[1]Dr. Nidhi Ranjan

[2]Dr. Balasaheb Balkhande

[3]Madhuri Ghuge

[4]Bhawana S. Dakhare

[5]Dr. Bhawna Ruchi Singh

[6]Dr. Anuradha Shukla

Efficient and Secure Blockchain-Based Access Control for Fog-Assisted IoT Cloud in Electronic Medical Records Sharing

Abstract: **-** Fog-assisted IoT Cloud environments have emerged as a result of the rapid spread of Internet of Things (IoT) devices and the requirement for seamless data sharing in the healthcare industry. The effective and safe management of access control to sensitive data, such as Electronic Medical Records (EMRs), becomes crucial in such configurations. The Efficient and Secure Blockchain-Based Access Control (ESBAC) framework, designed specifically for Fog-assisted IoT Cloud scenarios in EMR sharing, is our creative approach to this problem. The ESBAC architecture makes use of the blockchain's openness and immutability to provide reliable access control and auditability. The implementation of a consortium blockchain includes participants including healthcare providers, patients, and authorised entities. Each EMR has a smart contract attached to it that specifies access restrictions and permissions to make sure that only authorised parties are able to access and edit the data. Because of the decentralisation provided by the blockchain, security and privacy are improved because no single party has overwhelming control. Proposed framework uses attribute-based access control and lightweight encryption methods to provide a fair trade-off between security and efficiency. As a result, there can be fine-grained access control policies with the least amount of computing overhead. Comprehensive simulations are used to evaluate the suggested solution and compare it to current methods. The outcomes show that ESBAC improves security in EMR sharing and greatly lowers access latency.

Keywords: lightweight weight Encryption, IoT Fog layer, Medical Record, Blockchain, Access Control

I. INTRODUCTION

Medical histories, diagnoses, treatment plans, and other private and sensitive information about patients are all contained in electronic medical records. To preserve patient privacy and adhere to laws like the Health Insurance Portability and Accountability Act (HIPAA), it is crucial to guarantee the confidentiality and integrity of this data. In order to make wise judgements, healthcare professionals, authorised staff, and patients themselves need fast access to pertinent EMRs. Due to the dynamic and heterogeneous nature of IoT Cloud settings, traditional access control approaches, such as role-based access control, have limits when addressing their complexity. In order to overcome the issues of latency, bandwidth, and real-time processing in IoT ecosystems, fog computing has emerged as a potential paradigm. Fog nodes can be installed near the network's edge to process data closer to its source, lowering latency and improving responsiveness. This design is especially important for healthcare

[1] Associate Professor, Vasantdada Patil Pratishthan's College of Engineering & Visual Arts, Mumbai

Mumbai University, Maharashtra, India

[2]Associate Professor, Vasantdada Patil Pratishthan's College of Engineering & Visual Arts, Mumbai

Mumbai University, Maharashtra, India

[3]Assistant Professor, Bharati Vidyapeeth college of Engineering, Navi Mumbai, Mumbai University, Maharashtra, India.

[4]Assistant Professor, Bharati Vidyapeeth college of Engineering, Navi Mumbai, Mumbai University, Maharashtra, India

[5]Department of Applied Science, Bharati Vidyapeeth college of Engineering Navi mumbai, Maharashtra, India

[6]Narsee Monjee Institute of Management Studies, Navi Mumbai, Maharashtra, India

nidhipranjan@gmail.com[1], balkhandeakshay@gmail.com[2], madhurighuge27@gmail.com[3], bhawanadakhare@gmail.com[4], bhawnasingh77@gmail.com[5], anuradha.shukla@nmims.edu6

applications since prompt access to patient data might have an impact on clinical judgements. To maintain efficiency and security, it is necessary to address new difficulties brought on by the integration of fog computing into the access control system, such as node heterogeneity and shifting network conditions.

Due to its intrinsic qualities of openness, immutability, and decentralised consensus, blockchain technology has attracted a lot of attention. These characteristics make it a good choice for creating safe and impermeable access control systems. Blockchain can offer an auditable and accountable record of access events in the context of EMR sharing, boosting openness and accountability in data handling. A smart contract that establishes access restrictions depending on the characteristics of the requesting entity can be attached to each EMR, enabling fine-grained control over data access. Data mining is essential to the growth of the digital economy across a range of business models and sectors [1]. These data come from a variety of smart technology applications, including smart agriculture, smart cities, and healthcare. However, maintaining privacy and security for data mining records continues to be an important research area. Notably, wearable sensors and gadgets are being used in IoT-based smart healthcare to track patients' vital signs [2].

On the other hand, the study described in [3] sought to solve security and intrusion issues. Incorporating a bio-sensor to collect real-time patient health data that is then securely stored in the blockchain, their suggested solution combines blockchain technology and the Internet of Things (IoT) model. Given the sensitivity of the generated personal information, this biosensor technique enables precise, tamper-proof data storage, which is very important. However, this strategy poses latency limitations and lacks location awareness. Conventional smart health ecosystems frequently rely on cloud analysis and storage [4].Furthermore, time-sensitive scenarios cannot be accommodated by these centralised cloud solutions. For instance, quick access to patient data is essential in life-threatening medical circumstances like heart attacks [5].

