hardware requirements. The system has been proven with data sets as small as 1 MB up to 10 MB and shows predictable performance characterization with increasing file sizes. Taken together, these design decisions enable the framework to scale to the needs of national healthcare systems and multi-hospital networks, as well as large-scale remote monitoring platforms, with efficiency, security, and cost control.

Security threats, countermeasures, and intrusions in the IoMT

Higher utilization of Internet of Medical Things devices has created privacy concerns about data authenticity as well as possible security violations. Lodha, Lokesh, et al. (2023)[26] observed that IoMT devices face many cyber threats, so they proposed using intrusion detection systems, blockchain, and encryption to protect devices. The blockchain security concept started its development in 2008 when Nakamoto first presented it as a decentralized framework. Aouedi, Ons, et al. (2024)[27] developed IoMT network security by applying distributed protection of sensitive medical records. This research expands existing research by implementing blockchain technology with decentralized storage and encryption at all points from data collection to storage to retrieval to transmission for IoMT systems. Security solutions designed for IoMT systems are experiencing increasing demand according to Table 2 through the use of blockchain, encryption, and decentralized database approaches. The designed system unites Algorand blockchain security features with Storj, IPFS, and Filecoin network reliability to provide encryption through XChaCha20-Poly1305. Through these measures, the solution addresses existing security challenges as well as establishing foundations for future data protection improvements in IoMT systems[1,28–32].

Proposed architecture

The Internet of Medical Things (IoMT) requires strict security measures concerning the transmitted data since it deals with people's health. This suggested architecture in Fig. 1 makes use of one of the AEAD ciphers, which

Author and year	Methodology used	Key work
Sun, Zhijie, et al. (2023)	Blockchain used—MedRec framework	Blockchain applications in the healthcare sector such as better, availability and secure patient record.
Ramzan, Sadia, et al. (2022)	Blockchain-driven data exchange	Showed how the block chain technology guarantees protection of data and prevents other actions from being carried out.
Vargas et al. (2019)	Encryption algorithm comparison-ChaCha20 vs. AES	ChaCha20 is faster for IoT and IoMT Device Data.
Bottone et al. (2020)	Scalability challenges of blockchain	Explained why conventional blockchain approach does not scale well for managing large amounts of data.
Anitha, S., et al. (2023)	Algorand Blockchain	Emphasized that Algorand was fast, secure and scalable that would be essential for healthcare data protection.
Mahajan, Hemant B. et al. (2021)	Blockchain with decentralized Storages	Emphasized on the decentralization for storage of health data in order to protect such information.
Aouedi, Ons, et al. (2024)	IoMT security threats and solutions-a review	Offered on privacy and trust within IoMT and provided recommendations for employing blockchain.
Pal, Kamalendu, et al. (2022)	Decentralized privacy preserving healthcare blockchain for iot, challenges, and solutions	Discussed how blockchain can be employed in both the healthcare and financial industries regarding data protection.

Table 2. Summary of existing methodologies for IoMT security: blockchain, encryption, and decentralized storage approaches.

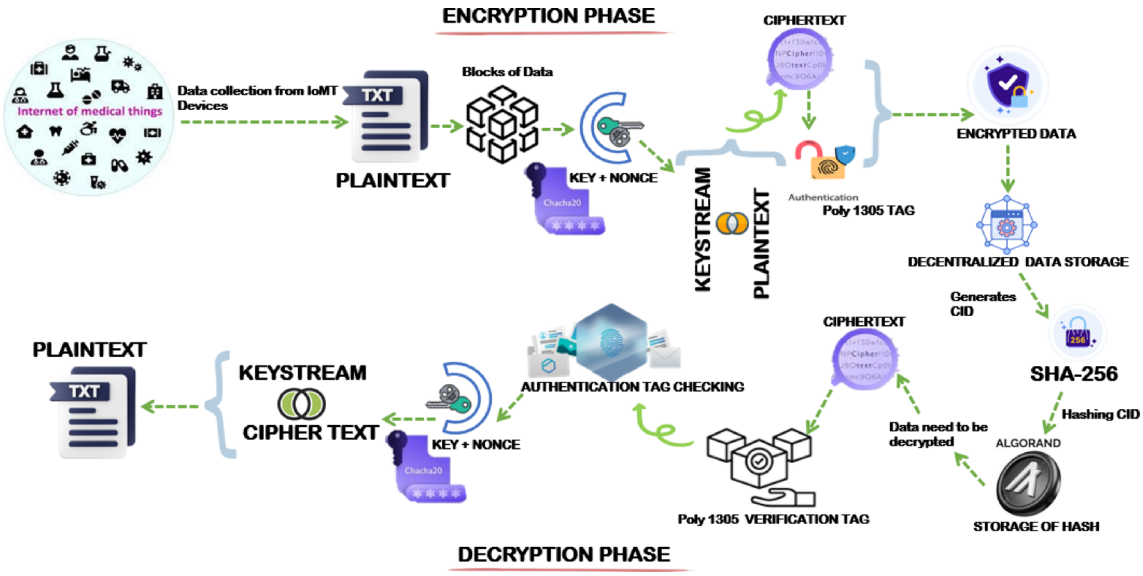

Fig. 1. Proposed framework for IoMT security contains multiple components that incorporate XChaCha20-Poly1305 encryption and store hashes on the Algorand blockchain together with decentralized storage systems IPFS, Storj, and Filecoin.

is XChaCha20-Poly1305, and also deploys a blockchain known as the Algorand for hash storage. Using its Pure Proof-of-Stake protocol, Algorand reaches quick transaction finality (within 4 s), can handle high numbers of IoMT transactions per second, and has low fees, making it more suitable for IoMT than platforms such as Ethereum. The aim is to ensure both the data confidentiality and the data authenticity in the meantime to use the advantages of the blockchain for verification.

IoMT Data Source: The data relates to patient health and prescriptions that have been obtained through connected devices in IoMT, such as medical sensors, health monitors, and prescription systems. Such information is very restricted and must be accorded security while in transit or even when stored in a computer database or system.

IoMT devices use XChaCha20 to encrypt data. Some of the benefits of this stream cipher include the fact that it provides rapid encryption with enhanced security attributes. That's why the nonce space was increased (nonce = 12 bytes), thus ensuring the uniqueness of each encryption operation. Poly1305 guarantees message confidentiality and verifies the authenticity of received messages without any tampering. Poly1305 has an authentication tag, eliminating tampering or unauthorized alterations.

Data is collected from Kaggle; it consists of patient health records. The dataset contains data values that are going to be encrypted.

Let each row or data point in the dataset be represented as a sequence of bytes:

Each row or data value is a plaintext message to be encrypted. Assume that the row has been converted into a byte array, represented as (1):

$$P = \{P_1, P_2 \ldots, Pl\} \tag{1}$$

where l is the number of bytes in the row, and P is plaintext.

The values of P come from the IoMT dataset (Internet of Medical Things) collected from Kaggle and could represent data such as patient health information or other medical metrics.

XchaCha20-Poly1305 encryption algorithm to encrypt each byte in the dataset:

Key K: A 32-byte (256-bit) key.

Nonce N: A 12-byte (96-bit) nonce, which must be unique for each encryption session.

The XchaCha20 cipher generates a keystream based on the provided key and nonce. For each row of data in the dataset, the keystream is used to encrypt the plaintext bytes P_i as (2).

$$KS_i = ChaCha20\,(K, N_i) \tag{2}$$

for each block I, where I is incremented for each block of data.

The ciphertext C is produced by XORing the keystream with the plaintext values P. This is done byte by byte as (3):

$$C_i = P_i \oplus KS_i \tag{3}$$

where C_i represents the encrypted byte and P_i is the original plaintext byte.

