Privacy Preservation Modelling for Securing Image Data using Novel Ethereum-based Ecosystem

Chhaya S Dule[1], Dr. Roopashree H.R[2]
Research Scholar, Dept. of CSE[1]
Assistant Professor, Department of CSE, Dayananda Sagar University Bangalore, India[1]
Research Supervisor and Associate Professor[2]
Department of Computer Science and Engineering[2]
GSSS Institute of Engineering and Technology for Women, Mysuru, VTU, Belgaum, Karnataka, India[1, 2]

Abstract*—The broad usage of images in real-time applications demands a cloud infrastructure due to its advantages. Many use cases are built where the image data is shared, sharing becomes the core function, and the medical domain takes its broad advantage. The cloud is a centralized infrastructure for its all-operation usages; it depends mainly on the trusted third party to handle security concerns. Therefore, the privacy preservation of the image data or any data becomes an issue of concern. The distrusted system advantages are achieved using blockchain technology for image data security and privacy concerns. The traditional approaches of the security and privacy models raise many apprehensions as these are designed on the centralized systems of the data sharing mechanisms. It is also observed that large data files are not wisely handled, which demands building a framework model that takes image data and any other data of any size to ensure a dependable optimal security system. This paper presents a framework model to achieve optimal time complexity for securing the privacy aspects of the image data or any other data that uses space optimal file system using distributed security mechanism for both the storage and sharing of the data. The proposed framework model for optimal time complexity and security uses a duplication algorithm using stakeholder agreement to ensure efficient access control to the resources using the cryptographic approach to the Ethereum ecosystem. The performance metric used in the model evaluation includes the degree of availability and efficiency. On benchmarks, it performs well compared to the traditional cloud-built distributed systems. The quantified outcome of the proposed scheme exhibits a 42.5% of reduction in time for data repositioning, a 41.1% of reduction in time for data retrieval, a 34.8% of reduction in operational cost, a 73.9% of reduction in delay, and a 61% faster algorithm execution time in contrast to conventional blockchain method.

Keywords*—Blockchain; data security; Ethereum; image data; privacy; security

I. INTRODUCTION

In the real world, many applications may include the Map image, medical images, or any other real-time images to be stored and shared to meet their respective objectives of map-based driving assistants, diagnostic systems for medical professionals, and smart transport systems [1-3]. These applications extract intrinsic information for the functional operation and computation of the applications, including general and private information. Vulnerability to private information is considered a loophole to the system's robustness [4-5]. Though the digital systems built for real-time applications boot the connivance of operation by suitable ecosystems, the cumulative data storage raises concerns about the considerable data handling challenges [6]. Application engineers and domain experts for an application built on the data storage and sharing required to analyze the data features of interest to meet the application goals. However, the data generator or uploader stakeholder may not be able to keep track of the data that might be useful to them. Digital data sharing provides ease of data analytics that ensures application efficiency and, as a result, yields an automatic and intelligent decision-making scheme for specific applications [7]. Though there exist many advantages of end-to-end systems for data or image data storing and sharing yet, significant challenges exist that require attention by the researchers, and those significant challenges include: 1) storage aspect of the extensive data in terms of time complexity of retrieval and 2) the vital security concerns. The research statistics reveal that data exist in heterogeneous formats, but the images are large in percentages [8]. The images are multi-dimension data and require larger storage space than other data formats. Its processing takes more and more computing storage to process and analyzes, limiting exploiting its usage for the application goals and efficiency. At the same time, vulnerability due to various system loopholes concerns data security and privacy information leakage. It lacks efficient interoperability requirements due to the inefficient trade-off handler capacity of the security models [9]. Most data possess critical and delicate material; therefore, preserving privacy is essential to maintain the stakeholder losses or damages, either financial or repute.

