Attribute-based Access Control Model in Healthcare Systems with Blockchain Technology

Prince Arora, Avinash Bhagat, Mukesh Kumar
Computer Applications, Lovely Professional University, Jalandhar, India

***Abstract*—Blockchain and the healthcare sector have a serious concern with context to scalability, which has a challenge of converting arbitrary values to fixed values. The transfer of arbitrary data coming from diverse resources has another point of concern in the blockchain. In this paper, the author proposed a model that will receive data from diverse sources and will convert it to a fixed type of value. The paper also proposes an access control scheme with various permission and consensus level protocols which will allow a reduction in block size with respect to scalability. The consensus level will allow access to the individual or a group of users and the permission level with respect to each block via considering the access granted to nodes of the blockchain. The addition of various permission and consensus levels will allow only a restricted type of data to pass the model. Once the data is verified and approved by various levels, then the data is all set to be part of the blockchain. The paper introduces a model where the time taken to create a new hash is 0.15625 microseconds. A total number of 64 transactions taken from the data set where the throughput is calculated for individual access are considered. After applying the formula, the calculated throughput is 32.5 microseconds. By the lighter block size data can be made available to the patients. The research is for the patients so they can keep track of their medical history and the deaths due to overdose of the medicines can be reduced.**

Keywords*—Blockchain; healthcare; permission level; consensus level; scalability

I. Introduction

Blockchains are incredibly popular nowadays. As the name indicates, a blockchain is a collection of blocks associated with a timestamp. It ensures the irreversibility and immutability of the data block. A blockchain technology is a distributed ledger which allows the data to be stored across the network along with the next hash and previous hash. There are some applications of the blockchain like bitcoin and etherium that ensure the correct transmission of the data over the network. Security and privacy challenges arise in the medical field due to rapid growth in data collection and subsequent analysis by a variety of organizations. The devices that relate to the internet or Internet of Things (IoT) data come from various sources. Scalability is a huge challenge that comes with it. Personal Health Records (PHR) are usually owned by the patients; however, they can also be shared with third-parties based on the patient's approval. Medical professionals can use Electronic Medical Records (EHR) to retain and share patient data, but paper-based medical records cannot be transferred across institutions or locations. Healthcare data collection is expected to reach 4.5 billion dollars by 2030. It is expected to expand at a percentage of 26.9 from 2022 to 2030 [1]. It becomes vital to design an online model which helps the patient and the doctors keep track of all the medicines and treatments given by the doctor to the patient. Consequently, third parties must be limited in their access to this data. Controlling who can and cannot access a system's resources is the major aspect of access control.

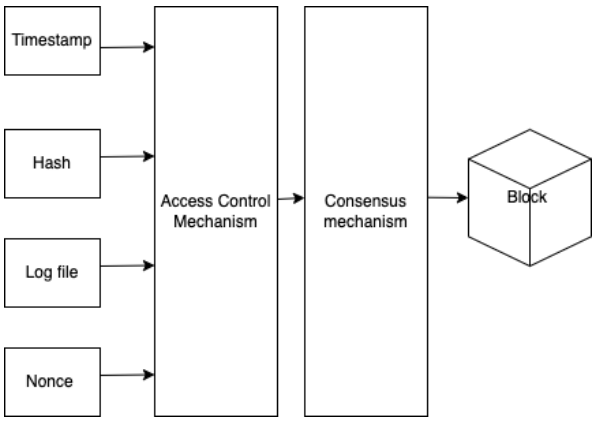

Fig. 1. A log file based access control model.

Personal or medical health data [2] kept by many parties, and which may be required for third-party access to third-party aims (such as medical or insurance companies), is a difficult task to manage. The data collected from heterogeneous sources is difficult to manage for any insurance or medical organization. This is due to the complexity of the data and the need to make it usable for the organization. Obtaining and normalizing the data from diverse sources requires considerable efforts, making it a challenging task for organizations. Interoperability is the major issue that comes up in this matter. The availability of the data cannot be achieved without the attribute-based scheme.

A timestamp embeds the time of the transaction. Fig. 1 explains the basics of the access control model. A hash value is used to ensure the uniqueness of the transaction. A Nonce is a randomly generated 32-bit number that is used by miners to adjust the hashing of a block and make it valid for use. Once the perfect nuance is found, it is connected to the hashed block. The log file is a part of the proposed model that stores the calculation of the address. By using this calculation, the next address can be allocated to the chain of the blockchain model. An access control mechanism is used to collaborate on the attributes of the block. Thus, the blockchain can have a unique value that easily differentiates the block with other blocks.

To resolve the issues related to address control in a huge system like e-Health, a technique is proposed in this study as shown in Fig. 1, which allows data to be accessed with various levels of authorization and granularity. Adding, updating, or removing rights to their data should be easy for the data keepers to do. Permissions should be able to be defined at the user and source level with sufficient precision in such a system.

An overview of access control in e-Health systems, focused on blockchain technologies for access control, is provided in the first section of this paper. In the following section, a breakdown is found for the intended solution architecture. As a next step, few essential components for building a working model are discussed. There are also a few concluding comments that summarize the contributions and hint at future advancements. The issue related to the healthcare field is the huge amount of data coming from diverse resources. Data management is a huge task, and, if any patient wants to fetch their medical history from the offline database, it would be even more difficult to find the data in a quick time. Another issue is the maintenance of centralized storage, which has various overhead issues and a high reliance on servers. To ensure that the data is available on time and at every end, the blockchain technology is used for the work.