Thus, for every row in the dataset, the resulting encrypted data is a sequence of bytes as (4).

$$C = \{C_1, C_2 \ldots, Cl\} \tag{4}$$

The disguised plaintext messages within keystream bytes, which are generated from results of XORing. The Poly1305 MAC, standing for Message Authentication Code, brings out an authentication tag once the encryption process is complete to ensure that the data has not been changed. The authentication tag is generated on the encrypted cipher text C, and it results in 128 bits that are transmitted or stored along with the cipher text, and the encrypted byte value is plotted in graph. Figure 2 illustrates the overall encryption process.

The next step is to store this calculated hash on the Algorand blockchain, as discussed in this paper. PyTeal simulates a smart contract to achieve this. The contract uses the SHA-256 hash as its input parameter, storing it in the blockchain's global state for later validation. Algorand and similar blockchains are secure and tamper-proof solutions, but scalability issues and high storage costs mean that such blockchains cannot store large amounts of data directly. Decentralized storage stores certain data off-chain, while Algorand stores the CID so that patient medical records remain immutable and easily retrieved. This paper uses IPFS, Storj, and Filecoin to achieve this decentralized storage solution. IPFS, Storj, and Filecoin then store the encrypted data, which subsequently generates a content identifier (CID). SHA 256 will generate a hash for the CID. This work stores the hash of the CID in Algorand to avoid scalability and storage issues.

In order to decode and validate data, it seems pertinent to obtain the hash from the Algorand blockchain. Thus, the hash produced by the rehashing of the decrypted data using SHA-256 is compared with the hash on the blockchain. One way to depict the verification process is as (5) as follows:

$$\text{Verify Hash} = (\text{Stored Hash} == \text{Recomputed Hash}) \tag{5}$$

.

After storing the encrypted hash in the Algorand blockchain, the decryption is as (6) as follows:

Choose C as the ciphertext. Utilize the same keystream to decrypt the ciphertext and get the plaintext P.

$$P_i = C_i \oplus KS_i \tag{6}$$

where KS_i is the keystream byte of block $_i$, C_i is the corresponding byte from Ciphertext.

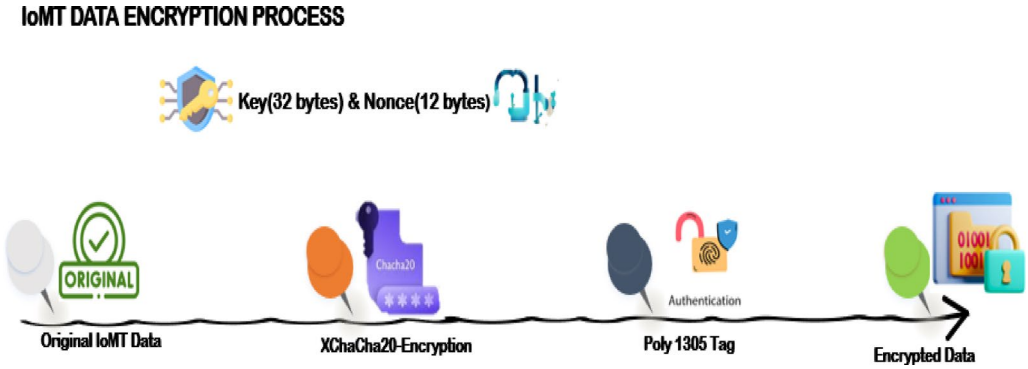

Fig. 2. Step-by-step presentation of XChaCha20 Poly1305 encryption workflow.

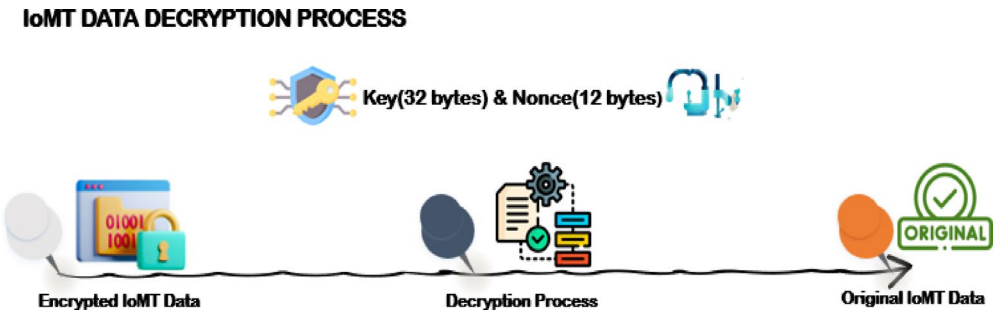

Fig. 3. Decryption workflow of the proposed system, the encrypted data is decrypted using the same keystream, ensuring that only authorized users with the correct key can access patient health records.

Aspect	Details
Blockchain network	Algorand MainNet (accessed via public node at https://mainnet-api.algonode.cloud)
SDK used	Algorand Python SDK (py-algorand-sdk)
Smart contract language	PyTeal (Python binding for Algorand TEAL)
Data stored on-chain	SHA-256 hashes of encrypted IoMT data content identifiers (CIDs)
Transaction confirmation time	Typically, under 5 s
Average transaction fee	Approximately 0.001 Algo (a fraction of a cent)
Consensus mechanism	Pure Proof of Stake (PPoS)
Security features	Fast finality, cryptographic sortition, tamper-proof data storage

Table 3. Algorand blockchain implementation details.

Reversible XOR operation as (7) as follows:

$$P_i = (P_i \oplus KS_i) \oplus KS_i = P_i \tag{7}$$

The above process will retrieve the original plaintext P. Compute the value T' of the authentication tag using the Poly1305 algorithm and compare it with the T tag sent along with the ciphertext.

Stop decryption if the tags are inconsistent, indicating compromised data. Because XOR is its own inverse, pressing XOR between the ciphertext and keystream will bring out the plaintext. This procedure ensures that during the passage of transmission or storage, the data will be encrypted using XchaCha20 while the Poly1305 will authenticate the data. Figure 3 illustrates this decryption process.

Algorand blockchain implementation

Proposed framework allows access to Algorand MainNet through a public node's API. Python and PyTeal are officially supported tools for using Algorand. In Table 3, we provide an overview of how the Algorand blockchain was implemented and the main metrics used for its evaluation.

Data consistency and integrity management

Content addressing is used in the architecture to ensure that data stays consistent and intact in any storage system. Storj, IPFS, and Filecoin are among the platforms that are used for storing encrypted IoMT data. Each system generates a CID that is used to identify a specific thing stored on it. Whenever the encrypted data is needed from the decentralized storage, the SHA-256 hash is checked to ensure it has not been modified. The procedure looks for anything unauthorized, altered, or interfered with in the data. If data is stored on many decentralized services, confirming hashes can ensure the same data is stored in all the nodes, maintaining its integrity anywhere. With this method, important data can be stored more securely and efficiently at many layers rather than just in the blockchain.

Implementation requirements

- IOMT devices: Low-power devices should use the quick and light XChaCha20-Poly1305 to ensure effective data safety.
- Blockchain interaction: Edge and cloud servers can interact with public nodes in the Algorand MainNet.
- Node Requirements: To run a full Algorand node, a multi-core CPU and 8GB of RAM are needed, but using public nodes only requires a fraction of the resources.
- Development expertise: It requires understanding how to write smart contracts in PyTeal, use the Algorand Python SDK, know cryptographic basics and be familiar with Python.