Designing, creating, and evaluating an Efficient and Secure Blockchain-Based Access Control (ESBAC) framework specifically for Fog-assisted IoT Cloud contexts in EMR sharing is the main goal of this project. The following major issues are addressed by the framework:

- Efficiency: Taking into account the dispersed nature of fog computing and the potential overhead of blockchain consensus methods, the access control mechanism must function effectively to provide timely access to EMRs. It's critical to strike a balance between security and effectiveness.
- Security: Maintaining data integrity and protecting patient privacy are of utmost importance. To guard against unauthorised access, manipulation, and data breaches, the framework must have strong mechanisms for authentication, authorisation, and encryption.
- Fog-assisted IoT Cloud systems are dynamic by nature, with shifting network circumstances, device capabilities, and the importance of data. While preserving its security guarantees, the architecture must change to account for these dynamics.
- Scalability: The framework must be scalable to meet the growing demand for access control services without sacrificing performance as the number of IoT devices and EMRs increases.

Major Contribution:

By putting out a cutting-edge strategy that combines blockchain technology, fog computing, and adaptive consensus mechanisms to address the issues mentioned above:

- This study hopes to advance the fields of healthcare IoT and access control.
- The ESBAC framework is anticipated to offer a comprehensive solution that guarantees effective and safe access control in IoT Cloud environments with Fog assistance for EMR sharing.
- The performance and effectiveness of the framework will be compared to current methods through thorough simulations and comparative analyses.

II. REVIEW OF LITERATURE

In the context of IoT cloud systems, numerous cryptographic approaches have been put forth to enable secure and precise data transfer. These initiatives have mostly aimed to increase the effectiveness and security of data manipulation through creative methods.For instance, in a study [14], a novel strategy was used in which the procedures of signing, verifying, and decrypting data gathered from IoT devices were contracted out to a fog layer. By using this method, the signature's length was greatly shortened and its independence from the number of

related attributes was ensured. Encryption, however, remained a computationally demanding job carried out on the IoT side.Similar to this, another research project [3] presented an access control method based on CP-ABE (Cipher-Policy Attribute-Based Encryption) to safeguard IoT data in a cloud context. In this case, the cloud server used a user-specific transformation key to carry out a sizable portion of partial CP-ABE decryption. This key allowed authorised users to retrieve plaintext data from partially decrypted ciphertext by tightly tying identification attributes to the keyholder. CP-ABE and cloud storage integration has also been studied in other studies. A CP-ABE-based storage approach, for instance, [15] sought to improve secure access for IoT data in a cloud service. By outsourcing decryption to a cloud server and streamlining the public key storage with an attribute authority management module, this technique decentralised decryption.

In a recent project [2], the full CP-ABE decryption process was outsourced to a trusted proxy in the cloud, with the focus being on data sharing in mobile cloud computing. Utilising a symmetric key generated during decryption reduced the amount of user engagement in decryption. The focus of this study, however, was not external encryption. To protect item-level data during cloud-assisted IoT data transfers, a tag-aided encryption technique [16] been suggested in the context of industrial IoT. For safe transfer of IoT records, participants were given item keys. Furthermore, other cases [17] [18] addressed the security of data transmission and aggregation from IoT devices, particularly in the healthcare industry, despite the fact that these approaches typically lacked fine-grained access control to encrypted IoT data. Blockchain technology and cloud computing have recently been combined in projects to provide effective data sharing systems and decentralised access control.

A series of informative blocks, each carrying time-stamped and unchangeable records, is referred to as a "blockchain" [8,9]. For the sake of keeping records, this technology effectively functions as a digital ledger system [10, 11, 12]. Each block's data storage is protected from hacking and breaches [10,11,12]. Information on the blockchain is accessible by network members due to its transparency. Blockchains fall into two categories: public blockchains and private blockchains. Public blockchains, also known as permission less blockchains, are accessible to everyone, whereas private blockchains, also known as permissioned blockchains, restrict access to registered members. A worry that is particularly pertinent to healthcare frameworks covered by privacy requirements like HIPAA or GDPR [15] is that public blockchains are unable to sufficiently secure the confidentiality and privacy of sensitive health data [13,14].

III. METHODOLOGY

The patient has the right to own their own health information because they are the actual owner of the data. This control includes the power to distribute the data as required. Smart contracts can be used to construct a strong access control system that uses SPAKE, or secure password authentication-based key exchange. With this in place, patients can grant access to their Electronic Health Records (EHRs) to particular people or organisations.After receiving authorization, a patient can give healthcare practitioners access to their electronic health records. The EHR can only be accessed by healthcare practitioners with their express agreement thanks to this permission-based approach. The use of blockchain technology to preserve EHR hashes and crucial features underpins the procedure. The InterPlanetary File System (IPFS) will be used to securely store the actual records, regardless of their format in different document kinds. The main goal of this research project is to build an EHR system that is focused on the needs and preferences of the patient. The main obstacle to attaining this goal is creating reliable access control methods while protecting the confidentiality of shared and accessible data.