Purpose and need of the study: The study is important because once the patient has undergone some treatment from the doctor, it is important that the medical health history being maintained by the patient and the doctor as well. If the patient is not satisfied by the treatment of the doctor, patient changes the doctor and it becomes vital for the patient to know what medicines or injections are already given to the patient, it can be maintained through Electronic Health Records (EHR). With the help of EHR data can be stored, in a blockchain based system which allows the availability of the data at patient end. When the patient changes the doctor, patient should be having the updated medical history available all the time so that it will be easy for the new doctor to understand the patient history. Every doctor who has done any treatment of the patient has to fill the attributes. The system works remotely and ensures the availability of the data. By using this, data can be made available to each end and access can be granted based on access control mechanism used in the proposed model. The model can be embedded with a variety of technologies like: Internet of Things (IoT) and Artificial Intelligence (AI). By associating these technologies with blockchain the medical record collection can be more automated; where if a patient has gone through X-Ray, the record can be automatically recorded in the EHR. A block in the blockchain typically consists of approximately 2000 transactions. To make the node lighter, reducing the size of the transaction can be beneficial. Gas amount is used to operate the blockchain, and a limited amount of gas can be passed. Heavy nodes with duplicate values allow only a few nodes to be connected to the blockchain; on the other hand, light nodes have less total weight, requiring less gas to operate the blockchain, allowing for more nodes to be added to the network [3].

Limitations of blockchain scalability: The scalability of current blockchain technology is limited by its transaction throughput, cost, network latency, data storage, and energy consumption. As the number of transactions grows, the cost of running a blockchain increases and the data stored on it becomes more difficult to manage. Furthermore, the time it takes for a transaction to be validated and added to the blockchain is too long, and the consensus algorithms used by blockchain networks are often very energy intensive. All these factors demote scalability.

The paper is arranged as follows: After the introduction section, the advancement of blockchain for healthcare, in Section II, Literature Review is discussed on blockchain and healthcare. Section III focuses on data sets where various attributes are taken to show the results and it discusses the proposed methodology to achieve the goal. Section IV talks about the evaluation parameter. Section V focuses on how the model can be developed. Section VI focuses on implementation of the proposed model. Section VII presents the results and discussions and Section VIII summarizes the paper.

II. Related Work

To find and analyse the results of the various existing models and compare them with the proposed model, various models are studied. The literature review is discussed in the related work section, where several existing models are there, and the results are compared in the final section. Ayache, M. et al. [2], proposed a Decentralized Accessible Scalable and Secure (DASSCare 2.0) model that works on real-time health monitoring that route all the data from various resources and makes it available to various end users, which allows the collaborative health monitoring and maintains the bills paid by the patient. The model gives an extra edge to other frameworks. Using a distributed database is a consensus of shared and synchronised digital data spread along a set of nodes. Contrary to popular belief, however, not all decentralized ledgers are in fact distributed ledger technology (DLT). The duplicity is high when the data is shared across various blocks.

Karaki, A. et al. [3], proposed a Decentralised Accessible Scalable and Secure (DASSCare) model which is a decentralised framework, which is scalable and accessible. It allows real-time access of data that comes from diverse resources. To maintain this, the generated clinical data is signed. The sign ensures that the type of data coming from diverse resources is of the same type, and then it is considered. This framework solves the problem of real-time access of medical records in healthcare, which is a primary part of the work and ensures that privacy is not compromised.

The healthcare data stored on various resources is a difficult task to be followed. Mira, S. et al. [4] proposed a CrowdMed model that works on managing the data and, to ensure the data is in the correct format, a review team is assigned. The data reviewer resolves two issues: one is to resolve the issues coming from diverse resources and the other is to make data more homogeneous to ensure the scalability of the chain across the network. In this

framework, the patient has full access to the data, so if the patient has taken any medical treatment of his own, the data can be updated by the patient itself.

The CrowdMed model allows the data reviewer to review the data and the data is reviewed at different ends simultaneously. Tampering of data is a prime concern that is associated with the CrowdMed model. To overcome this, Hu, C. et al. [5], developed a scheme CrowdMedII where the smart contract allows only insertion in the model. The healthcare workers are not allowed to update the data. By this, the data quality can be improved and the chances of tampering of data from diverse resources can be made more specific. The disadvantage is also associated with the model, which requires a lot of space.

Developed by Nakamoto, S. [6], the blockchain is a distributed record that serves as the foundation for the Bitcoin digital currency. Digital signatures and digital fingerprints (hashing) are two methods that can be used to ensure the integrity of data and prevent tampering with data. The ledger must be secure from malicious attempts to undermine it as well as from peers submitting incorrect data, computer/network failures that are only partially or fully finished, or even by peers providing incorrect data out of ignorance. The blocks that make up a blockchain contain data on transactions. A digital signature is attached to each one of these transactions. Using this method, a state transaction system (state machine) is implemented, in which every node adds a snapshot to the existing model to various existing models. The peer-to-peer network relies on a proof-of-work concept to move to consensus on a block's validity. There are various alternatives to proving work. The block that is to be pushed inside with various existing timestamps allows the transaction to be a unique transaction.

Blockchain, according to Buterin, V. et al. [7], is divided into three parts: public, private, and consortium. Unlike private blockchains, public blockchains (e.g., Bitcoin) are accessible to anybody who wants to read them, send transactions, and expect them to be added if they are genuine. "Fully-private blockchains" where the participants (e.g., a supply chain) are called "fully-private blockchains" since the write permissions are centralized within a single organization (even if they are spread across multiple facilities). An open blockchain may or may not restrict who has access to perform blockchain queries. To ensure that the access control mechanism is working well, identity is confirmed from where the data is fetched.

Salman, A. et al. [8] granted a controller which indicates that the identity is genuine or not. The address of the sender can be used as a certificate and attached with the complete model to ensure that the transaction is authentic or not. This scheme is an identity-based scheme where the identity of the sender acts as a certificate and allows only the verified transactions to be approved from the end. Nakamoto, S. [5] introduces the concept of "blockchain," a distributed ledger technology that allows data to be transferred from one node to another while retaining a copy in the user's node rather than storing all data in a single shared database. Maesa, D. et al. [9], present a paper which is based on bitcoin. The access control mechanism is based on the resources that are being used for the transactions of the blockchain. The XACML (Extensible Access Control Markup Language) is used to develop the code of the resources that allows the end resources to access and transform similar types of data.