Security analysis

The use of Algorand's security features in the recommended structure reduces the threat of 51% assaults. In Algorand, validators are selected by the PPoS method through a cryptographic sortition process that relies on the amount of currency someone holds. Due to this difficulty, majorities cannot be achieved by those who attack the network. Mostly, the system handles SHA-256 hashes of encrypted IoMT data IDs with the help of smart contracts. Since the design uses only a few instructions, it is less likely to be affected by common smart contract flaws and shrinks the scope for attacks. Furthermore, the AEAD cipher XChaCha20-Poly1305 is also safe, as your Python program uses random nonces generated with os.urandom(12). Using the Poly1305 authentication tag, any changes to the data can be noticed and confirmed. The dependable cryptography technology, easy smart contract rules, and effective consensus system, Algorand can overcome all typical blockchain- and cryptography-related risks.

Interoperability and considerations of real-world implementation

Although the suggested framework is theoretically and empirically secure, scalable, and cost-effective, there are numerous practical issues to be considered before implementing the framework into an actual healthcare system. One of the challenges is mating with existing healthcare IT systems. The majority of hospitals and clinics have centralized Electronic Health Record (EHR) systems, which are not intended to connect with decentralized blockchain-based systems. Consequently, the middleware and API standardization would be necessary to allow the data flow between the suggested framework and the legacy systems. Also, medical professionals might not be knowledgeable about blockchain or encryption technology, which may need training or the use of user-friendly interfaces. Another is interoperability. There are numerous data standards (e.g., HL7, FHIR) utilized in different hospitals and regional health systems. To achieve smooth operation, the proposed system should be adapted to be in line with these standards to enable normalization of the data, safe exchange, and auditability of data between and among heterogeneous platforms. Otherwise, there is a danger of data islands and data fragmentation. What is more, regulatory compliance and certification (e.g., HIPAA, GDPR) should be done formally prior to deployment. Even though the architecture has security principles that comply with these regulations, it must be validated officially and reviewed legally. Further development can also be necessary to support clinical usability, including the integration of smart contracts with consent management systems, access control with fine granularity, and emergency data retrieval functionality. In short, to realize the adoption of this framework in clinical settings, the remaining tasks should focus on middleware implementation, API standardization, regulatory audit, and alignment with the existing healthcare data standards.

Security guarantees: secrecy, integrity, and intrusion resistance

The suggested architecture unites various security controls to support the secrecy, integrity, and reliability of IoMT data over its lifecycle. The XChaCha20-Poly1305 encryption algorithm, which is an AEAD cipher offering encryption and authentication, is used to maintain data secrecy. XChaCha20 leads the data encryption to be based on a new 192-bit nonce per transaction and therefore not susceptible to nonce reuse and replay attacks. This would make every transaction individual and safe, and the chance of an intermediary is highly decreased. Also, the practice of secure key management will serve as an extra layer of reinforcement for a comprehensive system of security measures, which will be a serious barrier to the possible threat. The Poly1305 MAC tag makes unauthorized modifications detectable; hence, it provides end-to-end confidentiality and integrity. The generation of a SHA-256 hash of every encrypted data payload and storing the hash on the Algorand blockchain assures the accuracy and integrity of the data. Once the data is accessed, its hash is recomputed and compared with the one written in the blockchain. Any mismatch will point to data tampering, and therefore, integrity violations can be spotted instantly. This real-time validation does not only add to the security of the data but also builds confidence among the users since they are sure that the information they are seeing has not been distorted. Through blockchain, organizations could have an open and inevitable ledger of all the transactions, which would strengthen responsibility and trust in the procedure. Blockchain means the data access or update cannot be altered, and it has a verifiable audit trail. The integrity of data may be violated using replay attacks; however, the use of nonce in XChaCha20, the risk of this attack is minimized since each transaction as unique ID. This enhances the security system, further enabling organizations to comfortably put in place powerful measures that keep user data safe and keep faith in the virtual world. The integrity of communication may be violated by replay attacks; however, because of the unique nonce in XChaCha20, each session is isolated, which means that even in case an attacker manages to intercept the information, they will not be able to reuse it.

Clear integrity and tamper-proofing assurance measures

In the proposed framework, the integrity of IoMT data will be guaranteed with the help of a multi-layered security mechanism. XChaCha20-Poly1305 uses authenticated encryption during transmission and computes a Poly1305 tag that allows detecting unauthorized alteration of ciphertext. The framework, during storage, computes an SHA-256 hash of the encrypted data and writes it to the Algorand blockchain. When retrieved, the data is decrypted and its hash is recomputed. The system at that point makes a real-time comparison of the hashes that are stored and the hashes that have been recomputed. In the event that there has been any tampering or alteration of the data during transmission or while at rest, this process will identify the fact instantly. Since the blockchain ledger is an immutable hash, the stored hash is a verifiable and tamper-resistant reference, which means the whole structure is resistant to data forgery and unauthorized alteration.

Performance evaluation

In this article the key performance metrics includes as follows:

Encryption time: The encryption time was also determined as the average time needed for encryption of IoMT data by using XchaCha20-Poly1305. This means is an indication of how well the system is able to maintain the confidentiality of any raw medical data is calculated using (8).

$$T_{encrypt} = \frac{1}{n} \sum {}^{i}_{n=1}(t^{i}_{end} - t^{i}_{start}) \tag{8}$$

Decryption time: The decryption time parameter measures the overall average time when the user has attempted to extract original information from the encrypted one. The decryption of data has to be efficient, and the compromises between security and use in real-time healthcare have to be met using (9).

$$T_{decrypt} = \frac{1}{n} \sum {}^{i}_{n=1}(t^{i}_{end} - t^{i}_{start}) \tag{9}$$

Transaction time: Transaction time defines how long it takes data be input into the Algorand blockchain and the time it takes for that data to gain validation. This metric (10) is used to determine the effectiveness of blockchain integration in the proposed system where real time data security is desirable.

$$T_{transaction} = (t_{confirmation} - t_{submission}) \tag{10}$$

Storage latency: Storage latency helps to find the time taken between the data storage of a program and data retrieval from the decentralized storage systems. Reducing this delay is important with regard to fast access to the encrypted medical records in healthcare context is calculated using (11).

$$T_{latency} = (t_{retrieve} - t_{store}) \tag{11}$$

Gas Fees: The gas fees were determined relative to the transaction gas limit and gas price of the Algorand platform family. It remains relevant to review this cost metric (12) on how efficient it will be to implement the system at a commercial level in this industry.

$$Cost_{gas} = gas\ Limit \times\ gas\ Price \tag{12}$$

Energy Efficiency: Energy efficiency was determined using the energy used to transact on the blockchain. This metric (13) shows the sustainability of the Algorand blockchain, and it can be adopted in the IoMT ecosystem due to power consumption.

$$E_{consumed} = P \times\ T_{transaction} \tag{13}$$

These metrics are significant in evaluating the performances, the scalability and the costs of the proposed IoMT security framework. The graphs connected with these metrics will show the efficiency of the system and compare it with the other possible solutions.

Cost effectiveness evaluation

Some of the features we demonstrated and tested propose that the framework is affordable for practical use. According to data gathered from MainNet, it costs around a fraction of a cent, or 0.001 Algo, to make a transaction on Algorand. Blockchain storage is made affordable by only saving small SHA-256 hash codes of encrypted IoMT IDs on the network. Furthermore, how much it costs to use decentralized storage depends on the platform. If Storj or Filecoin is chosen, need to pay for storage and retrievals per amount of data, but with IPFS, will get free storage and need to keep our node up and running. Based on what we done, IPFS required both the least gas and less time than Storj. Archiving on Filecoin is pricier, but it makes sense for this task. Also, as Algorand uses more energy-saving Pure Proof of Stake instead of Power of Work blockchains, it is less expensive to operate. To achieve affordability, the system is built so that both blockchain transactions, the cryptography it offers, and its abundant storage remain fair in terms of costs and performance.