It is also essential that only the authenticated data be utilized to perform any analytical process, as the tampered image data or other data minimizes the accuracy and reliability of the results of the decision-making systems that may deceive the correctness of the system. The secure and fast system ensures better data interoperability, so sharing the data securely makes the system more robust and effective. The cloud ecosystem is today's most popular choice for flexible data storage and optimal sharing. However, towards the security of the data, the cloud ecosystem adopts practical cryptography and privacy preservation, and access control followed by the appropriate authentication schemes [10]. Irrespective of the various security schemes available for data security and privacy leakage protection, there are no full-proof adaptive

systems. The assumption lacks the reality that storage and data distribution do not have threats if it is through the cloud. This unreliability is because cloud security models largely depend upon a Trusted Third Party (TTP), and TTP suffers many collusion attacks without suitable non-repudiation schemes [11]. Regrettably, there is no typical confirmation instrument for prevailing systems, and there is no operative countermeasure to punish a malicious process in the cloud ecosystem. The most promising distributed technology platform Ethereum is gaining popularity. Recently, it has been used to build many security models or schemes to provide reliable and robust data-sharing systems using distributed databases [12]. The Ethereum-based platform facilitates distributed technology like blockchain. This open-source distributed database mechanism can be exploited to build effective authentication, access control, secure storage, and sharing schemes for an image or other data [13].

Though there are many significant advantages of the Ethereum-based distributed systems, many traditional approaches based on this technology limit their potential effect due to many of the issues that may include: Though there are many significant advantages of the Ethereum-based distributed systems. Still, many of the traditional approaches based on this technology limit their potential effect due to many of the issues that may include: 1) It lacks non-repudiation in the distributed databases as well as does not handle the large data effectively due to non-scalability factor as these distributed data is accessible to all the participating databases as a ledger. 2) Another associated problem is that it lacks control over the data access by the authenticated stakeholder. 3) And last but not least, to design an optimal system to minimize the time complexity and yet be robust enough to ensure system reliability and availability most securely. Literature reveals the fact that these problems are not handled well. Therefore, this paper deals with the two primary objectives: a framework component that balances the time complexity overhead for data security and privacy preservation of images or any other data over a distributed database storage and sharing ecosystem. This concept's prime agenda is also to balance privacy preservation with reduced time complexity associated with the data-sharing process on the distributed scale over cloud networks. To sum up, the contribution of the paper is as follows:

1) The framework model is deployed on the open-source Ethereum distributed database system over the cloud to validate the agreements among the stakeholders of the file storage and sharing process and authenticated access control mechanism.

2) The framework model exploits a unique type of file system, namely Space Optimal File System (SOFS), in the form of a node-to-node collaborative approach that can store the image or any other data to overcome the limitations of the centralized storing and sharing systems.

3) The framework is flexible to work not only on image data. Instead, it can work on any other data of regular or large files to overcome the limitations of the non-scalability in traditional systems built on distributed systems.

4) The cryptographic key mechanism is used for every chunk of the data so that data is not accessible to the SOFS ledgers

5) Finally, it provides a novelty of handling optimal time complexity and data security to ensure real-time feasible data storage and sharing mechanisms.

The paper is presented in six sections. The literature review is described in Section II, followed by a discussion of identified research gap in Section III. Section IV elaborates on the design and deployment aspects of the proposed framework model, an algorithm discussion is carried out in Section V, the performance analysis is described in Section VI, a discussion of the accomplished outcome is carried out in Section VII, and finally, Section VIII concludes the paper

II. Literature Review

Jiang et al. [14] choose a blockchain for the data store and search on the Ethereum platform by designing a price model using two distinguished stakeholders, namely the data owner, who is awarded for providing the data. Another stakeholder is the miner, who is granted the search operation. This model minimizes the keyword duplication cost to gain a cost advantage. Thus, Debe et al. [15] offer a distributed scheme using an Ethereum-based blockchain system to handle these issues. The system validation against the attack models shows resilience to it. In the work of Hasan et al. [16], a blockchain-based model deals with images and other data to handle the storage and the sharing contract among the stakeholders. A joint study on scalability and Adhoc usage of accountability is considered a research problem by Podgorelec et al. [17] and proposes a concept of state channel as a service (SaaS) that ensures secure distributed connections for off-site chain issues in the payment system. Another significant work in the healthcare domain is Madine et al. [18], which securely uses a specific file system, cryptography, and blockchain-based authorization architecture to share patient records' consent. In the work of Abou-Nassar et al. [19], an interoperable distributed trust model is proposed using blockchain using C# on Ethereum. A practical approach towards the design of "privacy-preserving permissioned blockchain architecture" has been presented by Lin et al. [20] by modifying the Ethereum and customized cryptographic intrinsic elements. The authors, Kumar et al. [21], highlight that along with health care, another domain like cryptosecurity, distributed data collaboration, and immutability take advantage of blockchain technologies. The work of Ullah et al. [22] highlights that though the current cloud ecosystem-based data store system provides many advantages but still lacks data leakage and risk to private information due to the centralized operations and dependency on the TTP, a single point of failure may collapse the system. In Yan et al. [23], a dynamic data upload process and search verification through a fuzzy keyword are proposed. Using E-blockchain and Rivest-Shamir Algorithm (RSA) ensures fairness between the user and the cloud data store. Xiang et al. [24] have presented a data trading mode using blockchain and machine learning by building a contract among the stakeholder by eliminating the TTP. The E-Blockchain is used to meet this requirement in the model proposed by Debe et al. [25], enables a decentralized agreement to establish trust-based sharing among the IoT devices and the fog, and performs well