Castiglione, A. et al. [10], proposed a model that is a device-based model. Various types of data are made available at various points. Different duties are allocated to various devices that play different roles in the transaction. Each device has its own restrictive access control mechanisms that allow only quality data to be inserted into it. To handle IoT devices, Novo, O. [11] proposes a distributed blockchain-based permission method. The work included a unique concept to prevent integrating blockchain with IoT devices, which is the major part of the model. This approach correlates the use of blockchain with IoT, particularly for devices with limited resources. Fair Access is a blockchain-based authorization mechanism described by Ouaddah A et al. [12]. Smart contracts were utilized to exchange access tokens for the fulfilment of access control protocols. The authors incorporated various IoT devices into the blockchain and investigated the issues of real-time permission and the efficiency of the scheme.

Using a smart contract, Xu, R. et al. [13] suggested a decentralized, federated capability-based access control method. The technique was used for multi-hop delegation and was also reliable and scalable. Based on objectives, models, architecture, and mechanisms, Ouaddah. A et al. [14] gave a complete review of various access control methods. The report also focuses on the various taxonomy-based author reviews and the advantages and disadvantages of each are discussed in the model. Novo, O. [15] proposed scalable decentralised access management for IoT devices based on blockchain technology. To avoid network overheads, the architecture removed IoT devices from the blockchain-enabled network. In terms of IoT access control, the system has various advantages, including accessibility, parallelism, lightweight, immutability, scalability, and transparency. This framework has managers that allow IoT devices to be registered and verified. Although this method achieves scalability by distributing query rights through management hubs, it faces various security risks.

Dorri, A. et al. [16] advocated leveraging private blockchain technology to provide a lightweight architecture for protecting the IoT. The proposed method ensures security with an access control permission list and their design, including various models. All the devices based on the model are mined by miners. This approach has control of the policies in the header part of the policy. It does not use a Proof of Work (PoW) concept to ensure its uniqueness. They claimed that the solution's overheads are modest in comparison to the security benefits. By concentrating on user preferences, which can find access and denying methods, Touati, L. et al. [17] suggested an activity control method (a broader version of context-aware access control). For dynamic access policy adaption, ciphertext-policy and a finite state automaton are used to keep track of all the updates in the network. By analysing the logical approach to trust computation from language-

based information received from IoT devices, Mahalle, P. et al. [18] proposed an energy efficient architecture which is both energy efficient and dynamic in nature. An individual or a group with the authority to provide access to privileges and resources can be easily accessed. The Table I compares the different models studied in literature review.

Zhang, R. et al. [19] suggested a sensor network-specific distributed privacy-preserving access control method. It requires users to have a token from the owner and then request sensor data, which is supplied after the token is verified. To prevent the reuse of tokens, which would allow unwanted access, they deploy a distribution token reuse detection system. Their focus was on preserving privacy and they did not consider access control settings for end devices. Access Control In current operating systems, Access Control Lists (ACLs) are a typical method of controlling access. An ACL lists people who have access to an object, as well as the amount of access (or privileges) they have. Alternatively, other systems employ an Access Control Matrix, which consists of rows and columns, where a column denotes an object and a class denotes a subject. Health care is a good example of the use of Oole-Enabled Access Control and privileges linked with those roles are used to determine a user's access rights in RBAC. The consortium's XACML can be used to express Attribute Based Access control Model (ABAC) policies Access control systems can be designed and implemented using the XACML standard's reference architecture that defines the system components and usage flow. More expressive access control policies can be defined using Entity-Based Access Control (EBAC) [27], another commonly used technique. Both attribute value comparisons and relationship traversals along arbitrary entities are supported, so this is possible. There is also an authorisation system that provides realistic policy language and an assessment engine for the system. Application of Blockchain to Access Control One solution to the issue related to access control in e-health is based on blockchain technology. According to Maesa. D et al. [9], the XACML standard architecture can be used to construct Attribute Based Access Control on top of blockchain technology for access control. Using Bitcoin as a base, this strategy can be proven to work.

TABLE I. RESEARCH PAPERS CONSIDERED FOR THE LITERATURE REVIEW PURPOSE

Name of Authors	Model Name	Access Control	Blockchain Enabled	Permission Control
Ayache, M. et al. [2]	DASSCare 2.0	Yes	Yes	No
Wang, T. et al. [23]	Audit Model	Yes	No	Yes
Karaki, A. et al. [3]	DASSCare	Yes	Yes	No
Salman et al. [8]	Access control list	Yes	Yes	No
Novo, O. et al. [11]	Blockchain based permission control method	Yes	Yes	Yes
Novo, O. et. al. [15]	IoT Access Control	Yes	Yes	Yes
Maesa, D. D. F. et al. [9]	Extensible Access Control Markup Language	Yes	Yes	No
Dorri, A. et al. [16]	Permission Control	Yes	Yes	No
Ouaddah, A. et al. [12]	Fair Access	Yes	Yes	No
Bogaerts, J. et al. [ ]	Entity Based Access Control Model	Yes	No	No
Castiglione, A. et al. [10]	Attribute Based Access Control Model	Yes	Yes	No
Zhang, R. et al. [19]	Network Specific Access Control	Yes	Yes	No

However, in the e-Health context, this method does not consider the possibility of having several authorities and/or companies as the resource owners.