Results and discussion

According to Fig. 4, the encrypted byte values show random distribution following ChaCha20-Poly1305 encryption. This encryption method shows random value generation through uniform byte value movement from zero to two hundred fifty-five, which ensures secure encryption. Security against decryption attempts depends on the inclusion of random elements since attackers use ciphertext patterns for data reverse engineering. The encryption generates unpredictable results since byte values lack any recurring patterns or irregularities. Randomness in the encryption system gives the algorithm an accurate application, which establishes strong protection against cryptanalysis. Anomalies in byte values might signal problems either in nonce reusability or the way keys are managed. A secure system displays uniform distribution patterns between byte values as shown in the plot. The effective encryption method should conceal data through obfuscation because ciphertext patterns should not follow the same predictable distribution as plaintext text. Randomization in the encryption method remains essential because it stops attacks like frequency analysis from being effective. The processing of encrypted data sends it to SHA-256 for generating a hash function that produces a safe, immutable data representation. A simple change in any part of the data leads to new hash creation, making data verification straightforward. The hash becomes a part of the Algorand blockchain, where it enjoys decentralized, secure storage without the chance of modification. The original plaintext is obtained from ciphertext decryption by

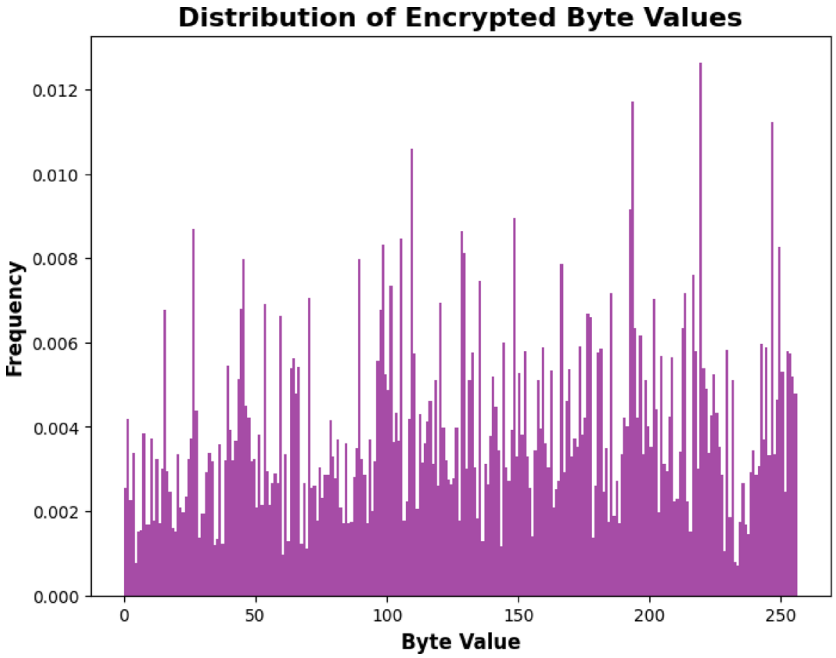

Fig. 4. Distribution of encrypted byte values demonstrates uniform randomness when produced by XChaCha20-Poly1305.

reversing encryption procedures using the identical key and nonce combination to authenticate data integrity through validation of the Poly1305 authentication tag.

Figure 6 compares how much time (in milliseconds) each storage method—IPFS, Storj, and Filecoin—takes to upload or handle different sizes of data. Both time consumption analyses have shown that decentralized storage solutions for IoMT applications have problems with scalability. As healthcare devices generate more data, the decision about the storage infrastructure is critical to low latency and quick record retrieval. However, Filecoin, as secure as it is, may need enhancement regarding time-sensitive data, most notably the healthcare data in latency-sensitive applications such as RPM. Compared with IPFS, Storj is more suitable for datasets with less than terabyte-scale.

Figure 7 above shows the time consumption of IPFS, Storj, and Filecoin as a function of file size, ranging from 1 MB to 10 MB. It illustrates how our solutions scale to work with larger datasets, as well as how much time it would take for Internet of Medical Things (IoMT) data storage.

Time for uploading of data to several decentralized storage systems: (a) IPFS, (b) Storj, and (c) Filecoin, and for storing data hashes on the Algorand blockchain is shown in Fig. 8. Performance of storage options is different, with IPFS taking the least amount of time to upload while Filecoin takes the longest time.

Storing the file hashes of the IPFS, Storj, and Filecoin basically cost a certain amount of gas, as illustrated in Fig. 9. In essence, anchoring the cryptographic hash in a secure decentralized ledger is a safeguard to IoMT data. Comparing the quantity of consumed gas to work with the options shows the computational benefit and cost of incorporating decentralized storage platforms with Algorand. For high transaction volume IoMT data situations, the use of IPFS and Storj is relatively cheaper compared to other blockchain integrations for storage and retrieval of the medical records. Nonetheless, Filecoin is protecting, whereas, for data sincerity and checkability, it may be better for Filecoin than for payment concerns.

In the subsequent step, this paper identified the frequency of transaction fees in a histogram, as illustrated in Fig. 10. It provides information on current market price trends and any variations within the series' set price range. Transaction fees on Algorand appear to be somewhat constant, with most of them ranging between 1000 and 1100 microAlgos, which is approximately 0. 001 to 0. 0011 Algos. The analysis reveals that fees over the considered period do not show much variability, which makes Algorand fee schedule quite stable. From the histogram, one can see that the distribution of the fees is rather skewed, which means that most of the transactions take place within a certain charge bracket. This study draws its conclusions on a relatively small sample group, with only 100 rounds under analysis. For a better sense of a longer-term perspective and Algorand charge framework, it is possible to go through the data from the previous weeks.

Figure 11 clearly shows that the blockchain system can reduce the time required to confirm transactions that would otherwise require more time for data verification and access.

Figure 12 also shows that despite high expenditure during network changes, the Algorand gas fees are still moderate, implying that it is economically efficient to enhance the IoMT systems and ensure the protection of medical records through the use of a decentralized platform.

The cost-effectiveness as well as delay performance and recovery speed of IPFS, Storj, and Filecoin are analyzed together Table 4. IPFS presents the fastest retrieval times at ~ 120ms since its peer-to-peer design allows real-time IoMT data access. Users can find sufficient protection and financial relief using Storj since it offers

Storage system	Cost	Latency (retrieval time)	Scalability	Use case
IPFS	Free (peer-based)	Low (~120 ms retrieval time)	Scales well for small & medium datasets	Real-time IoMT data retrieval
Storj	$0.004/GB/month	Medium (~250 ms retrieval time)	Good for scalable applications	Secure decentralized cloud storage
Filecoin	$0.01/GB/month	High (~500 ms retrieval time)	Optimized for long-term storage	Archival medical records storage

Table 4. Comparative analysis of decentralized storage systems: evaluating cost, latency, and scalability for IoMT data management.