Blockchain technology has recently emerged as a game-changing solution that cuts across several industries. Blockchain has a lot of potential in the field of Healthcare Informatics (HI), given the demand for patient-centric systems and the necessity to link various healthcare systems. The potential of blockchain resides in its ability to successfully handle security and privacy issues in healthcare systems.

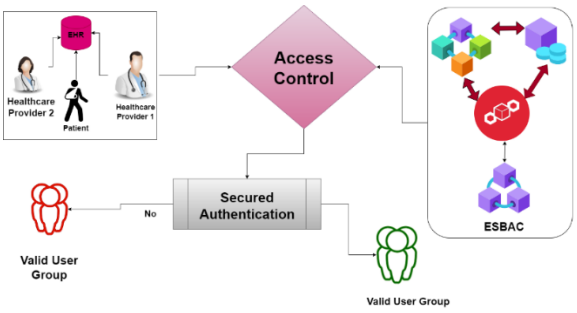

Figure 1: Architecture of secure authentication system for HER

This context serves as the backdrop for the research described here, which explores the area of blockchain-based healthcare data management with a primary focus on the sharing of Electronic Health Record (EHR) data between research studies and healthcare providers. This study intends to offer insightful information about improving data management practises in the healthcare industry by harnessing the inherent benefits of blockchain technology. In addition to ensuring improved security, the use of blockchain in healthcare data sharing also promotes a patient-centric mindset, which aids in the ongoing development of healthcare services.

A) Electronic Health Record (EHR) Data Storage:

The administration of patient health-related data in a secure, organised manner in a digital format is referred to as electronic health record (EHR) data storage. To enable successful healthcare delivery, decision-making, and research, it entails gathering, organising, storing, and retrieving a wide range of health data in a standardised manner. Electronic health records (EHRs) have many benefits over traditional paper-based medical records, including better accessibility, data exchange, accuracy, and efficiency.

The main components of EHR data storage:

- Data Entry: The process of storing EHR data begins with the gathering of various kinds of health data. Demographic information about the patient (name, age, gender), medical history, medications, allergies, test results, imaging studies (such as X-rays and MRI scans), treatment plans, progress notes, and more are included in this. This data is directly entered into the computer system by healthcare experts, ensuring that it is captured swiftly and properly.EHR data is maintained in a structured format that makes it possible to enter and categorise information in a consistent manner. This guarantees that various healthcare professionals can comprehend and interpret the data uniformly, improving collaboration and treatment continuity.
- Database Systems: Electronic databases, which can be housed on-site on the servers of a healthcare facility or in cloud-based environments, are where EHR data is kept. Data integrity, security, and effective retrieval are ensured by contemporary database management systems.
- Scalability: EHR systems must be scalable to meet the expanding data requirements of healthcare organisations due to the daily increase in the volume of health data created. Scalable storage choices that can be increased as needed are frequently provided by cloud-based solutions.
- Audit: Strong EHR systems keep audit trails, which keep track of who accessed a patient's records, what modifications were made, and when those changes took place. Enhancing transparency and assisting in the detection of any unauthorised activity, this accountability feature.

B) Blockchain-Based Model:

Enhancing data security, privacy, accessibility, and openness within the healthcare ecosystem is possible with a blockchain-based paradigm for protecting Electronic Health Records (EHR). Blockchain overcomes the problems with conventional EHR data storage, such as unauthorised access, data breaches, and a lack of interoperability, by using a decentralised and tamper-proof ledger system.

- Decentralised ledger and distributed computing: Blockchain works on a decentralised network of nodes, preventing total data control by a single party. A distributed ledger is created by each participant (node) maintaining a copy of the whole blockchain. As a result, there is no single point of failure and it is very challenging to change or manipulate data without network consensus.

- Data encryption: To increase the security of the blockchain, EHR data is encrypted before being added to it. The data can only be accessed by authorised individuals who have the proper decryption keys. The additional degree of security provided by this encryption helps prevent unauthorised access.
- Consensus Mechanism: To validate and reach consensus on the veracity of transactions or data additions to the chain, blockchain uses consensus processes (such as Proof of Work, Proof of Stake, or variants thereof). This consensus minimises the possibility of fraudulent activity by ensuring that only legitimate and authorised transactions are recorded on the blockchain.
- Smart contracts are self-executing agreements with established terms and conditions. They use predetermined triggers to automate processes. Smart contracts can implement access control regulations in a blockchain-based EHR paradigm, making sure that only authorized parties can access particular EHR data.
- Immutable Records: It is nearly impossible to change or remove data after it has been added to the blockchain. Because of its immutability, EHR data is guaranteed to be accurate, making it a trustworthy source of information for healthcare professionals.
- Privacy and Access Control: Blockchain enables granular access control for EHR data. A special private key is given to each user, enabling access to their records. Based on certain requirements and user responsibilities, access rights can be given or denied. This system makes sure that only those with permission can access the information they require.
- Real-time auditing of transactions and data access are made possible by the transparency of blockchain. A visible and verifiable audit trail is produced by the blockchain, which records all alterations and interactions with the EHR data.