A Healthcare Data Gateway (HGD) blockchain model can be used for e-Health by Chen, Y. et al. [20] has the capability to store patient records where patients can keep track of their medical history. The patient's history is recorded on blockchain as part of this solution. I. Baldine et al. [21], has a solution to the issues raised in the previous paper, despite the uniqueness of this strategy, it is likely to need a significant amount of time and effort to implement, which may put the current utility of this method into question. If the patient is unable to enable the access, or if some governmental regulations require that the data be accessed without the patient's permission, then this solution has no capacity to do so (e.g., some family members allow the data access). Keeping e-health data on the blockchain will cause its size to explode, far beyond the capacity of currently available hard drives, necessitating the purchase of specialized hardware for full nodes and possibly even leading to the centralization of the blockchain.[28,29]

III. MATERIALS AND METHODS

The dataset which is used for the implementation is taken from Kaggle, which consists of a huge variety of databases related to EHRs. Data is gathered and, as per the model, the data is converted into a decision-based format where the data can be made available for the blockchain construction. The description gives an overview of the dataset and focuses on various attributes used for them [22]. The data set consists of various attributes to maintain the patient records. The data set is based on the chronic kidney disease of the patients, which requires the medical history of the patients to be stored so that if the patient is undergoing some surgery or treatment, the data can be accessed from

the EHR that maintains the history of the patient. The detailed description of the dataset taken into consideration for this study is given in Table II.

TABLE II. DETAILED DESCRIPTION OF THE DATASET USED FOR THIS STUDY

Attribute Name	Domain Values	Attribute Name	Domain Values
Gender	{0= M, 1=F}	HTNmeds	Range = {0, 1}
AgeBaseline	Range = {23, … ,89}	ACEIARB	Range = {0, 1}
HistoryDiabetes	Range = {0, 1}	CholesterolBaseline	Range = {2.23, … ,9.3}
HistoryCHD	Range = {0, 1}	CreatinineBaseline	Range = {6, … ,123}
HistoryVascular	Range = {0, 1}	eGFRBaseline	Range = {60, … ,242.6}
HistorySmoking	Range = {0, 1}	sBPBaseline	Range = {92, … ,180}
HistoryHTN	Range = {0, 1}	dBPBaseline	Range = {41, … ,112}
HistoryDLD	Range = {0, 1}	BMIBaseline	Range = {13, … ,57}
HistoryObesity	Range = {0, 1}	TimeToEventMonths	Range = {0, … ,111}
DLDmeds	Range = {0, 1}	EventCKD35	Range = {0, 1}
DMmeds	Range = {0, 1}	TIME_YEAR	Range = {0, … ,9}

This is a dataset of electronic medical records of 491 patients collected at Tawam Hospital in Al-Ain city (Abu Dhabi, United Arab Emirates). The patients included 241 women and 250 men, with an average age of 53.2 years. Each patient has a chart of 22 clinical variables, that expresse her/his values of laboratory tests and exams or data about her/his medical history. The attribute starts with patient name and is based on various attributes like doctor and medicine. The patient record is based on the updating done by various doctors and patients. The dataset contains the information of attributes related to the patients and the results are calculated based on that data. The record of the patient can be updated by the doctor and if any medicine is given to him that must be added to the chain. To achieve scalability, the block of the blockchain is compressed by using various hashing techniques. The attributes are defined in the model so to ensure the fixation of the inputs prescribed by the doctor.

IV. EVALUATION PARAMETER

Wang, T. et al. [23], proposed a model. The paper also includes various factors by which the model can be evaluated and compared with the other models that are based on various factors like execution time, latency, and throughput. Xu, Z. et al. [24], evaluates the performance of the model based on the time that it takes to generate the hash, the amount of delay that is required to keep the transaction and the time required to complete the transaction. Description of each evaluation parameter is discussed in Table III.

TABLE III. DIFFERENT EVALUATION PARAMETERS OF PROPOSED MODEL

S. N	Evaluation Parameter	Description of the parameters
1	Execution Time	It is the time taken as the difference between once the transaction is confirmed and the execution of the blockchain.
2	Latency	It is the time taken by the system that waits for the other system to complete the action.
3	Throughput	It is the amount of data that can be shifted from one block to other block of the blockchain in a unit of time.
4	Performance Assessment	It is the measurement done on the models by providing the described hardware and can be calculated based on time frame.

To understand how the proposed model performs, various users can apply operations on the blockchain-based model.

All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout conference proceedings.

V. PROPOSED ATTRIBUTE-BASED ACCESS CONTROL MODEL

After Access control Data management is used to ensure that the data coming from various sources must have an arbitrary value that is difficult to handle. The model will ensure that the data coming from various resources is converted into fixed values. The model access controller establishes a relationship with various subjects and objects, which ensures the data can be easily stored and passed through the blockchain model and creates a block. The methodology works on various entities like permission levels, data keepers, policies, and records [25, 26]. The proposed attribute-based access control is given in Fig. 2. Classes and entities of the proposed attribute-based access control are discussed below:

Entity (UID): The entity contains the records of the various transactions, read, write or any other. Whether the

entity should be given read, write or read/write access, is maintained in the record file.

Data Keeper: The data keeper keeps track of all the access granted so that it can be compared with the upcoming transactions. It records the various levels of the permissions that can be granted to the various entities of the model. The type of the access granted to the entity is also decided by the data keepers.

Policies are rules and regulations that govern which types of access are granted. Policies are based on permission levels and consensus levels, which are useful for filtering the data. The consensus level policy, which is based on permission level, requires Unique Identity (UID), record and permission level to fetch the data. Once the UID is compared and verified, the permission is granted based on levels and the consensus level policy works on UID, record and the type of permission granted. Various policies can be created to improve the quality of the blockchain model. The policies correlate various data keepers with their permission level. Some exceptional cases, like if a patient wishes to have a medicine without the permission of the doctor, can also be considered in the patient's record history file. The permission level defines various types of permissions that can be read, written, or both read and written. The access, once granted, is compared with the access required by the transaction to be verified and completed.

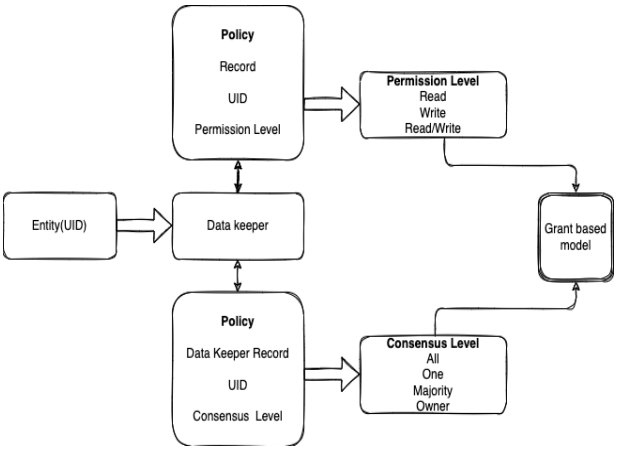

Fig. 2. Proposed attribute based access control model.