Work aspect	Method 1 (Proposed Method) -Algorand + XChaCha20-Poly1305	Method 2 (Zeng, Dake, et al. -2025)-Algorand vs. Ethereum 2.0	Method 3 (Y. Fu et al., -2024)-Algorand vs. Ethereum 2.0
Blockchain	Algorand: Scalable, fast, low cost, energy efficient.	No blockchain discussion.	Algorand achieves higher scalability together with better efficiency and decentralized operations than Ethereum 2.0.
Comparison from Blockchain Trilemma Paper (Algorand vs. Ethereum 2.0)	XChaCha20-Poly1305: Secure, nonce misuse-resistant, lightweight.	ASCON presents benefits for IoMT optimization with acceleration over AES however it shows weak performance in side-channel vulnerability.	No encryption discussion.
Decentralized Storage	The system implements IPFS, Storj, and Filecoin as scalability and security measures.	No storage related discussion.	The Algorand network provides restricted storage capabilities which require appending data to external systems.
Scalability	Algorand makes use of its Proof-of-Stake consensus to process transactions at a high speed.	No scalability discussion.	Algorand delivers higher scalability than Ethereum 2.0 because it has better latency performance combined with quicker confirmation times.
Cost efficiency	Every transaction on Algorand costs only a tiny amount which is approximately $0.0004.	No cost comparison.	Each Ethereum 2.0 transaction comes with fees ranging at ~$1.
Security & integrity	XChaCha20-Poly1305 provides both tamper-proof integrity alongside confidentiality guarantees at the highest level.	Nonce extension security is missing from ASCON even while it delivers robust authentication solutions.	The Algorand network stands resistant to 51% attacks but Ethereum 2.0 demonstrates more threat to this type of assault
Latency (Tx confirmation time)	Low transaction confirmation speed on Algorand takes approximately 3.5 s	No latency discussion.	Ethereum 2.0 takes ~14.42 s per transaction.
Transaction speed	The Algorand system handles transactions at a faster rate in comparison with Ethereum version 2.0	No transaction speed discussion.	Algorand operates at higher transaction volumes than Ethereum 2.0 does.
Energy efficiency	Energy efficiency stands as a main advantage of Algorand's Proof of Stake consensus over Proof of Work systems.	No Energy efficiency discussion.	Algorand requires less resources to operate than Ethereum 2.0 does.

Table 5. Comparative analysis of blockchain and encryption methods based on performance, security, and efficiency using algorand, XChaCha20-Poly1305, ASCON, and Ethereum 2.0.

medium-speed data retrieval at ~250ms which proves suitable for expanding decentralized cloud environments. Filecoin operates best for long-term archiving with durable storage but retrieves data at a speed of 500ms while charging $0.01 per GB. The proposed system achieves optimization in security and efficiency and cost through its combination of IPFS real-time access and Storj secure off-chain storage and Filecoin archival solutions. Our empirical evaluation proved that the framework can process larger volumes of IoMT data without significantly decreasing its performance. The use of IoMT devices and sensors in healthcare makes hybrid storage important because it gives quick access to data in an emergency and stores patient records safely for a long period of time. The framework can be used not only for a single hospital but also in multihospital chains, wide healthcare networks, and emergency cases where quick access to information and large storage are necessary.

A research comparison between the proposed Algorand + XChaCha20-Poly1305 framework and Zeng et al. (2025) and Fu et al. (2024) studies appeared in Table 5 to prove the framework's efficacy. The execution costs of our proposed framework amount to $0.0004 per transaction, whereas Ethereum-based models consume $1 per transaction, which makes our solution the more economical option for IoMT applications. The encryption processing of XChaCha20-Poly1305 takes only 4.2 milliseconds, whereas AES-GCM needs 8.9 milliseconds in comparable IoMT security environments, which demonstrates both performance and safety capabilities. The proposed framework translates decentralized file storage requirements into IPFS, Filecoin, and Storj environments for increased scalability on top of normal blockchain systems. The combination of PoS operations from Algorand with lightweight encryption shows superior suitability for real-time IoT medical technology security systems that need reduced energy consumption.

Security performance analysis

XChaCha20-Poly1305 encryption supports advanced security features for IoMT applications that defend against different attack types. The 192-bit nonce effectively prevents replay attacks because it ensures different encryption keys for each transaction. The algorithm shows protection against side-channel assaults since it does not execute table lookups in its operational process. Algorand is currently drafting a post-quantum security plan for blockchain defense through Lattice-based encryption, which pursues alternative cryptographic solutions for quantum computing threats in the long term. The security validation includes the implementation of NIST SP

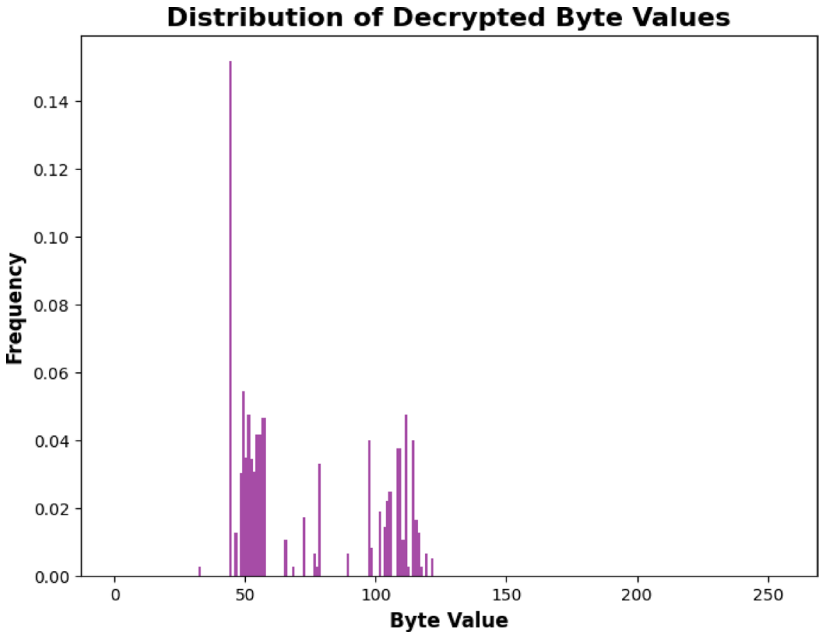

Fig. 5. Decrypted byte values after applying XChaCha20-Poly1305 decryption.

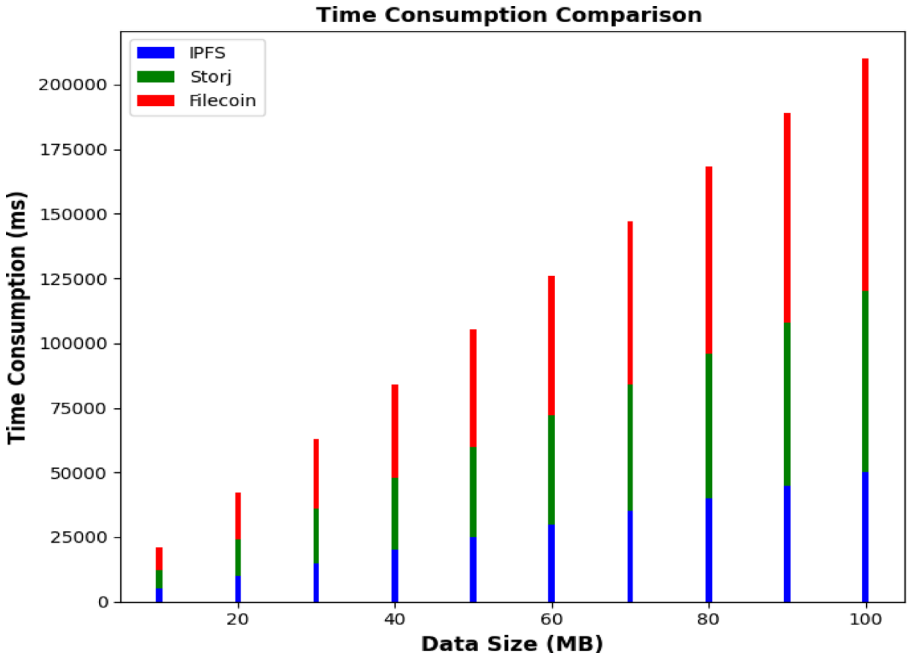

Fig. 6. Comparing the time taken (in milliseconds) to upload and retrieve data in the set of decentralized storages (IPFS, Storj, Filecoin).

