IMPROVING SECURITY: BLOCKCHAIN BASED IOT SOLUTIONS FOR THE HEALTHCARE

PAVITHRA P S[1], DURGADEVI P[2]

[1]Research scholar, Department of computer science and Engineering, SRM Institute of Science and Technology, vadapalani, Chennai-26, India
[2]Assistant Professor (S.G), Department of computer science and Engineering, SRM Institute of Science and Technology, vadapalani, Chennai-26, India
E-mail: [1] Pavithraps1296@gmail.com, [2]durgadep@srmist.edu.com

ABSTRACT

Blockchain and the IoT together provide a new paradigm with the potential to transform healthcare as we know it. This study delves into the revolutionary possibilities of blockchain technology as it pertains to healthcare IoT application security and optimization. Data security, integrity, and interoperability are major concerns with healthcare IoT devices since they produce large volumes of personal patient data. A strong answer to these problems is blockchain technology, which uses a distributed and unchangeable record. Integrity of data, audit trails that are easy to see, and safe information exchange among stakeholders are all possible with blockchain protocols in healthcare IoT systems, all while protecting patients' privacy and obtaining their consent. In addition, the article explores practical examples of healthcare IoT systems enabled by blockchain that have been shown to be beneficial. Secure patient data sharing among healthcare providers, tamper-proof administration of medical records, and supply chain authentication of medications are all examples. Also discussed are some of the restrictions and difficulties that come with using blockchain technology in healthcare IoT, including issues with scalability, regulatory compliance, and interoperability. We provide solutions to these problems and hope that they will encourage blockchain technology to proliferate throughout healthcare IoT networks.

Keywords: *IOT, Blockchain, Healthcare, Security, RSA Algorithm*

1. INTRODUCTION

The healthcare sector holds paramount significance for both rising and developed economies, since it directly influences the welfare and livelihoods of individuals, rendering it a crucial matter of concern. Continuous research and development in the Healthcare sector is vital as it contributes to enhancing the standard of living by combating a multitude of health conditions and diseases. The progress and current innovations in technology have led to noticeable enhancements in the Healthcare industry. The Healthcare and Medical Sector can enhance its current capabilities by incorporating cutting-edge computer technologies. These advanced technologies can aid doctors and medical professionals in the early detection of different diseases, significantly improving the accuracy of diagnosis in the initial stages.

Several cutting-edge computer technologies, such as the Internet of Things (IoT), Blockchain, Machine Learning, Data Mining, Natural Language Processing (NLP), Image Processing, and Cloud Computing, are already being implemented in various industries with remarkable outcomes [1].

The healthcare industry faces a significant difficulty in securely recovering and effectively managing the substantial volume of individual health data generated through service operations and regular commercial activities. The majority of health data is not readily accessible or standardized across systems, making it challenging to exchange, utilise, and comprehend. These data are gathered from multiple sources and housed in centralized IT systems, which makes it difficult to distribute and manage them. Effort and resources are necessary to create, receive, transmit, and solicit medical data [2]. Secure data retrieval and management facilitate healthcare systems in enhancing health outcomes, communication, treatment quality, and overall patient perspectives [3].

Blockchain technology is a highly praised technological innovation that is expected to profoundly transform human activities and relationships [4,5]. Consequently, scholars, programmers, and professionals have shown a heightened level of interest. Consequently, a multitude of platforms, systems, and prototypes are created. Bitcoin, Ethereum, and Hyperledger are prominent platforms that have had a significant impact on different aspects of blockchain utilisation.

The fundamental life cycle of IoT has four components: (1) Data is collected using sensors on devices; (2) The collected data is saved in the cloud for analysis; (3) The analysed data is then transmitted back to the device; and (4) The device responds accordingly. IoT has several applications, making our lives more comfortable. The key IoT applications include Smart Homes, Smart Cities, Agriculture, Smart Retail, Driverless Cars, and Healthcare. Security is essential for the effective running of IoT networks and all technologies. Current IoT security efforts focus on data confidentiality, authentication, access control, privacy, trust, and policy enforcement. IoT security difficulties stem from irresponsible programme design, resulting in vulnerabilities and network security concerns. [6].