Grant based Model Structure: Model of Access Control There are many entities and relationships that must be defined before a model can be created. Fig. 3 shows such a model, and it may be used to classify objects into five different types. There are three types of access that can be granted to the model, like Read, Write, and Read/Write. The data keeper keeps a record of all the data and ensures that only authentic people can access it. The data keeper tracks the UID, consensus, and pointer to maintain the integrity of the record as well. This also prepares a policy to provide more validation to the access by checking the record and entity and allocating a certain permission level. The permission level can be read, write, or read and write as well. By ensuring this, the quality of the access mechanism can be enhanced and not every type of transaction can access all types of data in it. Each policy with various permission levels generates a particular consensus level which allows the model to get restricted input from various channels. The state machine can also be a useful part of the model. This machine gives an inside view of how the permissions are granted by the data keeper. Fig. 3 indicates that once the transaction is inserted into the model, it must pass through various blocks like request, verify, and require.

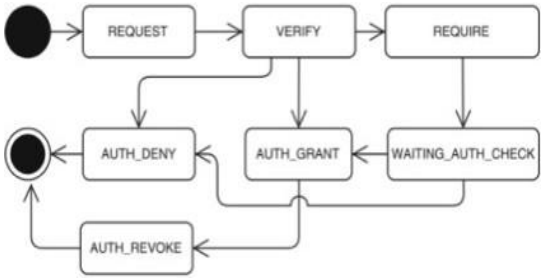

Fig. 3. Grant based access model.

The request block allows the block to be requested and verified by using the properties of the blockchain like: irreversibility and immutability. The verification also checks the hash value of the block. The hash value is compared with the previous block hash value then it is a valid transaction. Once the verification is successful, the access is granted and the transaction is performed. The verify block in the model also has the power to deny the access when the requested block does not match the hash value in further. If the access granted is only a write operation access that usually is given to the doctors of the hospitals then the medical history of patient can be written. Once the updating in the record is done by the doctor then the revoke operation can be performed on the transaction. After the verification of the hash values time stamps are compared with the previous block, if there is a scenario where any other specific requirement is there. The hash value matches but the issues are there in the timestamp, in that case the transaction is sent to the waiting state that will wait for the grant condition to be performed on it. Various parts of the block model for blockchain structure are mentioned in Table IV.

TABLE IV. NUMBER OF CASES AND THE REDUCTION IN EXECUTION TIME

S. N	Components	Description of the components
1	Index	Represents the present index of the block
2	Timestamp	Represents the time when block is generated
3	Previous Hash	The hash of the previous block
4	Digital Sign	Cryptographic hash of the most recent data block
5	Data	This block's content. Access control policies, records information, and individual authorizations are all described in this set of transactional data

6	Nonce	For a block's hash to include leading zeroes, it must have this value set. Iteratively, the value is implemented until it is completed and discovered to meet the requirements. The correct nonce value is proof of effort because it takes time and resources to get it right
7	Hash	Hash of the block data in SHA256 form. The effort of the proof-of-work is defined by the leading sequence of this hash, which must be predetermined. Additionally, the data field must be comprehensive because it serves as a repository for transaction information. There are three sub-fields that make up this data category: a) A record is a piece of data pertaining to a certain state machine transaction, such as the creation, modification, or deletion of an e-Health record. b) Information on the creation and revocation of access policies related to transactions in the state machine shown in Fig. 2. Transactions relating to individual authorization by each of the Record Data Keepers in connection to each Policy. c) There is no need for a central authority because any change in data would result in a new hash, which would invalidate the next blocks on a chain of transactions that is immutable without a central authority. Accountability and auditability are additional possible outcomes. Assuring the authenticity of each block on the blockchain is done by assigning an individual key pair to each entity with access to it

VI. Implementation of Proposed Attribute-Based Access Control Model

The model starts with registration of the patient in the system; various peers are the sources from where the data is originated. To ensure that the access control mechanism works well, the levels which are discussed in Fig. 2 ensure the type of the data that will only be allowed to be inserted in the node. In Fig. 4, the security level object ensures the type of the access provided by the system to the framework. The security level checker matches the access type from which the access is being granted and the type of data which comes from various resources with various access rights. If the data matches the access granted and the access demanded by the transaction coming from the source, the access is considered as high-level access. The peer level stores the access related data, when the data requirement comes from any patient or the doctor, it is compared with the access that is being demanded by the transaction. The role of patient is just to have a view of the data so the access read is required all the time. Consider a situation where the patient wants to write the medical record but not mentioned in the peers. In that situation, low level access is given. The reason why these protocols are being added to the model is that once the data is being transferred to the block chain the data should be of fixed type that is being approved by various peers.

When the high-level access is being granted, in that case the transaction has passed the peers and it can move to the blockchain as shown in Fig 4.The blockchain easily accepts the type of attribute based fixed transaction. The algorithm also defines some roles which includes insertion, updating and deletion of the data. While working with various operations, the add functions inserts a value along with the parameter passed to the function.

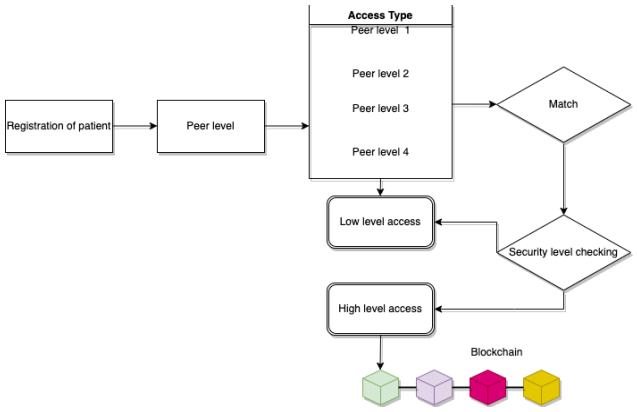

Fig. 4. Methodology of designing attribute-based access control model in healthcare system.