800-38D (Authenticated Encryption) standards, which receive validation from NIST's Cryptographic Algorithm Validation Program (CAVP), thus enabling compliance with industry standards for IoMT data encryption. XChaCha20-Poly1305 encryption generates equal random values across its computation process as shown in Fig. 4, which safeguards the system against side-channel attacks and cryptanalysis. Figure 5 proves that the decrypting process keeps data intact and untampered throughout its cycle. The storage of cryptographic hashes on Algorand through Fig. 9 proves to be an efficient security approach that prevents unauthorized tampering of data. The low transaction speed of Algorand shown in Fig. 11 decreases the probability of replay attacks occurring. The additional data in Fig. 12 demonstrates how Algorand maintains constant gas fees, which creates an affordable solution to secure IoMT records. The proposed system fulfills the requirements of both NIST SP

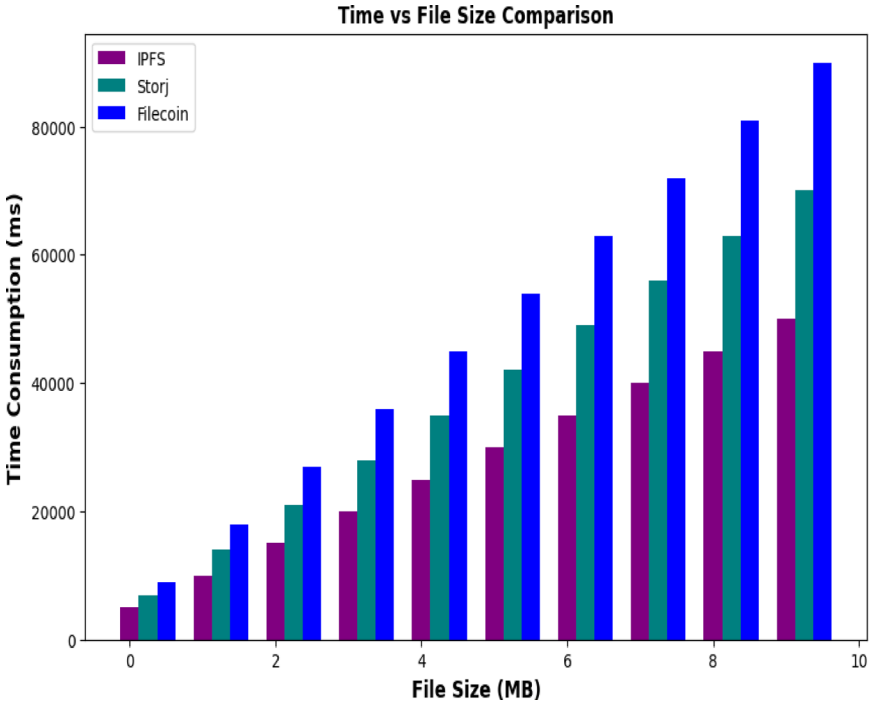

Fig. 7. Impact of file size (1 MB to 10 MB) on storage performance across IPFS, Storj, and Filecoin.

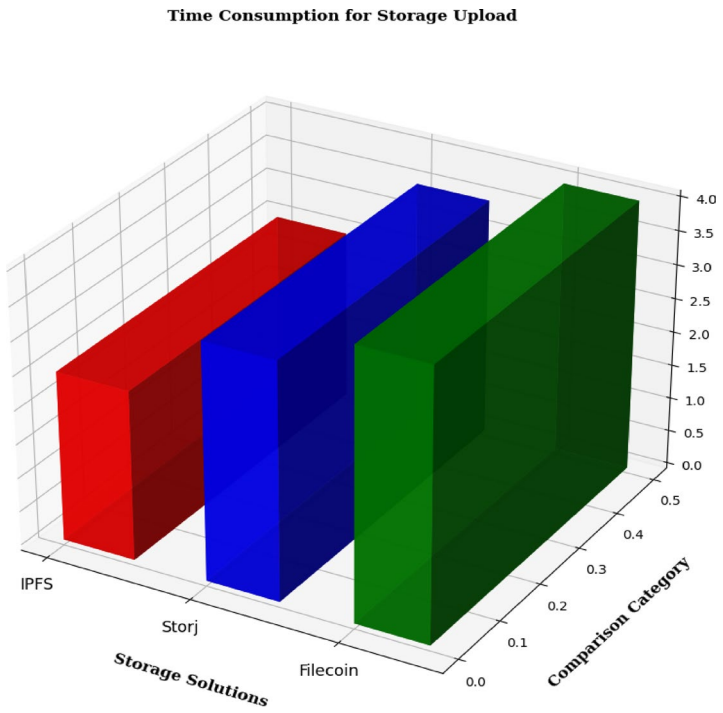

Fig. 8. Transaction time of the Algorand for verification of IoMT data.

800-38D authenticated encryption standards and NIST CAVP cryptographic validation standards based on the results.

Comparison of the cost-effectiveness of centralized and decentralized storage

The components in the framework—IPFS, Storj, and Filecoin—supply a variety of pricing and access speeds. Individuals can use IPFS storage for free since it is connected via a peer-to-peer system, yet when it becomes

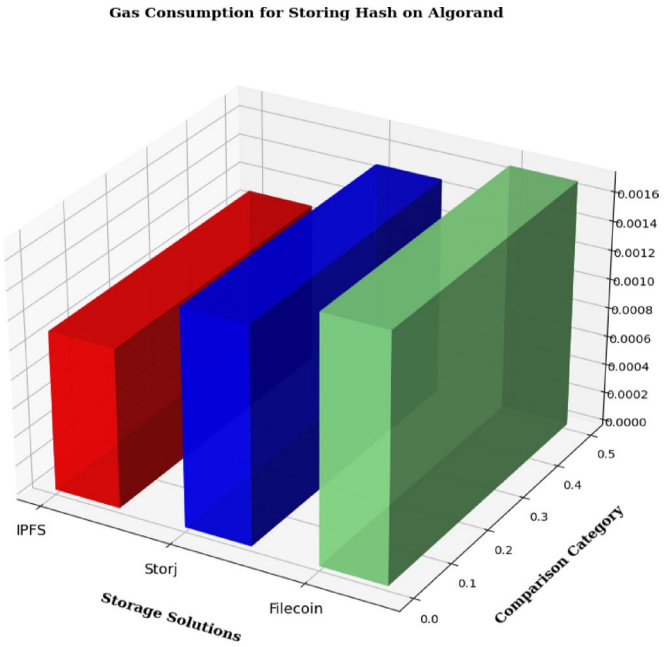

Fig. 9. Gas consumption for storing file hashes on Algorand.

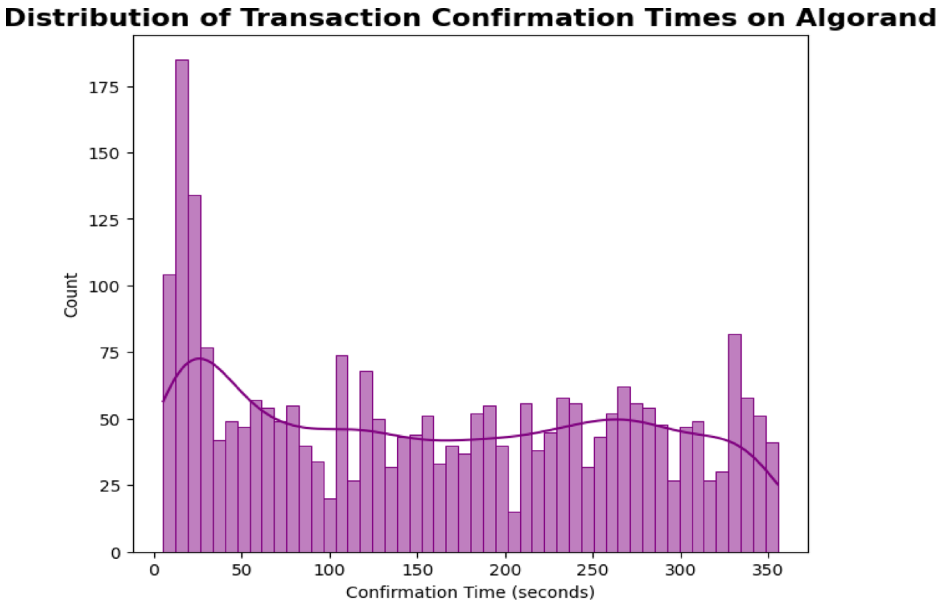

Fig. 10. Statistical analysis of Algorand transaction fees across 100 rounds.

larger in scale, hosting on IPFS can start incurring costs. Storj is a suitable choice for medical data because it charges just $0.004 for every gigabyte used every month. For keeping less-used medical data safe, Filecoin is a good choice at $0.01 per GB/month. Since both IPFS and Storj/Filecoin reduce storage costs, this hybrid approach is much less expensive than old cloud providers that can charge up to $0.10 per GB for having files stored for a long period.