compared to the existing trust model, which is centralized for its operation. Yet another recent and significant work by Hasan et al. [26] proposes the data chunk transfer process decentralized using blockchain that ensures privacy and confidentiality using a proxy cryptographic approach using a specific file system. Yang et al. [27] presented a layer-based trust approach using the Hyperledger architecture to handle this problem. It has been validated against the attack, namely distributed denial service (DDoS). However, one interesting fact about Ethereum, blockchain, and Smart Contracts is discussed in the work of Chen et al. [28], where the users encounter the threats of resource abuse. Saini et al. [29] presented a framework using Smart Contracts (SC) and blockchain (BC) for access control to secure healthcare-related data. Debe et al. [30] present a scheme that uses BC and SC for a decentralized Bidding process and a reputation system that cost-effectively ensures security. The use of BC and Ethereum with SC is also found in Kaynak et al. [31]. Table I highlights the summary of the above-related studies on security.

TABLE I. SUMMARY OF RELATED WORK

Approaches	Advantage	Limitation
Blockchain-based [14]-[19]	can secure different forms of data	No benchmarking
Blockchain with Cryptography [33]-[37], [39], [40]	Ensure privacy preservation, better access control, secure sharing	Computationally complex process
Homomorphic encryption [42]	Secure, ubiquitous data	Slow execution time
Traditional Public Key Encryption [32][41][38]	Simpler architecture, the supportability of wide varieties of application	Not resistive to dynamic attackers

Thus, this paper aims to fill this gap by designing a generalized framework model that supports image and non-image data using the Ethereum platform and cryptography for privacy preservation in an optimal time complexity way. The next section outlines problems derived from existing approaches.

III. IDENTIFIED RESEARCH CHALLENGE

After reviewing the existing schemes, specific research challenges have surfaced, which are as follows:

- A centralized server stores the information in most of the existing blockchain-based schemes. Such storage often invites identity theft, privacy leakage, and other associated security issues.
- Adopting complex security architectures requires proper knowledge to handle them in case of unidentified attacks on data. Mishandling of security features by data owners eventually leads to intrusion. At the same time, they also have to dependF on adopting trusted third parties, which are equally vulnerable from a data ownership viewpoint.
- Conventional blockchain-based operations cannot manage large-scale data and very often lead to scalability issues that degrade the performance of repositioning and querying the data from miners.
- The majority of existing studies suffer from loosely coupled ownership of data. Once the blockchain stores the data, the availability and reachability of data are far more to other users using malicious access policies.

Hence, the above mentioned research problems have been identified and are subjected to proposed solutions emphasizing data privacy preservation. Apart from this, the storing the image in conventional blockchain is usually centralized and there is higher possibility of intrusion, whereas Ethereum-based approach are decentralized and its control of validation is carried out by multiple nodes with higher accountability. Hence proposed study considers Ethereum-based ecosystem for this purpose. The following section discusses the adopted research methodology.

IV. RESEARCH METHODOLOGY

This paper proposes a customized framework model that supports image data security for its privacy preservation in the optimal time complexity by exploiting the Ethereum-based distributed data store system characteristics like blockchain.