The limit for the passing of the arguments can be at most the total number of the patient attributes. Except the doctor one is not allowed to insert the data into the blockchain environment. Once the data is verified, the registration number is updated with 1. Suppose, if the patient has taken medicine after doctor prescription 76 times the new entry where the data is added can be considered as 77, also if the patient has taken medicine by his own consent, the database is required to be updated. The OR gate allows that both the doctor and patient is capable for the necessary modification in the record. The updating can be done with the update function record but more validation check is being added to it. If the sender of the data is the concerned doctor or the patient, then the other condition is checked and verified. The patient ID is compared with the existing ID available of the patient that allows or denies the updating of the data. Once the criteria meet both the conditions, the data can be updated otherwise the data needs to be on hold for the upcoming transaction.

Algorithm 1: Algorithm used for attribute-based access control Model

```
Add Data:
method Add Patient Record (var1, var 2.....n)
if (record.input = = doctor || patient || healthworker)
Regist_ID = Regist_ID+1
end if
end method
Data added successfully

Update Data:
method Update Patient Record (var1, var2.....n)
if (record.input = = doctor || patient ||healthworker)
and if (id = = patient id)
then Update patient_record
end method
Data updated successfully

Delete Data:
method Delete Patient Record (patient id)
if (record.input = = doctor)
and if (id = = patient id)
then delete patient record & Abort
Set Record =Record-1;
end method
Record deleted successfully
```

The deletion of the data depends on the id verification, the patient ID is compared with the existing ID, once the ID is verified then the deletion of the data can be processed. Inside the method, if the data is sent by the doctor and the patient ID is verified to be true, the account of the patient which is also considered as a block is verified as true as shown in algorithm 1. The record set is decreased by 1. One block in the blockchain contains the record file which consists of the total values used in the block. The value of the record is decremented by 1.

VII. Results and Discussion

The focus of result is on data calculation and on that basis the performance of the blockchain is calculated. The section explains the metrics based on those metrics the results generated by the models can be compared and evaluated with the other models. The results prove that the performance of the model can be enhanced based on some inputs. The performance can be improved as when the hash value is generated with high participants, the chance of getting the maximum digits of the model can be same. The model allows the performance to be enhanced based on increase in number of users.

Execution Time is the time taken for the process to be completed. It starts with the initialization of the transaction with the completion of the transaction. The hash value is generated by SHA-256 algorithm in the blockchain. The average time taken to generate the hash value is 3ms and if the transactions are 100 transactions, 300 ms would be taken to complete the transactions.

Case 1: Let us take a hash key that is of 64 bits and the genera5on of 100 hash values will take 300 ms. By applying the proposed model various improvements can be done in the existing blockchain model. This case covers the cases and assumes that if the value of hash next evaluated hash has a single bit change.

Hash Key =
8F434346648F6B96DF89DDA901C5176B10A6D83961D
D3C1AC88B59B2DC327AA4

- Total number of digits used by Hash = 64
- Generation of 100 Hash values will take 300 ms
- Total number of digits for 100 Hash values =6400
- Time consumed for one bit Hash Key generation= 300/6400=0.046875
- Block size generation after applying attribute-based log file model

Case 2: Let us take a Hash Key that is of 64 bits and the generation of 100 hash values will take 300 ms. By applying the proposed model various improvements can be done in the existing blockchain model. This case covers the cases and assumes that if the value of hash next evaluated hash has all the bits changed as written in Table V.

Hash Key =
8F434346648F6B96DF89DDA901C5176B10A6D83961D
D3C1AC88B59B2DC327AA8

- Number of digits modified in the block=1 Ratio of digits =1/64
- Total number of digits used by Hash=64
- Generation of 100 Hash values will take 300 ms
- Total number of digits for 100 Hash values =300
- Time consumed for one bit Hash Key generation= 300/300=1

One out of 100 cases exists in the model the results can be improved by transferring the data from 1/100 which makes 99.015625 to 1. Increase in number of cases will improve the quality of the algorithm as compared to another non-attribute-based model.

Average Execution Time=Total Execution Time/Total number of Transactions.

TABLE V. Number of Cases and the Reduction in Execution Time

Numbers of Cases	Execution Time	Growth Rate
1	99.015625	0.0984375
2	98.03125	1.96875
3	97.046875	2.953125
4	96.0625	3.9375
5	95.078125	4.921875

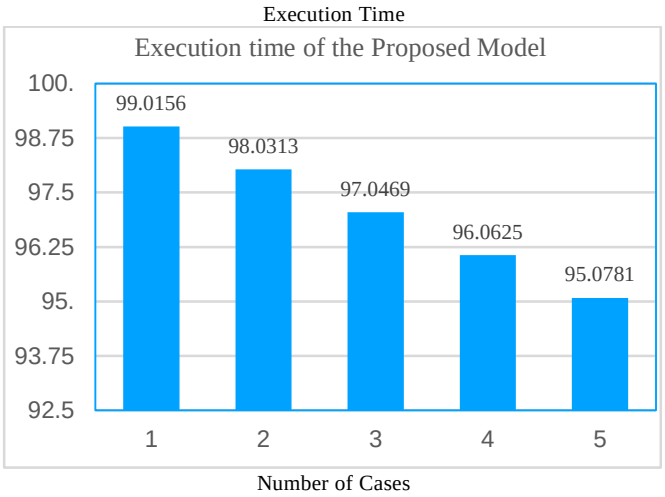

Fig. 5. Execution time of the proposed model.