Blockchain can make it easier for various healthcare systems and organisations to communicate with one another. Authorised parties can safely access patient data across platforms using standardised protocols and APIs, improving patient care coordination.

IV. PROPOSED METHODOLOGY

A) Background of ESBAC System:

According to the suggested system design, web apps for a single company would be developed using a user-permissioned blockchain powered by Hyperledger Composer and built on Hyperledger Fabric. The operations of the organisation will be improved by this architecture in terms of data security, accessibility, and transparency. Three peer nodes are strategically placed throughout the organisation to perform various functions. One of these nodes performs the role of a validating peer node, guaranteeing the veracity and authenticity of transactions. The two remaining nodes are dedicated ordering nodes in charge of handling transaction ordering and registering stakeholders. The InterPlanetary File System (IPFS) is used by the system to provide effective and distributed data storage. With the help of this technology, numerous peer nodes can access the same database, enhancing data availability and reliability throughout the company. A data certificate authority is included into the architecture to guarantee data security and integrity. It creates digital certificates to verify the legitimacy of data transfers. The shared ledger is updated in a crucial way by smart contracts, which are self-executing contracts. Both operations are automated and established business rules are enforced.

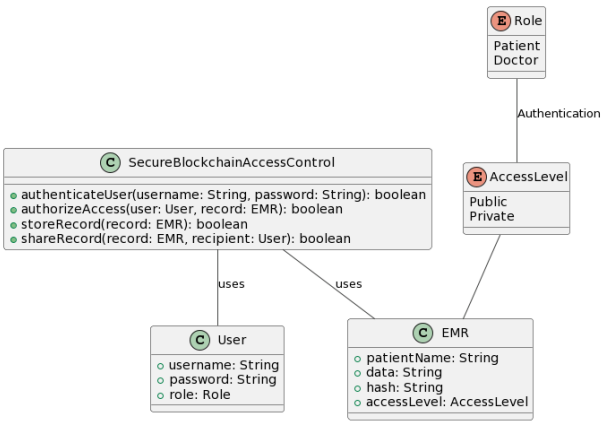

Figure 2: Flowchart architecture of proposed system

A Membership Service Provider (MSP) is a system that controls the identities and access rights of network users. It makes sure that the blockchain can only be accessed by those who are authorised. The blockchain network is connected using a solo order node. In order to ensure that all nodes are in agreement before storing data on the blockchain, this node allows the transmission of transactions and consensus across the network. The architecture supports the insertion of several peer nodes on various machines. Scalability testing is made possible by this capability, which aids in assessing the system's performance in various scenarios. This is essential to ensuring that the network can manage growing demands and loads. The network's components are designed and managed using Hyperledger Composer. The communication between peer nodes in this design is streamlined by a single channel. For network processing, transactions are started and forwarded to PE0, PE1, and PE2 as well as other peer nodes.A Health Record (HR) chain network can be created using blockchain technology thanks to its architecture. Each block in the blockchain's chronological chain contains hashed information regarding modifications made to the system. The data's immutability and transparency are guaranteed by this audit trail.

B) Blockchain-Based Access Control (ESBAC) framework:

The workload connected to a certain transaction, designated as $Transaction\_Workload$, makes up the majority of the block of a ledger record that is relevant to a patient's health record. Also included are the current transaction's specifics ($marked\ as\ Current\_Transaction\_Details$) and the previous transactions' hash values ($designated\ as\ Previous\_Transactions\_Hash$). It is possible to compute the burden of the block effectively by using these elements.

Algorithm: Using SHA-256 to Create and Update Health Records in Secure Blockchain Transactions

Step 1: Initialization:

- Start with the information to be entered or modified in the health record.
- Create an empty string at the beginning to hold the timestamps and concatenated data.
- Create a transaction object and fill it with information about the health record.

Step 2: Data addition:

- Combine the newly acquired or updated data with the information already present in the health record.
- Add a timestamp once the data has been concatenated.

Step 3: Determine Hash:

- Use the SHA-256 algorithm to determine the hash value of the concatenated data (data + timestamp).