The summary of the adopted method is as follows: The overall structure of the implementation is classified into four stages. The *first stage* of development is associated with constructing the Ethereum module, which maintains various associated repositories of data identity, timestamp, Secured Hash Algorithm (SHA), and auditor identity. The *second stage* of development is primarily responsible for request assessment and management of metadata. This module further contributes towards applying asymmetric encryption over the split data in adherence to the bandwidth capacity. The idea is to secure the storage units. The *third stage* of development performs authorization to the data requestor while Ethereum records are validated. Finally, the *fourth stage* of the proposed method introduces the smart agreement process, where the transactions are assessed and duplicate records are identified. The module finally performs a key updating process.

The framework aims to support or work on image data or other small to large-size and multi-dimension data to ensure the system's scalability. The core idea of the proposed scheme is to introduce an authorization mechanism for image data from various perspectives of the application using images; it could be for multi-disciplinary applications. It will also eventually mean that considered image data could easily take the shape of high-dimensional data, progressively increasing its challenge during the computational process. In the proposed scheme, the user is facilitated with the privilege to construct a tailored policy towards accessing their intellectual property (image) using an intelligent agreement system when applied with Ethereum blockchain. Further, a specific administrative use is responsible for uploading the comprehensive image data over the proposed storage network. The complete operation of uploading and accessibility to the file system calls for the usage of the exclusively designed request control message. The blockchain users initiate the uploading process upon receiving the request control message from the comprehensive storage network. Similarly, the retrieval process also demands the usage of different variants of request control messages by the blockchain user.

This operation further facilitates accessing and storing the data on the user's device. This data could also be accessed (after authorization) by other legitimate users and administrators to obtain prior and new information. The proposed scheme constructs the entire network in a peer-to-peer method where the role of the secure storage service provider can be played by the user, who is further required to get registered to play the role of blockchain user. Upon accomplishment of this initial step, such a user can facilitate all the computing nodes and accessibility towards storage services. To eliminate the constraints associated with storage and channel capacity, the proposed system adopts using distributed cloud server as the primary point of storage instead of opting for multiple local storage units. Once the request control message is obtained for prompting towards file storage task, the proposed scheme applies asymmetric encryption for its data to be stored in the blockchain network. Therefore, adopting encryption over securing the primary data acts as a security shield against any attempt of a security breach.