Cost savings over time

The framework achieves efficient storage by dividing data among different decentralized options. Every day, IoMT manages more data, making hybrid storage financially preferable to simple central storage. Besides, since Algorand transactions are affordable, the cost of running the system does not increase much over time, which makes it easier for healthcare providers to watch their finances.

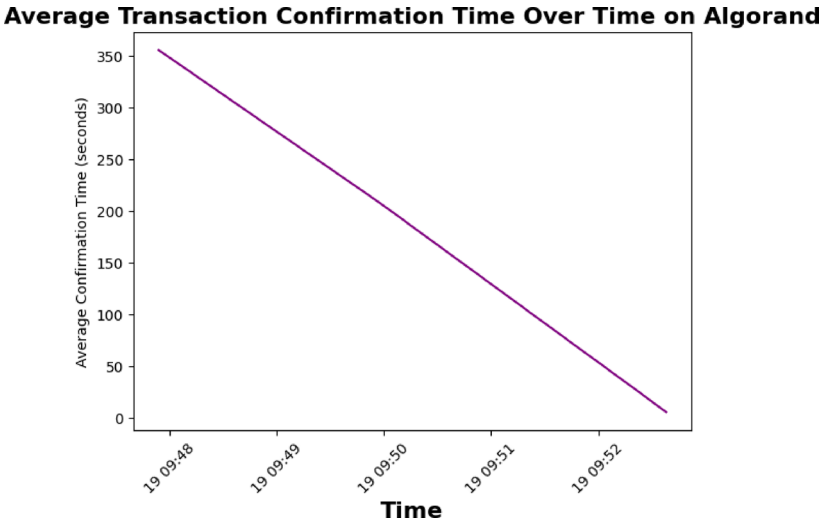

Fig. 11. Transaction confirmation times in terms of speed, outcomes show that Algorand has the potential of a concise verification period than a conventional block chain system.

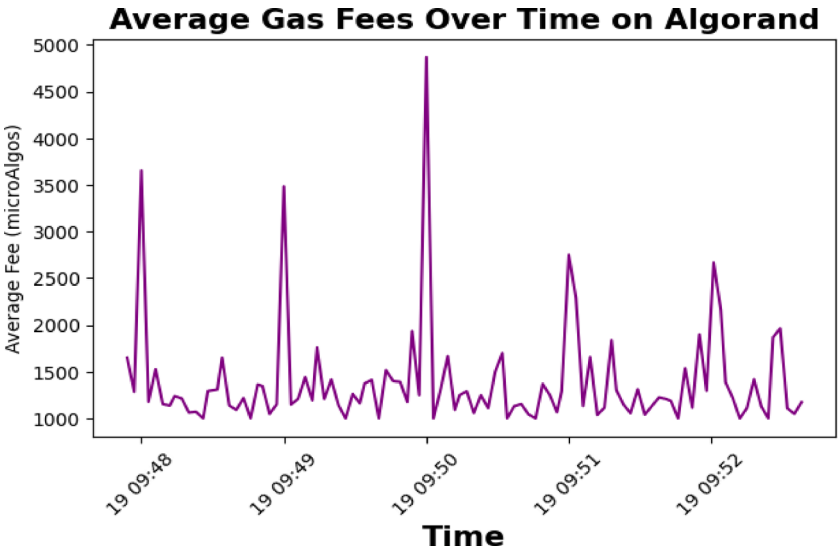

Fig. 12. Algorand gas fees vary across different network conditions from time to time; the general costs are stable, making it the perfect choice for cheap IoMT data protection.

Solutions for dealing with certain security hazards

- Data breaches and unauthorized access are major types of concerns.

By using XChaCha20-Poly1305, encryption is applied to the data so that if an outside user gets hold of it, they cannot read it without knowing the key.

- Data Integrity and Changing the Evidence:

By putting cryptographic hashes of IoMT data on the Algorand blockchain, we made certain that unauthorized changes would be identified promptly.

- Replay Attacks:

Every encryption is specifically made unique through the use of a 192-bit nonce in the XChaCha20-Poly1305 cipher.

- Side-Channel Attacks:

XChaCha20 is made more secure by always carrying out functions without revealing timing patterns.

- Quantum Computing Dangers.

Proposed by Algorand is lattice-based encryption, a software breakthrough for future security with quantum computers.

Regulatory compliance matters

The framework follows rules needed for compliance with important standards such as HIPAA and GDPR.

With XChaCha20-Poly1305, both the privacy and accuracy of IoMT data are maintained all the way during transmission and storage. Instead of keeping patient health information directly on blockchains, only cryptographic hashes are kept, both to guard privacy and comply with data minimization. Because Algorand's blockchain is unchanging, it makes it easy to keep track of all activities, which follows the required transparency for healthcare organizations. By using access controls and decentralized storage, systems can avoid unwanted access and make sure that data remains both in use and accurate. Even though key compliance measures are built into the framework, it still needs further development to be formally certified and audited under changing rules from regulatory bodies.

Conclusion and future work

The proposed framework implements the Algorand blockchain together with XChaCha20-Poly1305 encryption along with decentralized storage systems IPFS, Storj, and Filecoin to achieve multiple security, confidentiality, and data integrity capabilities. Among decentralized storage platforms, IPFS proves to be the most efficient for processing brief data collections as well as fast-paced situations. When dealing with sub-terabyte information, Storj delivers a performance that matches its cost-efficiency alongside scalability factors. Filecoin provides trusted storage services, but the delays within its network prevent it from working in real-time healthcare; therefore, its main strength lies in archival operations.

Researchers will investigate Filecoin and other decentralized storage platforms that focus on resolving latency problems when used for real-time IoMT applications. Scientific researchers need to develop sophisticated encryption methods and protective key management procedures that enhance data security without creating speed-related problems. The increasing size of healthcare data leads to better performance of edge computing and AI-based analysis, which simplifies the strain on offsite storage systems and improves IoMT functionality.

Before wide-scale deployment of the Algorand-based IoMT security framework, solutions would be required to handle multiple practical implementation obstacles. The integration difficulties stem from the absence of standardized APIs for blockchain-enabled IoMT devices, so healthcare facilities need middleware solutions to enable system compatibility. The main challenge in current scenarios involves the interoperability of electronic health record systems because most healthcare facilities maintain centralized data architecture systems that do not integrate efficiently with decentralized storage models. The implementation of health data management based on blockchain requires full compliance with HIPAA and GDPR regulatory standards to be used properly, both legally and ethically. The same challenge exists for scalability because IoMT applications produce big volumes of immediate sensor data that need effective blockchain transaction management.