Average Latency: It can be calculated by the difference between the request sent and the response generated by the model. However, the latency of the model is calculated by JMeter. In Fig 5, it is clearly visible that execution time is reduced after each bit change. The average latency can be measured in the context of milliseconds. The average latency can be measured:

Average Latency = Time taken to update Hash/Number of Hash bits

The performance of the model is also evaluated by accessing the size and cost of the generated Hash value. The transaction payload can also be accessed by the transaction size.

TABLE VI. NUMBER OF CASES AND IMPROVED LATENCY

Hash size	Change in hash bits	Time taken by existing model in ms	Same bits in hash value	Proposed model
64	4	64	60	0.0625
64	3	64	61	0.046875
64	2	64	62	0.03125
64	1	64	63	0.015625
64	0	64	64	0

One Hash code is of 64 bits, the time taken to 1 bit Hash = 1 sec,

Time taken to update 64-bit Hash =64 seconds

Latency of log-based model =1/64=0.015625.

Time taken to generate the 2nd Hash Value=0.015625 + 2nd Hash value

Throughput is the amount of the data to be passed from one location to the other location. The throughput can be referred based on time and data. Only a single hash bit is required to be changed and the throughput time can be reduced by the possible number of favorable cases.

Throughput = Time taken to get result/Number of units.

A total number of 64 transactions taken from the data set where the throughput is calculated for individual access is considered. After applying the formula, the calculated throughput is 32.5 ms. The value of throughput can be considered as 32.5 ms. The average throughput can be considered as 32.5/64 which is 0.5078125ms where 32.5 is the sum of the throughput of the total 64 cases and the number of total cases is 64. The average latency of the 64 units can be calculated as 32.5/64 which is equivalent to 0. 5078125ms. The proposed framework works better when the complete data set with 64 different values are applied to it. With the existing model the throughput is considered as 1 ms but the proposed model improves the average throughput by approximately 49 percent. The Table VI demonstrates the reduction in the time taken to construct the hash.

Different parameters are discussed that are based on which comparisons can be made without compromising the security and privacy of the model. After incorporating these parameters, the model can be further optimized as demonstrated in Table VII.

A. Scalability

Scalability is considered as the ability of the system never degrades once the data is increased or decreased. Scalability requires a permanent solution of the problem. The proposed system reduces the block size which makes the chain light in size. The logic behind the model is that the data stored in blockchain is comparatively lighter than the actual data. The log file associated with it keeps the load light and enhances the scalability of the network. This is also ensured that the security is not compromised while enhancing scalability.

B. Access Control

By adding the access control mechanism it is ensured that the restricted amount of data is required to be passed from the model. The definition of the roles is defined and data is passed from the chain. This not only promotes the security but also when the data is verified and passed the mechanism converts it into fix set of values. The fix data is forwarded to the blockchain model easily. This promotes scalability as well as security.

C. Security

The security is one of the prime attributes of the blockchain. The model allows the arbitrary values to be cross verified by the attribute-based model. This proposed model uses various permission and consensus levels to ensure the security of the model. Only authentic data is required to be transmitted from one node to other. Moreover, the data becomes even secure using blockchain technology because of its temper-proof and immutable nature.

TABLE VII. COMPARISON OF PROPOSED MODEL WITH RELATED WORK

Parameter	DASSCARE 2.0 [2]	Permission Control Model [11]	DASSCare [3]	CrowdMed [4]	Proposed Model
Scalability	High	High	Low	Low	High
Access Control	High	Moderate	Low	Moderate	High
Security	High	Low	Moderate	High	High
Data Integrity	Moderate	High	High	High	High
Access Control	Moderate	High	High	High	High

D. Integrity

Integrity is the trustfulness of the system which can be easily achieved by the blockchain technology. The stored information can never be changed by unauthentic channel. Integrity allows the information to be available to end users like doctors and patients. The developed smart contract does not allow any entry to change the values of the model. The access control model is responsible for managing and making the data available at each end.

E. Data Confidentiality

Data Confidentiality: The patient's medical records are stored and are confidential from any third-party disturbance. All these types of data are made available to the doctors and the patients. The patient data include various reports like blood group, records of X-Rays and Magnetic Resonance Imaging (MRI) scans. Smart contracts make this confidential as it consists of some strict rules placed inside it. The privacy can be ensured by using blockchain as well as the access control mechanism.

VIII. CONCLUSION

A solution to the challenge of managing access control in an e-health ecosystem has been described in this paper. This paper describes a solution to the problem of managing access control in an e-health ecosystem. Access control in e-health is particularly difficult because resources and data are dispersed across various places and institutions. The problem is exacerbated by the fact that not all e-health resources are owned by a single organization or individual. To establish the correctness of the scheme idea, a proof-of-concept had to be built and implemented. Success was largely due to proof-of-concept. Even if they are preliminary, some functional and application tests and validations verify that the technique is sound. Overall, we believe the technique is feasible, with numerous advantages over existing systems when compared. The benefits of this system include, but are not limited to, the fact that access control policies are communicated and synchronised across the consortium's institutions and organizations, assuring their integrity, transparency, and authenticity. The paper introduces a model where the time taken to create a new hash is 0.15625 microseconds. A total number of 64 transactions taken from the data set where the throughput is calculated for individual access are considered. After applying the formula, the calculated throughput is 32.5 microseconds. By the lighter block size, data can be made available to the patients. The research is for the patients so they can keep track of their medical history; and the deaths due to overdose of the medicines can be reduced. The future work of the proposed model includes finding more computational forces to make the blockchain size lighter and more scalable. Additionally, access control mechanisms should be implemented to ensure the integrity of the data coming from various sources.

REFERENCES

[1] Cision PR Newswire Prenswire https://www.prnewswire.com/news-releases/us-experienced-highest-ever-combined-rates-of-deaths-due-to-alcohol-drugs-and-suicide-during-the-covid-19-pandemic-301552480.html (Accessed-on 17/Oct/2022).