IoT architecture requires physical initialization to prevent unauthorized receiver access. The IoT architecture has five layers: Perception, Network, Middleware, Application, and Business. Each layer has its own goals and challenges. Key IoT security goals include Confidentiality, Integrity, and Availability (CIA) [7]. There are four sorts of attacks in IoT based on vulnerabilities: "Physical attack," "Software attack," "Network attack," and "Encryption attack."

Blockchain, a distributed network, eliminates the need for third parties in transactions and communication [8]. Blockchain technology enables autonomous and segregated transactions, making cryptocurrencies a novel notion. Cryptocurrency is considered very safe and unhackable. The Block-chain concept can be applied to other networks to boost security. The Blockchain is a public distributed ledger system accessible to anyone. Blockchain records store data publicly and chronologically. Block is a container for transaction details. The blocks contain data, the hash of the preceding block, and the hash of the affected block. It consists of two parts: Header and Transaction Details. The header contains block-related information. A “Timestamp” records the creation time of the block. The “Difficulty level” determines the difficulty of mining a block. The “Merkle Root” reflects the fingerprints of all transactions in the block, whereas “NONCE” solves the mathematical riddle in the Proof-of-work algorithm.

Experts have used blockchain technology into the Industrial Internet of Things to enhance data security. [13–15]. Blockchain technology ensures Industrial Internet of Things data security and trust through decentralization, openness, transparency, and non-tampering. Blockchain smart contracts may be utilized to record encrypted agreements between industrial IoT devices, enabling automated execution and enhancing efficiency. The blockchain data layer stores data in a Merkle tree. The Merkle tree lacks non-member verification, necessitates substantial memory, and cannot be arbitrarily destroyed. Cryptographic accumulators, which have the potential to substitute Merkle trees in blockchains, have been increasingly popular in recent years. The accumulator's robust, universal, and compact qualities enable non-member proof, member deletion, and reduced data storage memory.

The widespread adoption of electronic services and applications has resulted in significant advancements in telecommunications networks and the advent of the Internet of Things (IoT). The Internet of Things (IoT) is a developing communication paradigm where devices function as objects or "things" that can detect their surroundings, establish connections with one other, and share data via the Internet [11,12]. By the year 2022, there will be a total of one trillion IP addresses or things that will be connected to the Internet via IoT networks [14].

The Internet of Things (IoT) concept has been lately employed to develop intelligent settings, including smart cities and smart homes, encompassing many application domains and associated services. The objective of creating smart settings is to enhance human productivity and comfort by addressing issues pertaining to the living environment, energy usage, and industrial requirements [15]. The intent is evident in the substantial proliferation of Internet of Things (IoT) services and applications across diverse networks. The Padova Smart City in Italy is a prime example of a successful use of Internet of Things (IoT) technology. [16].

2. RELATED WORKS

There are three tiers in a typical Internet of Things system [17]. The first layer is the perception layer, which is responsible for obtaining information about objects at any time and in any location. The second layer is the network layer, which is responsible for accurately transmitting the information about objects in real time through the integration of telecommunications networks and the Internet. The application layer, the third tier in the system, is responsible for processing the information gathered by the perception layer. Its main purpose is to enable practical applications such as intelligent identification, location, tracking, monitoring, and management. [18].

Blockchain is unquestionably a native invention of satoshi nakamoto. blockchain is a distributed ledger and online store that spans numerous peer-to-peer (P2P) machines, each of which is referred to as a "node" and contains every record of transactions that take place on the internet between P2P using the consensus procedure. hash functions that are encrypted enable distributed ledgers to work over the internet. peer-to-peer transactions via the consensus protocol are append-only, immutable, and unchangeable. blockchain allows activities to be documented without requiring trust from a third party. it is an effective method for verifiably and effectively documenting communications between both parties in an open setting.

Network allows for the recording of transactions without requiring confidence from a third party. it's a method for effectively and verifiably documenting communications across two parties in an open setting. It continuously tracks transactions and is aware of who has what at any given moment. when an arrangement takes place, it ensures that everything or property has one owner and that there are no dual uses occurring within the network blockchain technology has numerous qualities that make it clear, dependable, and secure. in our structure, we have used blockchain for security reasons so that information generated by Internet of Things (IoT) network sensors may be protected against any form of imitation.