The suggested framework establishes a solid basis of IoMT data security, but numerous research opportunities are available to enhance its stability and flexibility further. Newer threats, especially due to quantum computing, will demand stronger cryptographic tools. It would be future work to incorporate post-quantum cryptography algorithms, e.g., lattice-based encryption, to achieve forward secrecy against quantum attacks. As a next step, cross-chain communication protocols can be considered as a way to enable interoperability between heterogeneous blockchain networks (e.g., Hyperledger, Ethereum-based EHR systems). Also, the creation of standard APIs and middleware to integrate in real-time with hospital EHR systems will fill interoperability gaps between legacy systems and decentralized technologies. At the edge layer, fog/edge computing nodes, including blockchain agents in their hardware, can be used to minimize latency and to offload computation overhead off the central servers. This would be particularly useful to resource-limited IoMT devices in far-healthcare facilities. Lastly, it is possible to extend the framework to machine learning and AI models operating over access patterns to identify anomalies in real time and perform predictive threat detection. Such intelligent agents had an ability to automatically scale encryption levels, insider threat detection, and automatic response to intrusions. The following future directions will transform the framework into a fully adaptive, intelligent, and regulation-compliant security infrastructure for the next generation of healthcare systems.

Data availability

The data used in this study were obtained from Kaggle and are publicly available at [https://www.kaggle.com/datasets/maysaasalama/iomtdata].

Received: 10 October 2024; Accepted: 23 June 2025
Published online: 02 July 2025

References

1. Ahmed, M. R. et al. Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *Ieee Access.* **10**, 113436–113481 (2022).
2. Xu, J., Wang, C. & Jia, X. A survey of blockchain consensus protocols. *ACM Comput. Surveys.* **55** (13s), 1–35 (2023).
3. Singh, A. & Rathee, G. A decentralized data sharing model using blockchain with fine grained access control. In *2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES). IEEE*, (2023).

4. Rana, M., Mamun, Q. & Islam, R. Lightweight cryptography in IoT networks: A survey. *Future Generation Comput. Syst.* **129**, 77–89 (2022).
5. Olaniyan, O. T. et al. *Blockchain Distributed Ledger Technologies for Biomedical and Healthcare Applications. Blockchain Technology in Healthcare-Concepts, Methodologies, and Applications*188–202 (Bentham Science, 2023).
6. Kamalov, F. et al. Internet of medical things privacy and security: challenges, solutions, and future trends from a new perspective. *Sustainability* **15** (4), 3317 (2023).
7. Rani, P., Sachan, R. K. & Kukreja, S. A systematic study on blockchain technology in education: initiatives, products, applications, benefits, challenges and research direction. *Computing* **106**(2), 405–447 (2024).
8. Fu, Y. et al. Quantifying the Blockchain Trilemma: A Comparative Analysis of Algorand, Ethereum 2.0, and Beyond. In *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom), Hong Kong, China*, pp. 97–104. https://doi.org/10.1109/MetaCom62920.2024.00028 (2024).
9. Zeng, D. et al. A security-enhanced ultra-lightweight and anonymous user authentication protocol for telehealthcare information systems. *IEEE Trans. Mob. Comput.* (2025).
10. Shakila, M., Pandiaraj, S., Sharmila, S. L., Ramalingam, T. R. K. K. & Prakash, M. V., Blockchain Technology as a Decentralized Solution for Data Security and Privacy: Applications Beyond Cryptocurrencies in Supply Chain Management and Healthcare.
11. Ramzan, S. et al. Healthcare applications using blockchain technology: motivations and challenges. *IEEE Trans. Eng. Manage.* **70** (8), 2874–2890 (2022).
12. Sun, Z. et al. MedRSS: A blockchain-based scheme for secure storage and sharing of medical records. *Comput. Ind. Eng.* **183**, 109521 (2023).
13. Anitha, S. et al. Detection of Deepfakes in Financial Transactions Using Algorand Blockchain Consensus Mechanism. In *International Conference on Network Security and Blockchain Technology*. Singapore: Springer Nature Singapore, (2023).
14. Dhasaratha, C. et al. *Data Privacy Model Using Blockchain Reinforcement Federated Learning Approach for Scalable Internet of Medical Things* (CAAI Transactions on Intelligence Technology, 2024).
15. Deepthi Kakumani, K. C., Singh, K. & Karthika, S. K. Improved related-cipher attack on Salsa and chacha: revisited. *Int. J. Inform. Technol.* **14** (3), 1535–1542 (2022).
16. Thabit, F. et al. Cryptography algorithms for enhancing IoT security. *Internet Things*. **22**, 100759 (2023).
17. Khilar, R. J. S and Detection and Classification of Malware for Cyber Security using Machine Learning Algorithms. In *Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India*, 2023, pp. 1–6. https://doi.org/10.1109/ICONSTEM56934.2023.10142575 (2023).
18. Venkatesh, S. P., Lalitha, K., Maheswaran, S. & Jeyanthi, P. Secure IoT with Blockchain for Industrial Application. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–6). IEEE. (2024).
19. Yuvarani, R. & Mahaveerakannan, R. Enhancing Cloud Computing Data Security in Attribute-based Encryption Schemes using Cryptographic Algorithm. In *2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN)* (pp. 660–666). IEEE. (2024).
20. Ramesh, P. S., Sudha, I., Jagannathan, J., Pandiarajan, R. & Ponmalar, A. Optimizing User Data Privacy and Confidentiality in Cloud Storage Systems Through Advanced Obfuscrypt Encryption Methods for Enhanced Security and Efficient Data Protection. In *2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)* (pp. 1–6). IEEE. (2024).
21. Sharma, T. et al. AES vs AES_GCM for Data Protection: A Comprehensive Security Comparison. In *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0. IEEE*, (2024).
22. Storj Labs. *Storj: A Decentralized Cloud Storage Solution* (Storj Labs Technical Paper, 2019).
23. Protocol Labs. Filecoin: A Decentralized Storage Network. Filecoin Technical Report. (2017).
24. Mahajan, H. B. Emergence of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems: solutions, challenges, and future roadmap. *Wireless Pers. Commun.* **126** (3), 2425–2446 (2022).
25. Attaran, M. Blockchain technology in healthcare: challenges and opportunities. *Int. J. Healthc. Manag.* **15** (1), 70–83 (2022).
26. Lodha, L. et al. A blockchain-based secured system using the internet of medical things (IOMT) network for e-healthcare monitoring. *Meas. Sens.* **30**, 100904 (2023).
27. Aouedi, O. et al. A survey on intelligent internet of things: applications, security, privacy, and future directions. *IEEE Commun. Surv. Tutorials* (2024).
28. Wang, Z., Qingqing, C. & Liu, L. Permissioned blockchain-based secure and privacy-preserving data sharing protocol. *IEEE Internet Things J.* **10** (12), 10698–10707 (2023).
29. Vidhya, S. & Kalaivani, V. A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme.*Peer-to-Peer Netw. Appl.* **16**(2), 900–913 (2023).
30. Xiang, X., Jin, C. & Fan, W. Decentralized authentication and access control protocol for blockchain-based e-health systems. *J. Netw. Comput. Appl.* **207**, 103512 (2022).
31. Bhansali, P. K. et al. Cloud-based secure data storage and access control for internet of medical things using federated learning. *Int. J. Pervasive Comput. Commun.* **20** (2), 228–239 (2024).
32. Pal, K. et al. *A Decentralized Privacy Preserving Healthcare Blockchain for Iot, Challenges, and Solutions. Prospects of Blockchain Technology for Accelerating Scientific Advancement in Healthcare*158–188 (IGI Global Scientific Publishing, 2022).

Author contributions
All the authors have contributed in an equal manner.

Declarations

Competing interests
The authors declare no competing interests.

Research involving human participants and/or animals
This article does not contain any studies with human participants or animals performed by any of the authors.

Additional information
Correspondence and requests for materials should be addressed to D.K.

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.