$\boldsymbol{Function\ SHA-256(message)}$:

$\boldsymbol{Initialize}$:

$constants\ for\ SHA-256$

$Initialize\ initial\ hash\ values\ (h0, h1, h2, h3, h4, h5, h6, h7)$

$\boldsymbol{Pre-processing}$:

$Pad\ the\ message\ to\ ensure\ it's\ a\ multiple\ of\ 512\ bits\ (64\ bytes)$

$For\ each\ 512-bit\ chunk\ in\ the\ padded\ message$:

$Prepare\ message\ schedule\ (W[0]\ to\ W[63])$

$Initialize\ working\ variables\ (a, b, c, d, e, f, g, h)\ with\ the\ current\ hash\ values$

$\boldsymbol{Compression}$:

$For\ t = 0\ to\ 63$:

$Calculate\ working\ variables\ using\ logical\ and\ arithmetic\ operations$

$Update\ working\ variables$:

$$t1 = h + \Sigma 1(e) + Ch(e,f,g) + K[t] + W[t]$$

$$t2 = \Sigma 0(a) + Maj(a,b,c)$$

$$h = g$$

$$g = f$$

$$f = e$$

$$e = d + t1$$

$$d = c$$

$$c = b$$

$$b = a$$

$$a = t1 + t2$$

Update hash values:

$$h0 = h0 + a$$

$$h1 = h1 + b$$

$$h2 = h2 + c$$

$$h3 = h3 + d$$

$$h4 = h4 + e$$

$$h5 = h5 + f$$

$$h6 = h6 + g$$

$$h7 = h7 + h$$

$Concatenate\ hash\ values\ h0\ to\ h7\ to\ get\ the\ final\ hash$

$Return\ the\ final\ hash$

$End\ Function$

Establish Transaction:

- Create a new transaction containing the following information:
- Metadata (patient ID, date, etc.) concerning the medical record
- The sender's digital signature verifies their identity.
- timestamp for transactions

Access Management:

- Using digital signatures and access constraints, confirm the sender's identity.
- Verify the sender's consent to the health record change.

Interaction with Blockchain:

- The secure blockchain ledger will now include the transaction.
- To verify the consensus, broadcast the transaction to participating nodes.
- Verification of the consensus
- Through consensus processes, the participating nodes confirm the transaction.

- Verify access controls, transaction integrity, and sender authenticity.

Update Method:

- If consensus is reached and the transaction is valid:
- Put the updated information and timestamp in the health record.
- In the blockchain, save the fresh SHA-256 hash.

Updates and verification:

- The current hash should be retrieved from the blockchain when updating the health record.
- Combine the newly updated data with the information already included in the health record.
- Add a fresh timestamp after the data has been concatenated.
- compute the new concatenated data's SHA-256 hash.
- Hashes in comparison
- The hash that was calculated and the hash that was recorded in the blockchain.
- The update is valid if the hashes match, indicating that the data has not been altered.

A blockchain update:

- Make a new transaction with the updated hash and the necessary metadata.
- The safe blockchain should now contain the transaction.

Encryption and Access Control:

- To limit who can read and make changes to health records, implement strong access control methods.
- To ensure privacy, think about encrypting important information in the health record.

Protected Communication

- Establish secure routes of communication for the parties to the transaction.
- Encryption and other security measures can be used to protect data while it is being transmitted.

C) Secure Password Authentication-Based Key Exchange:

A cryptographic protocol called Secure Password Authentication-Based Key Exchange (SPAKE) enables two parties to safely create a shared secret key based on their unique passwords. In situations when users want to identify themselves and create a secure communication channel without actually sending their credentials over the network, it is especially helpful. SPAKE's main objective is to keep the passwords themselves secret while ensuring that the shared secret key is derived from both parties' passwords. This is accomplished by means of a sequence of interactive actions that incorporate cryptographic operations and calculations.

A high-level summary of the SPAKE protocol is provided below:

Setup:

- Alice and Bob each have their own unique password.
- It is decided to use a hash function that is widely used (like SHA-256).

Initialization:

- From their individual passwords, Alice and Bob each independently compute a commitment (commit).
- The process of commitment converts a password into a value without revealing anything about the password itself.

Transfer of Promises:

- Bob and Alice switch off their commitments.

Advanced Key Computation:

- Both sides compute an intermediate key using their respective commitments and the received commitment.
- The commitments are used to derive the intermediate key in such a way that the password values cannot be deduced from it.

Reciprocal Authentication

- Using the intermediary key, Alice and Bob demonstrate their understanding of their own passwords.
- A sequence of cryptographic calculations involving the intermediate key are often used to accomplish this.

Key for the session:

- After successful mutual authentication, the parties utilise the intermediate key to create a shared session key.
- The subsequent cryptographic actions of encryption and authentication can be performed using the session key.

V. RESULT AND DISCUSSION

The performance graphs in the following figures provide a visual representation of the research findings. The time required to upload a specific quantity of data, including the encryption process and data transport, is referred to as "uploading time". However, "downloading time" also takes into account the time needed to download the same fixed data volume and then decrypt it. Data sizes included in the inquiry range from 0.003 MB to 100 MB. Notably, there is a direct correlation between data size and uploading and downloading times.

As the quantity of the data increases, it is shown that the rate of rise in downloading time is more pronounced than the rate of increase in uploading time. With a larger block size, this trend is more obvious. In essence, longer uploading and downloading times are caused by greater data volumes, and this effect is especially noticeable during the downloading stage, where the increase is comparably more significant.