[2] M. Ayache, A. Gawanmeh and J. N. Al-Karaki, "DASS-CARE 2.0: Blockchain-Based Healthcare Framework for Collaborative Diagnosis in CIoMT Ecosystem," 2022 5th Conference on Cloud and Internet of Things (CIoT), 2022, pp. 40-47, doi: 10.1109/CIoT53061.2022.9766532.

[3] Al-Karaki, Jamal N.; Gawanmeh, Amjad; Ayache, Meryeme; Mashaleh, Ashraf (2019). [IEEE 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC) - Tangier, Morocco (2019.6.24-2019.6.28)] 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) - DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework.

[4] Mira Shah, Chao Li, Ming Sheng, Yong Zhang, Chunxiao Xing rowdMed: A Blockchain Based Approach to Consent Management for Health Data Sharing. Print ISBN: 978- 3-030-34481-8 Electronic ISBN: 978-3-030-34482-5 Copyright Year: 2019 https://doi.org/10.1007/978-3-030-34482-5.

[5] Hu.C., Li, C., Zhang, G. et al. CrowdMed-II: a blockchain-based framework for efficient consent management in health data sharing. World Wide Web (2022). https://doi.org/10.1007/s11280-021-00923-1.

[6] Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system, p. 9 (2008).

[7] Buterin, V.: On public and private blockchains, August 2015. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 06 June 2017.

[8] Salman, Tara, et al." Security services using blockchains: A state of the art survey." IEEE Communications Surveys Tutorials 21.1 (2018): 858-880.

[9] Damiano Di Francesco Maesa, Paolo Mori, and Laura Ricci. 2017. Blockchain based access control. In IFIP International Conference on Distributed Applications and Interoperable Systems. Springer, 206– 220.

[10] Castiglione A.; De Santis, A.; Masucci, B.; Palmieri, F.; Castiglione, A.; Li, J.; Huang, X. Hierarchical and shared access control. IEEE Trans. Inf. Forensics Secur. 2015, 11, 850–865.

[11] Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet Things J. 2018, 5, 1184–1195.

[12] Ouaddah, A.; Abou Elkalam, A.; Ait Ouahman, A. Fair Access: A new Blockchain-Based access control framework for the Internet of Things. Secur. Commun. Netw. 2016, 9, 5943–5964.

[13] Xu, R.; Chen, Y.; Blasch, E.; Chen, G. Blendcac: A smart contract enabled decentralized capability- Based access control mechanism for the iot. Computers 2018, 7, 39.

[14] Ouaddah, A.; Mousannif, H.; Elkalam, A.A.; Ouahman, A.A. Access control in the Internet of Things: Big challenges and new opportunities. Com- put. Netw. 2017, 112, 237–262.

[15] O. Novo, "Scalable Access Management in IoT Using Blockchain: A Performance Evaluation," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4694-4701, June 2019, doi: 10.1109/JIOT.2018.2879679.

[16] Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Com- puting and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.

[17] Touati, L.; Challal, Y. Poster: Activity-based access control for IoT. In Proceedings of the 1st International Workshop on Experiences with the Design and Implementation of Smart Objects, Paris, France, 7–11 September 2015; pp. 29–30.

[18] Mahalle, P.N.; Thakre, P.A.; Prasad, N.R.; Prasad, R. A fuzzy approach to trust-based access control in internet of things. In Proceedings of the Wireless VITAE 2013, Atlantic City, NJ, USA, 24–27 June 2013; pp. 1–5.

[19] Zhang, R.; Zhang, Y.; Ren, K. Distributed privacy-preserving access control in sensor networks. IEEE Trans. Parallel Distrib. Syst. 2012, 23, 1427–1438.

[20] Chen, Y., Meng, L., Zhou, H., & Xue, G. (2021). A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection. Wireless Communications and Mobile Computing, 2021.

[21] I. Baldine, Y. Xin, A. Mandal, P. Ruth, C. Heerman, and J. Chase, "Exogeni: a multi-domain infrastructure-as-a-service testbed," in Testbeds and Research Infrastructure. Development of Networks and Communities, pp. 97–113, Springer, 2012.

[22] https://www.kaggle.com/datasets/davidechicco/chronic-kidney-disease-ehrs-abu-dhabi (Accessed-on 17/Oct/2022).

[23] T. Wang, Y. Mei, X. Liu, J. Wang, H.-N. Dai, and Z. Wang, "Edge-based auditing method for data security in resource-constrained internet of things," Journal of Systems Architecture, vol. 114, p. 101971, 2021.

[24] Z. Xu and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," IEEE Journal on Selected Areas in Communications, vol. 38, no. 5, pp. 968–979, 2020.

[25] X. Liu, M. S. Obaidat, C. Lin, T. Wang, and A. Liu, "Movement-based solutions to energy limitation in wireless sensor networks: state of the art and future trends," IEEE Network, vol. 35, no. 2, pp. 188–193, 2021.

[26] W. Jerbi, O. Cheikhrouhou, H. Hamam, H. Trabelsi and A. Guermazi, "A blockchain-based storage intelligent," 2022 International Wireless Communications and Mobile Computing (IWCMC), 2022, pp. 635-640, doi: 10.1109/IWCMC55113.2022.9824790.

[27] Bogaerts, J., Decat, M., Lagaisse, B., Joosen, W.: Entity-based access control: supporting more expressive access control policies. In: Proceedings of the 31st Annual Computer Security Applications Conference, ACSAC 2015, pp. 291–300. ACM, New York (2015).

[28] Sharma, A., Yadav, D. P., Garg, H., Kumar, M., Sharma, B., & Koundal, D. (2021). Bone cancer detection using feature extraction-based machine learning model. Computational and Mathematical Methods in Medicine, 2021.

[29] Kumar, M., Bajaj, K., Sharma, B., & Narang, S. (2021). A Comparative Performance Assessment of Optimized Multilevel Ensemble Learning Model with Existing Classifier Models. Big Data.