2.1 Blockchain technology

Blockchain is widely acknowledged as the underlying technology powering the cryptocurrency Bitcoin [19]. Decentralization is a basic principle underlying the notion of a blockchain (fig1). Blockchain does not keep its databases in a single location. Instead, it replicates and distributes the blockchain across the network of members. Every computer connected to the network will update its blockchain to accurately reflect any changes that occur when a new block is added to the blockchain. The decentralized design possesses the advantages of being impervious to manipulation and devoid of vulnerabilities resulting from a singular point of failure. These benefits can guarantee the dependable and secure operation of the blockchain.

Essential components of Blockchain: Data block: A blockchain is a linear structure that starts with the genesis block and continues to each successive block linked in the chain. Each block has several transactions and is linked to its immediate predecessor block using a hash label. By adhering to this approach, it is possible to trace every block in the chain back to the previous one, rendering it unfeasible to modify or amend any data within a block. The fundamental structure of a data block format comprises of two main components: transaction records and a blockchain header. [19]. In this system, transaction records are arranged in a hierarchical structure known as a Merkle tree. Each leaf node in the tree represents a transaction made by a user of the blockchain. For instance, a user can request the inclusion of associated metadata to establish a transaction that is additionally authenticated using the user's private key to ensure trustworthiness. Simultaneously, the block header includes the subsequent information: (1) The block's hash is used for verification purposes. (2) The Merkle root is utilized to keep a collection of transactions within each block. (3) The nonce value is a number generated through the consensus process in order to construct a hash value that meets a specific difficulty level. (4) The timestamp indicates the exact time at which the block was formed.

A database that is shared and replicated between entities over a peer-to-peer network is called a distributed ledger. Anyone inside the blockchain ecosystem who is a network participant can access the shared database. In a distributed situation, network members can come to a consensus through a consensus process, doing away with the requirement for third parties to mediate transactions.

As nodes start exchanging or sharing data on the blockchain, there are no centralized entities in place to control transaction policies or safeguard data from security threats. This is because consensus algorithms govern the data sharing and exchange process. To avoid issues associated with counterfeiting, such as attacks involving double spending, it is crucial to confirm the legitimacy of the block, keep an eye on data flow, and facilitate safe information exchange. It is possible to fulfil these conditions by employing a verification mechanism that is known as a consensus algorithm.

When discussing blockchain technology, the term "consensus algorithm" refers to a procedure that is utilized to enable several untrustworthy nodes to reach a consensus on a single data block.

Bitcoin's blockchain is one example of a consensus-based application. Bitcoin's consensus process is based on a proof of work algorithm (PoW). [20,21] to maintain security in networks that are not trusted. Miners are responsible for running this algorithm.

Smart contracts refer to programmable applications that are designed to operate on a blockchain network. Smart contracts have gained significant attention in the blockchain industry since the introduction of Ethereum [22], the pioneering smart contract platform in 2015. This technology has developed as a very innovative field within the blockchain sector. When a person initiates a financial transfer by executing a smart contract, the funds will be immediately delivered across the blockchain network. The transfer details will be documented as a transaction and securely saved on the blockchain, which functions as an unchangeable record-keeping system. [23]. The smart contract is made immutable and immune to outside attack by using a self-executing protocol that is dependent on code. [24-26].

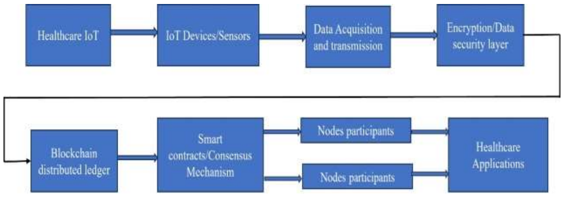
Healthcare IoT
IoT Devices/Sensors
Data Acquisition and transmission
Encryption/Data security layer
Blockchain distributed ledger
Smart contracts/Consensus Mechanism
Nodes participants
Nodes participants
Healthcare Applications

Figure 1: Basic Blockchain Based Healthcare Iot Architecture

2.1.1 Healthcare IoT:

It refers to the use of diverse IoT devices and sensors in the healthcare sector to gather patient data, including vital signs and other relevant information.