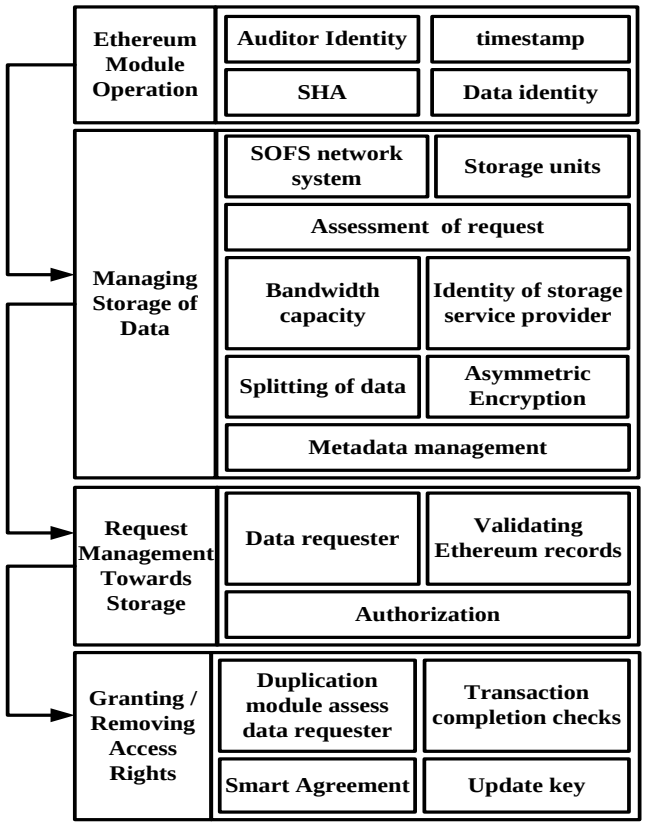

Fig. 1. Proposed architecture

Further the blockchain network is introduced with the recently encrypted data that also carry out sharing of information (related to secret key) in the blockchain network. This process also transforms private and public keys, which facilitates the blockchain user to gain potential control over the user's data either by revoking the request or permitting access. It should be noted that the proposed blockchain network performs interaction with the service provider of data using web 3.0. The usage of the Ethereum blockchain assists in managing multiple transactions records more effectively and securely. High-level planning of the functional framework model is shown in Fig. 1 with the inclusion of the stakeholders in general, which can be easily customized to any functional domain along with the intrinsic technologies used for the security and privacy-preserving way data is stored and shared. According to Fig. 1, four essential blocks of operation are carried out towards achieving the target of privacy preservation, mainly emphasizing balancing the security demands and optimal computational efficiency. Each modular block carries a discrete set of interconnected operations where the core image file is subjected to security processing over the Ethereum distributed data system.

The complete operation stated in Fig. 1 is highly sequential from top to bottom. Initially, the Ethereum module is constructed with hash-based encryption followed by asymmetric encryption over the split data. A scheme also maintains a better indexing process using metadata management based on every request. The module also assists in performing validation of the Ethereum records followed by final management of removing or accessing rights permission. A unique and smart agreement is designed, followed by updating key. The core logic of the architecture mentioned above is to ensure faster and safer data repositioning over a cloud environment in a distributed manner. The consecutive section further illustrates all the blocks discussed earlier regarding algorithm design.

V. Algorithm Implementation

From the discussion carried out in prior section, it is noted that proposed Ethereum-based ecosystem introduces a novel mechanism of image splitting which supports an extensive decentralization scheme followed by efficient request management for controlling image sharing. This section discusses the design of an algorithm implementation towards the methodology briefed in the prior section.

A. Strategies for Algorithm Implementation

The algorithm's execution begins with a user who forwards its data to the interface, delivering the data to the request's handler. This request is sent to the Ethereum module, further interacting with the SOFS and duplication modules. In parallel with this process, the encrypted data from the storage is also forwarded to the Ethereum client. A decentralized datastore system using hashing is used to arrange this data. This hashed data is then sent to the transaction pool and authenticator module, further updated towards the Ethereum client. The data from the duplication module is now forwarded to the intelligent agreement management module controlled by the data owner. It is also delivered to the request handler for the next Ethereum client module. Updating operations of these transactions are simultaneously carried out in this process. Apart from this, the complete blocks of the data considered for the proposed implementation are the access scheme, duplication module, and pairing of keys. All these three blocks consist of essential information associated with the identity of the auditor for the Ethereum client, innovative agreement, the signature of the user, identity of the client, identity of data, value of hashed data, and time stamp. These are also the seven essential components of the Ethereum module. It should be noted that proposed scheme of privacy preservation adopted are hybridized form of both transactional and smart contract-based

privacy in Ethereum in order to keep a balance in storage and security at same time.

B. Algorithm Design

The core algorithm of the proposed scheme consists of the following operations, i.e., Ethereum module operation, managing storage of data, request management towards storage, and granting/removing access rights. The core steps of the proposed algorithm are as follows:

Algorithm for Securing image using Ethereum

Input: m (Components of Ethereum)
Output: d_{val} (validated data)
Start
1. **For** c=1:m
2. $R_{req} \rightarrow E_c$
3. $E_c \rightarrow S_{net} \rightarrow$
4. $S_{net} \rightarrow val(avail(S_c))$
5. $S_{net} \rightarrow confirm(S_c)$
6. $data_1 \leftarrow f_1(Data)^n$
7. $data_2 \leftarrow f_2(data_1)$
8. $data_3 \rightarrow f_3(data_2)$
9. obtain d_{val}
10. **End**
End

The discussion of prime operations toward each algorithmic step is as follows:

- *Ethereum Module Operation*: This is the initial module of implementation, which models the proposed Ethereum module focusing on privacy preservation towards image data. The proposed study considers the auditors' identity based on their computing devices. The study also uses a conventional Secured Hash Algorithm of a crucial size of 256 bits to hash the data for each image data chunk. A unique identifier is used for allocating the identity of stakeholders. There must be trust established between the SOFS network and the requestor node. The proposed system considers an innovative agreement, similar to smart contract, a well-structured program executed over the Ethereum module. Its primary responsibility is to validate all incoming data access requests for storage that are accessible to all the users of the Ethereum module. All the transactions of any form are carried out by the Ethereum module, which is highly distributed to offer better and faster access to files. The algorithm considers *m* number of components of the E_c Ethereum module (Line-1), where the data provider performs initiation of its reposition request R_{req} via its interface (Line-2).