Table 1: Data uplink and Downlink time

	Size of Data								
	Data Size	**5**	**10**	**20**	**40**	**60**	**80**	**100**	**200**
Time	Uploading	3	12	14	18	29	31	54	76
	Downloading	10	21	25	32	58	70	120	150

The system's performance was assessed using data sets with sizes ranging from 5 MB to 200 MB. The data table that is provided provides a summary of the findings of this evaluation. Both the uploading and downloading times showed a discernible rising trend as the size of the data rose. For instance, the uploading time was about 3 seconds and the downloading time was about 10 seconds when the data size was 5 MB. However, the uploading time climbed to 12 seconds and the downloading time grew proportionally to 21 seconds as the data quantity doubled to 10 MB.

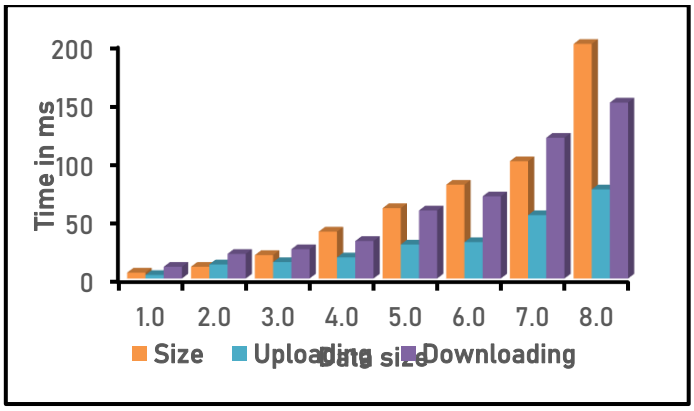

Figure 3: Representation of Data uplink and Downlink time

As the amount of data grew, this tendency maintained. Notably, as the data quantity increased, the disparity in the rates of rise between uploading and downloading times got more pronounced. The pattern suggested that downloading times were more strongly impacted, especially for larger data sets. This insight aids in understanding the relationship between data size and uploading/downloading times and offers useful details about the system's performance characteristics.

Table 2: Computational time with different key size

Key Size	Computational Time	Block Creation Time
16 bits	6	1.23
32 bits	8	0.98
64 bits	16	0.54
128 bits	24	0.12
256 bits	40	0.1
512 bits	51	0.03

The system's performance metrics were assessed for a range of key sizes, from 16 bits to 512 bits. The findings, including the computing time needed for various operations and the time necessary for block generation, are summarised in the data table that is provided. The observed measurements saw noticeable changes as the key size rose. Using a key size of 16 bits as an example, the computing time was roughly 6 units, while the block building time was 1.23 units. The computational time decreased noticeably to 51 units for bigger key sizes, like 512 bits, and the block generation time dropped to 0.03 units. These findings highlight how key size affects the system's ability to create blocks quickly and efficiently. It emphasises the trade-off between key size and speed, with bigger key sizes typically leading to faster block formation and shorter calculation times.

Figure 4 shows the link between the time required to create a block and the cryptographic key's length, expressed in various bit sizes. The graph offers important insights on how, in the context of the illustrated system, the size of the cryptographic key affects the effectiveness of block creation.

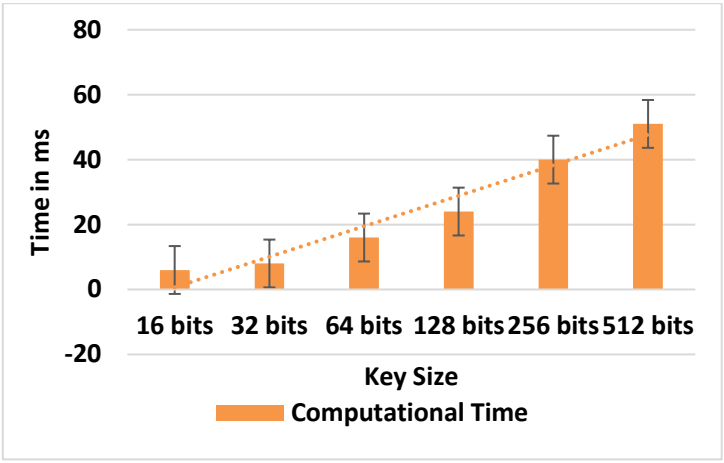

Figure 4: Representation of time for block creation with different bit key

The graph shows that there is a definite pattern in the data. The time needed to create a block tends to decrease as the bit size of the cryptographic key grows. The foundational ideas of cryptography are responsible for this connection. Because longer cryptographic keys add more complexity and entropy to the encryption and decryption operations, they often offer a higher level of security. Longer keys, however, may also necessitate more time and computer power to carry out cryptographic operations. The graph's data points demonstrate a gradual reduction in block formation time as key size rises. For instance, the related time for the smallest key size (16 bits) is 1.23 units, whereas the associated time for the maximum key size (512 bits) is 0.03 units. This pattern suggests that the system's cryptographic operations get more simplified and effective as the key size increases, leading to a speedier block production.