2.1.2 Data Acquisition and Transmission:

The gathered data is sent to the subsequent layer Encryption/Data Security Layer: The data is subjected to encryption and additional security protocols to guarantee its integrity and secrecy before being stored on the blockchain.

2.1.3 Distributed Ledger:

An immutable ledger is created by storing data in blocks over a decentralized network. This layer utilizes consensus processes and smart contracts to validate input and execute predetermined actions.

2.1.4 Nodes/Participants:

These are the entities that actively engage in the blockchain network by validating and appending blocks to the chain.

2.1.5 Healthcare applications:

The last stage in which healthcare-specific apps utilize blockchain data for different reasons such as managing patient records, tracking supplier chains, and handling invoicing.

2.2 IoT Architecture

The architecture of the Internet of Things (IoT) is comprised of a number of layers and components that make it possible for objects and systems to interact with one another when it comes to connectivity, communication, data processing, and other related activities (fig2). The following is an overview of the architecture in an overall manner.

2.3 Perception Layer (Sensing Devices):

2.3.1. Sensors and actuators

This layer comprises a diverse range of sensors, including temperature, humidity, and motion sensors, as well as actuators like as switches and motors. These components are responsible for gathering data and facilitating interactions with the physical environment.

2.3.2 Edge devices

These devices perform data preprocessing at the network edge before to transmitting it to the cloud or other layers for subsequent processing.

2.4 Network layer

2.4.1. Connectivity

The connectivity layer encompasses several communication protocols such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, etc., which facilitate the interconnection of devices with each other and with the internet.

2.4.2 Gateways

Intermediate devices serve as data aggregators, collecting information from various sensors or edge devices and transmitting it to higher layers. They have the capability to carry out protocol translation and data preparation.

2.5 Middleware layer

2.5.1 Data processing and management

Middleware platforms are responsible for receiving, storing, processing, and managing data that originates from the perception layer. They frequently incorporate features such as data analytics, filtering, and normalisation.

2.5.2. Device Management

Tools and platforms for configuring, monitoring, and managing devices, which also include firmware upgrades and security management.

2.6 Application layer

2.6.1 Applications and services

This layer encompasses a diverse range of applications and services that utilise IoT data for specific objectives. These applications can encompass a wide range of areas, including smart home technology, industrial automation, healthcare, and smart cities.

2.6.2 User interface

End-users engage with IoT systems via interfaces, typically accessed through mobile applications, online portals, or dashboards.

2.7 Security and privacy

2.7.1 Authentication and access control

Implementing stringent measures to restrict access to data and systems only to authorised devices and users.

2.7.2 Encryption and Data Integrity

Ensuring the confidentiality and integrity of data during its transit and storage to avoid unauthorised access or alteration.

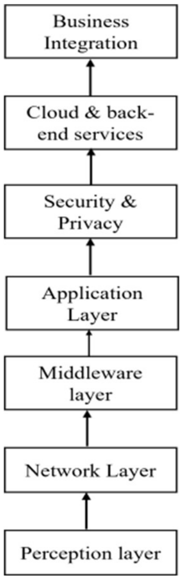

Figure 2. General Iot Architecture

2.8 Cloud and Backend Services

2.8.1 Storage and computing

Cloud services store vast amounts of data and offer computational resources for the purposes of data analysis, machine learning, and predictive analytics.

2.8.2 Backend infrastructure

Handles data routing, event processing, and orchestrating interactions between devices and applications.

3. RSA ALGORITHM

The RSA algorithm, coined after its creators Rivest, Shamir, and Adleman, is an asymmetric cryptographic method employed for the purposes of encryption, decryption, digital signatures, and key exchange. Below is a concise summary of the

3.1 RSA algorithm:

Security: The RSA security system is based on the challenge of factoring the result of multiplying two big prime integers (p and q) into their individual prime factors.

The strength of a system is directly proportional to the magnitude of the modulus (n), which is calculated by multiplying the prime numbers together.

3.1.1 Key Management:

The secure storage and effective administration of private keys are essential for ensuring security.

Private keys must be held securely and accessible exclusively by authorised entities.

3.1.2 Efficiency Concern:

The process of RSA encryption might require a significant amount of processing resources, particularly when using bigger key sizes. It is important to consider the performance and resource limitations while dealing with IoT devices.

3.1.3 Blockchain integration:

By including these RSA procedures into the design of the blockchain, the IoT healthcare system guarantees the safe storage, transfer, and verification of healthcare data.

3.2 Distributed Denial of Service (DDoS)

A distributed denial of service (DDoS) attack disrupts the regular flow of network traffic by overwhelming the targeted computer or server with an excessive amount of traffic, causing a traffic flood (fig 3). The attack referred to is the most commonly acknowledged one for wireless sensor networks and nodes connected to the Internet of Things (IoT) network. It results in the inefficient utilisation of network resources and restricts access to authorised users.

4. Proposed methodology

In an RSA-based blockchain system designed for IoT healthcare, every participant, including healthcare providers, IoT devices, and patients, possesses a cryptographic key pair consisting of a public key for encryption and a private key for decryption. The use of this asymmetric key configuration guarantees the establishment of secure communication channels across the whole network.

Patient-generated health data obtained from IoT devices is encrypted using a public key prior to transmission to the blockchain. Access and interpretation of the data may only be done by the authorized entity, usually the healthcare practitioner or the patient, as the matching private key is necessary for decryption. The utilization of this cryptographic procedure greatly boosts the level of data secrecy, thereby safeguarding sensitive medical information from unauthorized access.

Smart contracts, an essential aspect of blockchain technology, may utilize RSA encryption to ensure safe execution. By including predetermined regulations, these agreements can automate the process of managing consent, guaranteeing that patient information is only accessed and shared with specific authorizations. RSA encryption enhances the access control mechanisms included into smart contracts, hence strengthening the security and privacy of the healthcare ecosystem.

The blockchain functions as a decentralized and immutable ledger, which enhances the RSA encryption by preserving an unchangeable record of all transactions and data inputs. The openness and integrity of the system enhance the efficiency and reliability of auditing and tracking the movement of health data throughout the network.

4.1 Algorithm for key generation

1. Choose two separate prime numbers: p and q.
2. Calculate n = p * q (n is the modulus).
3. Calculate φ(n) as (p - 1) * (q - 1) (φ is Euler's totient function).
4. Choose an integer e with 1 < e < φ(n) and gcd(e, φ(n)) = 1 (e represents the public exponent).
5. Determine d as the modular multiplicative inverse of e modulo φ(n) (d represents the private exponent).

Public key: (n, e).
Private Key: (n, d).

4.2 Algorithm for Encryption

1. Convert the plaintext message M to a numerical representation m.
2. Calculate the ciphertext: c = m^e mod n.
3. Send or store the ciphertext c securely.

3.3 Algorithm for Decryption

1. Obtain the ciphertext c.
2. Calculate the plaintext message: m = c^d mod n.
3. Restore the numerical representation m to the original plaintext message M.

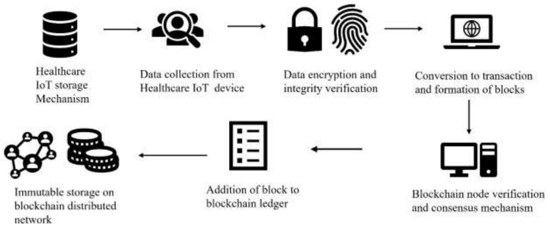
Healthcare IoT storage Mechanism
Data collection from Healthcare IoT device
Data encryption and integrity verification
Conversion to transaction and formation of blocks
Blockchain node verification and consensus mechanism
Addition of block to blockchain ledger
Immutable storage on blockchain distributed network

Figure 3. Proposed Blockchain Based Iot Healthcare Storage Mechanism

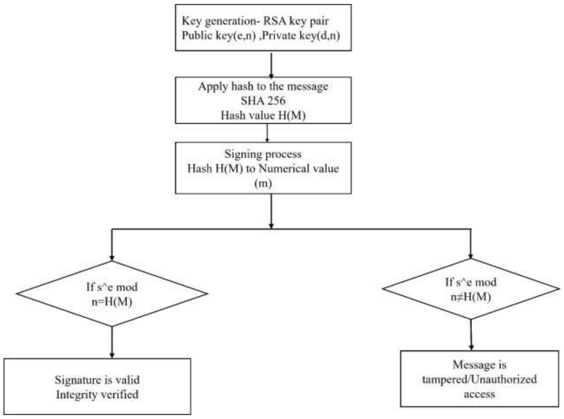

Figure 4. RSA Digital Signature Generation

RSA digital signatures offer authenticity, integrity, and non-repudiation, guaranteeing that the sender of the communication cannot dispute their role in sending it. Preceding the signing process with hashing guarantees that the content of the communication remains undisclosed within the signature and minimizes the computational burden (fig 4). The security of a system is highly dependent on the correct creation, administration, and safeguarding of private keys.