The ramifications of this graph can have a big impact on how blockchain technology are used in real-world applications. When deciding on the right key size for their blockchain applications, businesses must strike a balance between security and performance. Longer keys increase security, but they may also add computational burden that degrades system performance as a whole. Decision-makers may better grasp the trade-offs between key length and block formation time thanks to this figure's visual portrayal, which enables them to make decisions that are suited to their particular security and performance needs.

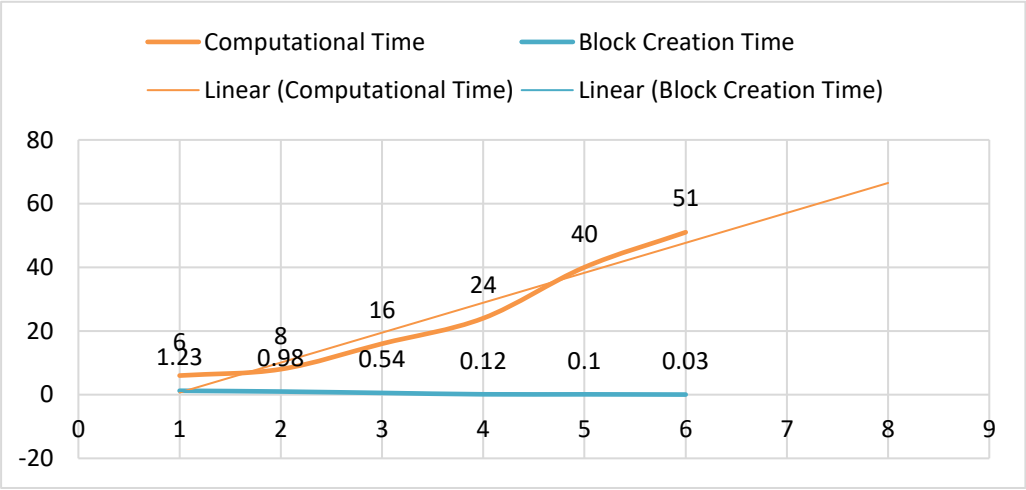

Figure 5: Comparison of Computational time and Block creation time

The information given compares the control policies between the suggested approach and an already-in-use system known as "Medchain." The different datasets designated as Data 1 through Data 9 are used to evaluate the control policies. The numerical values describe the results of applying the control policies to these datasets in terms of a quantifiable metric that is not mentioned directly in the information provided. Analyses show that the suggested solution consistently outperforms the Medchain system across a range of datasets. For instance, the

proposed technique produced a value of 4100 in Data 1, but Medchain produced a value of 3200. Similar to this tendency, the suggested method consistently yields greater values than the Medchain system across the datasets.

Table 3: Transaction of Health Record in Data time

Control Policies	Proposed Method	Medchain
Data 1	4100	3200
Data 2	10000	8750
Data 3	14000	11280
Data 4	9500	7850
Data 5	8000	5600
Data 6	11000	9680
Data 7	4800	3180
Data 8	7000	4580
Data 9	1000	678

The data points indicate that the suggested method is superior to the Medchain system in accomplishing the goals of these policies, despite the fact that the details of the control policies and the metrics being measured are not provided.

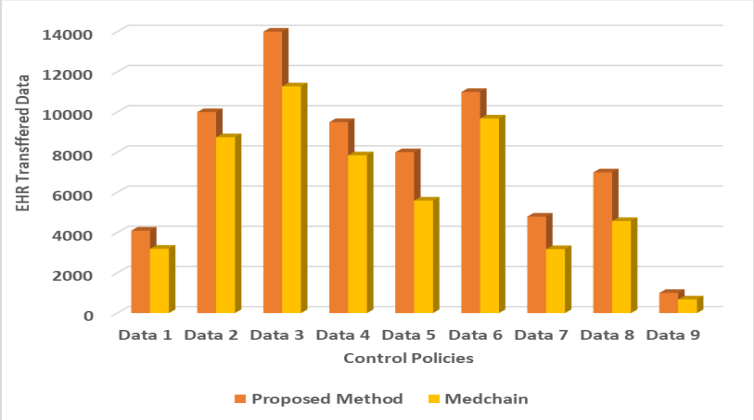

Figure 6: Transaction of Health Record in Data time

This could be attributable to a number of things, including improved resource allocation tactics, better algorithms, and better optimisation. It is significant to note that accurate findings concerning the superiority of the suggested method over the Medchain system would require a thorough understanding of the particular metrics being assessed, as well as the context of these control rules. A fuller understanding of the importance of the performance variations between the two techniques across the datasets would be possible with more information about the characteristics of these control policies and the underlying evaluation criteria.