5 Results and discussion

Although recognised for its resilience and safeguarding capabilities, blockchain technology is nevertheless susceptible to specific forms of attacks. Notable instances of assaults and weaknesses in blockchain systems encompass. The architecture of a Blockchain-based Intrusion Detection System (BIoTIDS) incorporates several approaches and techniques to guarantee strong security, efficient detection of intrusions, and dependable integration of blockchain technology in IoT contexts.

In the typical scenario, where there is no network attack, we used five nodes, N1 through N5, and their initial 10 requests, as shown in Table 1 above. Each node received ten queries from N1 to N5, resulting in the development of Algorithm 2. A pseudo-code for a Distributed Denial of Service (DDoS) Attack Intrusion Detection System (IDS) for Internet of Things Networks that uses Blockchain database query requests and accompanying l values of 103, 59, 122, 51, and 63 will be saved in blocks created by each node. The values of t from N1 to N5 are 77.25, 41.3, 91.5, 38.25, and 47.25 milliseconds. This means that the threshold request time, t, is expected to be 75% of l. In other words, node N1 submitted the first request 95 milliseconds later, then the second request 100 milliseconds later, the third request 90 milliseconds later, and so on. Figure 5 depicts the initial request for N1 through N5, as well as the request time and total number of queries. Following this initial data, the average request time l is updated with each request issued by nodes. This happens after the initial data is collected. Now that the initial data has been obtained, each node will send out additional requests, as illustrated in Table 2. After receiving ten more requests, BIoTIDS calculated the average amount of time each node took to process them. Figure 6 shows the average time it takes nodes to react to requests for more information. Figure 6 clearly shows that the average request time for node N2 was 18 milliseconds, which is less than 75% of its initial average request time of 65 milliseconds, and matches the threshold value of 48 milliseconds. IDS detects that node N2 is making malicious requests more frequently than usual, and it issues an alert to the administrator of the Internet of Things network, indicating that node N2 is infected or under DDoS attack since it is operating abnormally. This is because N2's l value is less than the threshold request time of 48 milliseconds. IoT network managers can remove N2 from the network and cease all operations; nevertheless, until it is fixed, N2 will continue to make 38 requests. In this case, only one node was affected, and BIoTIDS identified it. However, BIoTIDS may identify several infected nodes at the same time. As a result, it is obvious that the BIoTIDS framework is capable of detecting assaults on Internet of Things networks; hence, the proposed framework operates in compliance with the design specifications.

Table 1: Data Provided For Various Nodes

Number of Requests/Node	Node 1	Node 2	Node 3	Node 4	Node 5
1	95	60	130	50	74
2	100	65	115	45	68
3	105	50	120	60	66
4	90	55	110	55	62
5	110	57	116	47	72
6	115	63	124	53	60
7	105	62	128	50	52
8	95	58	118	48	58
9	100	60	130	53	52
10	110	62	126	52	64
Average Request time (Tavg)	102.5	59.2	121.7	51.3	62.8

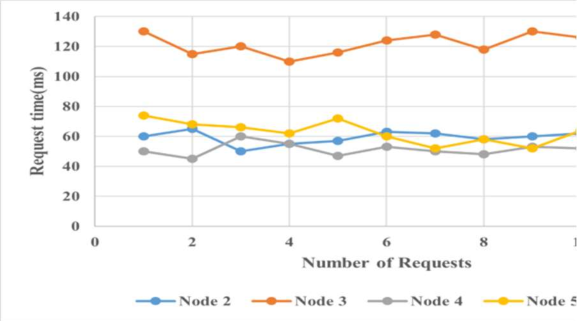

Figure 5. First-time query format

6. Mitigation Strategies

To mitigate Distributed Denial of Service (DDoS) attacks, a comprehensive strategy is employed to minimise the adverse effects of these attacks on networks, systems, and services. Below are a number of highly effective mitigating strategies.

6.1 DDoS Detection and Monitoring

6.1.1 Anomaly detection mechanisms

Deploy surveillance tools and anomaly detection systems to detect atypical traffic patterns that may suggest the presence of a Distributed Denial of Service (DDoS) attack.

6.1.2 Traffic monitoring

Perpetually observe network traffic to detect any abnormal surges in volume, patterns, or origins of traffic.

Table.2 Assessing Nodes For Each Data Point

Number of Requests/Node	Node 1	Node 2	Node 3	Node 4	Node 5
1	104	28	124	64	82
2	106	26	136	62	74
3	116	30	104	52	54
4	118	32	122	54	46
5	126	24	106	46	62
6	102	22	112	54	64
7	96	20	132	46	42
8	104	18	138	44	46
9	102	16	76	42	84
10	110	24	78	46	86
Average Request time(Tavg)	108.4	24	112.8	51	64

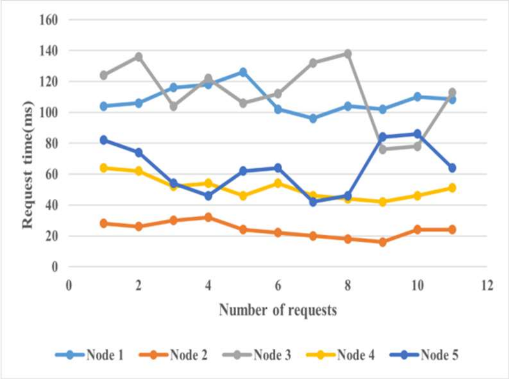

Figure.6 Assessment of the BIoTIDS Framework

6.2 Cloud-based Protection Services

Employ DDoS mitigation services provided by cloud providers or specialised DDoS protection firms that can effectively absorb and filter harmful network traffic.

6.3 Distributed Defense Mechanisms

Sinkholing involves redirecting hostile traffic to a controlled environment, known as a "sinkhole," for the purpose of analysis and neutralisation.

Coordinated Response: Engage in collaboration with Internet Service Providers (ISPs), Computer Emergency Response Teams (CERTs), and other organisations to exchange information about potential threats and synchronise activities in responding to them.

6.4. Network Infrastructure Enhancement

Scalable Architecture: Create network designs that can easily accommodate unexpected increases in traffic by utilizing Content Delivery Networks (CDNs) or cloud-based services to evenly spread the load.

Firewalls and Access Control Lists (ACLs): Set up firewalls and ACLs to effectively screen and prevent traffic from suspected or identified harmful origins.

7. CONCLUSION

The potential of healthcare IoT solutions based on blockchain technology is significant. The adoption of this technology has the potential to enhance connectivity, security, and patient-centeredness in the healthcare system as it progresses and overcomes challenges. Blockchain technology has the potential to improve patient outcomes, streamline processes, and establish a healthcare environment that is both more efficient and transparent, thereby transforming the healthcare industry. Distributed Denial of Service (DDoS) is the most common and harmful threat to an Internet of Things (IoT) network infrastructure, making it vulnerable to its effects. To address this issue, we developed an intrusion detection system using blockchain technology. Each block contains requests for data from IoT nodes. The study finishes by emphasizing the significant capacity of blockchain technology to revolutionize healthcare Internet of Things (IoT) applications. Blockchain technology enables the creation of a healthcare environment that is safer, more integrated, and focused on the needs of patients. It provides unparalleled efficiency, transparency, and security. To effectively leverage blockchain's disruptive powers in healthcare IoT, further study, collaboration, and the establishment of standardized protocols to overcome existing difficulties are required.

REFERENCES

[1] J. M. Kizza, “Internet of things (iot): growth, challenges, and security,” in Guide to Computer Network Security, pp. 517– 531, Springer, Berlin, Germany, 2017

[2] Clim, A.; Zota, R.D.; Tinica, G. Big Data in home healthcare: A new frontier in personalized medicine. Medical emergency services and prediction of hypertension risks. Int. J. Healthc. Manag. 2019, 12, 241–249.