VI. CONCLUSION

The creation of an effective and secure access control system for cloud IoT environments aided by fog, with an emphasis on sharing electronic medical records (EMRs). Model performance analysis produced results and

insights that shed light on the efficiency of the suggested solution. The data specifically shows that the size of the data being transferred affects the uploading and downloading times of data. This highlights how crucial it is to streamline data transmission procedures in order to provide fast access to medical records while upholding data security. To keep medical data private without sacrificing system performance, it's crucial to strike a balance between security and efficiency. Proposed method access control system makes use of blockchain technology's potential to create a patient-centric framework for EHR exchange. We have made sure that only authorised parties can access and share electronic medical records by using secure password authentication-based key exchange (SPAKE) and integrating smart contracts. This adds to the overall integrity of healthcare systems while also improving patient privacy. We have paved the way for a promising direction in healthcare data management by fusing fog computing, blockchain, access control systems, and performance optimisations. Adopting cutting-edge technologies that protect delicate medical information while permitting smooth data sharing is of the utmost importance as the healthcare landscape continues to transform.

REFERENCES

[1] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, ‘‘A smart-contract-based access control framework for cloud smart healthcare system,’’ IEEE Internet Things J., vol. 8, no. 7, pp. 5914–5925, Apr. 2021, doi: 10.1109/JIOT.2020.3032997.

[2] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, ‘‘BPDS: A blockchain based privacy-preserving data sharing for electronic medical records,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2018, pp. 1–6, doi: 10.1109/GLOCOM.2018.8647713.

[3] A. AlMamun, F. Jahangir, M. Umor, S. Azam, M. S. Kaiser, and A. Karim, ‘‘A combined framework of interplanetary file system and blockchain to securely manage electronic medical records,’’ in Proc. Int. Conf. Trends Comput. Cogn. Eng. Singapore: Springer, 2021, pp. 501–511

[4] J. Zhang, Y. Yang, X. Liu, and J. Ma, ‘‘An efficient blockchainbased hierarchical data sharing for healthcare Internet of Things,’’ IEEE Trans. Ind. Informat., vol. 18, no. 10, pp. 7139–7150, Oct. 2022, doi: 10.1109/TII.2022.3145851.

[5] S. Fugkeaw, L. Wirz, and L. Hak, ‘‘An efficient medical records access control with auditable outsourced encryption and decryption,’’ in Proc. 15th Int. Conf. Knowl. Smart Technol. (KST), Feb. 2023, pp. 1–6, doi: 10.1109/KST57286.2023.10086904

[6] S. Alshehri, O. Bamasaq, D. Alghazzawi, and A. Jamjoom, ‘‘Dynamic secure access control and data sharing through trusted delegation and revocation in a blockchain-enabled cloud-IoT environment,’’ IEEE Internet Things J., vol. 10, no. 5, pp. 4239–4256, Mar. 2023, doi: 10.1109/JIOT.2022.3217087.

[7] O. Cheikhrouhou, K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. R. Moosavi, ‘‘A lightweight blockchain and fog-enabled secure remote patient monitoring system,’’ Internet Things, vol. 22, Jul. 2023, Art. no. 100691.

[8] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, ‘‘Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices,’’ IEEE J. Biomed. Health Informat., vol. 27, no. 2, pp. 710–721, Feb. 2023, doi: 10.1109/JBHI.2022.3187037.

[9] F. Daidone, B. Carminati, and E. Ferrari, ‘‘Blockchain-based privacy enforcement in the IoT domain,’’ IEEE Trans. Depend. Secure Comput., vol. 19, no. 6, pp. 3887–3898, Nov. 2022, doi: 10.1109/TDSC. 2021.3110181

[10] Dataset used: https://archive.ics.uci.edu/dataset/46/hepatitis

[11] Abedi, M.; Pourkiani, M. Resource Allocation in Combined Fog-Cloud Scenarios by Using Artificial Intelligence. In Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 20–23 April 2020; pp. 218–222.

[12] Winnie, Y.; Umamaheswari, E.; Ajay, D. Enhancing Data Security in IoT Healthcare Services Using Fog Computing. In Proceedings of the 2018 International Conference on Recent Trends in Advance Computing (ICRTAC), Chennai, India, 10–11 September 2018; pp. 200–205.

[13] Elie, E. Keynote speech 3: Intel Optane™ technology as differentiator for Internet of everything and fog computing. In Proceedings of the 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 23–26 April 2018; p. 3.]

[14] Mittal, M.; Saraswat, L.K.; Iwendi, C.; Anajemba, J.H. A Neuro-Fuzzy Approach for Intrusion Detection in Energy Efficient Sensor Routing. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–5.

[15] Zhang, Z.; Wang, F.; Zhong, C.; Ma, H. Grid Terminal Data Security Management Mechanism Based On Master-Slave Blockchain. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15–18 May 2020; pp. 67–70.

[16] Khetani, V. ., Gandhi, Y. ., Bhattacharya, S. ., Ajani, S. N. ., & Limkar, S. . (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2951

[17] Tuli, S.; Mahmud, R.; Tuli, S.; Buyya, R. Fogbus: A blockchain-based lightweight framework for edge and fog computing. J. Syst. Softw. 2019, 154, 22–36.

[18] Narula, S.; Jain, A. February Cloud computing security: Amazon web service. In Proceedings of the 2015 Fifth International Conference on Advanced Computing & Communication Technologies, Rohtak, India, 21–22 February 2015; pp. 501–505.