[3] Attaran, M. Blockchain technology in healthcare: Challenges and opportunities. Int. J. Healthc. Manag. 2022, 15, 70–83

[4] Aste T, Tasca P, Di Matteo T. Blockchain technologies: the foreseeable impact on society and industry. Computer 2017;50(9):18–28. https://doi.org/10.1109/ MC.2017.3571064.

[5] P. De Filippi, M. Mannan, and W. Reijers, “Blockchain as a confidence machine: the problem of trust & challenges of governance,” Technol Soc, vol. 62, p. 101284, Aug. 2020, doi: 10.1016/j.techsoc.2020.101284.

[6] P. Gokhale, O. Bhat, and S. Bhat, “Introduction to IOT,” International Advanced Research Journal in Science, Engineering and Technology, vol. 5, no. 1, pp. 41–44, 2018.

[7] M. A. J. Jamali, IoT Architecture Towards the Internet of ings, pp. 9–31, Springer, Berlin, Germany, 2020.

[8] J. Wang, W. Chen, L. Wang, Y. Ren, and R. Simon Sherratt, “Blockchain-based data storage mechanism for industrial internet of things,” Intelligent Automation & Soft Computing, vol. 26, no. 5, pp. 1157–1172, 2020

[9] Y. J. Ren, F. J. Zhu, P. K. Sharma, T. Wang, J. Wang et al., “Data query mechanism based on hash computing power of blockchain in Internet of Things,” Sensors, vol. 20, no. 1, 207, 2020.

[10] J. Ren, Y. P. Liu, S. Ji, A. K. Sangaiah and J. Wang, “Incentive mechanism of data storage based on blockchain for wireless sensor networks,” Mobile Information Systems, vol. 2018, pp. 1–10, 2018

[11] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad and J. Wang, “Blockchain enabled distributed security framework for next generation IoT: An edge-cloud and software defined network integrated approach,” IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6143–6149, 2020.

[12] King J, Awad AI (2016) A distributed security mechanism for resource-constrained IoT devices. Informatica (Slovenia) 40(1):133–143

[13] Weber M, Boban M (2016) Security challenges of the internet of things. In: 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, Opatija. pp 638–643

[14] Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, Vienna. pp 84–90

[15] Kafle VP, Fukushima Y, Harai H (2016) Internet of things standardization in ITU and prospective networking technologies. IEEE Commun Mag 54(9):43–49

[16] Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32

[17] B. Yin and X. T. Wei, “Communication-efficient data aggregation tree construction for complex queries in IoT applications,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3352–3363, 2018.

[18] Q. Wang and Y. G. Wang, “Research on power Internet of Things architecture for smart grid demand,” in 2018 2ndIEEE Conf. on Energy Internet and Energy System Integration (EI2), Beijing, pp. 1–9, 2018

[19] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen and B. C. Ooi, “Untangling blockchain: A data processing view of blockchain systems,” IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366–1385, 2018.

[20] Z. Q. Xia, J. J. Tan, J. Wang, R. L. Zhu, H. G. Xiao et al., "Research on fair trading mechanism of surplus power based on blockchain," Journal of Universal Computer Science, vol. 25, no. 10, pp. 1240–1260, 2019.

[21] J. Y. Zhang, S. Q. Zhong, T. Wang, H. C. Chao and J. Wang, "Blockchain-based systems and applications: A survey," Journal of Internet Technology, vol. 21, no. 1, pp. 1–14, 2020.

[22] K. Christidis and M. Devetsik IoT is, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[23] W. Wang, D. T. Hoang, P. Hu, Z. Xiong and D. Niyato, "A survey on consensus mechanisms and mining strategy management in blockchain networks," IEEE Access, vol. 7, pp. 22328–22370, 2019.

[24] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," IEEE Access, vol. 7, pp. 77894–77904, 2019.

[25] Y. J. Ren, Y. Leng, Y. P. Cheng and J. Wang, "Secure data storage based on blockchain and coding in edge computing," Mathematical Biosciences and Engineering, vol. 16, no. 4, pp. 1874–1892, 2019.

[26] Y. Yu, Y. Li, J. Tian and J. Liu, "Blockchain-based solutions to security and privacy issues in the Internet of Things," IEEE Wireless Communications, vol. 25, no. 6, pp. 12–18, 2018.