- *Managing Storage of Data*: This module is responsible for managing all forms of incoming requests, encryption, and storage simultaneously. The Ethereum client E_c forwards its information to the S_{net} SOFS network (Line-3). It should be noted that all form of file request for storage is initially accepted by the storage units, which are regular users and part of the Ethereum client system interconnected via the cloud ecosystem. The confirmation of the storage space S_c must be done by the Ethereum client (Line-5) by priorly validating them using the *val* method concerning their availability (Line-4). The S_c module carries out the request verification by constructing an array that retains all transactions of accepted files to be stored (Line-5). This operation significantly reduces time complexity from both storage and query processing. The S_c module carries out the identity of the storage unit offered by any cloud service provider concerning channel capacity and storage space availability with a duplication module.

- *Request Management Towards Storage*: This module carries out specific operation steps before managing all forms of requests. The complete input of an image data is split into the equivalent size of blocks of *n* number using an explicit function $f_1(x)$ to generate split data $data_1$ (Line-6). This operation offers a beneficial solution for dealing with more extensive or high-dimensional datasets. It is to be noted that the process carried out by SOFS is entirely decentralized, and hence there is no event of failures in storing split data over multiple storage units over the cloud. Further, an explicit function $f_2(x)$ is used for performing the RSA, which is stored in the form of tree-based networks over the storage units (Line-7). This operation results in multiple encrypted data $data_2$ (Line-7). The time complexity problem further reduces as the complete encryption is carried out in parallel to all the chunks of the data.

- Apart from this, storing the stakeholder's metadata on the E_c module's block is essential, although they are stored in the SOFS network system for their original data input. The proposed scheme also audited this data at a specific periodic interval, forwarding the signature to the following consecutive data blocks. The E_c will synchronize all the generated encrypted blocks of data. An interesting point from a security perspective is that a tiny amendment being carried out on any one block will change the whole setup of blocks of data due to any malicious activity. Hence, even if one block of data is stolen or compromised, it will be useless for an attacker. An additional layer of security is further implemented by storing the hashed value of these data to mitigate the problem of data leakage over cloud servers. The complete management of the data blocks is carried out so that the proposed algorithm evaluates the legitimacy of the data requester as a mandatory step. Suppose the requestor's identity is legitimate (from the metadata). In that case, it is added to the Ethereum distributed data system record, which is finally forwarded to the data storage unit. This operation potential assists in retaining maximum accountability of image data on SOFS network. Moreover, this accountability is carried out at period interval of time to keep the blocks updated thereby maintaining higher transparency. All the accessing of data can be carried out from this module. However, if the data requestor is found illegitimate (not a data owner), the proposed algorithm checks the access policy by updating the

records maintained by the Ethereum-distributed data system. In short, the Ethereum client maintains all the forms of the legitimate and illegitimate list of requestor nodes, resisting any attacker from accessing the file maliciously.

- *Granting / Removing Access Rights*: Using the verification process managed by the Ethereum client system, the valid data requestor can initiate the transactions, followed by regular updating towards the Ethereum client. However, for optimal security, the algorithm further steps towards updating its public or private key by generating a new version of it. The SOFS network system carries out this operation to control crucial sharing by granting or removing access rights. The beneficial aspect of this operation is that it can offer a higher degree of data privacy, eliminating the probability of key-based attacks. In this process, an explicit function $f_3(x)$ is designed to manage the intelligent agreement system which is primarily response for handling data access request along with permission to be granted for access/deny (Line-8). For this purpose, the proposed scheme develops a duplication module for testifying its evidence based on four types of keys, i.e., keys to be used for preliminary instance, keys that are eliminated for the first time, and second and third time considering public and private keys. This operation generates $data_3$, which ultimately yields validated data d_{val} (Line-9). The proposed algorithm also maintains a record of all the access *Rec*. The process carried out by function $f_3(x)$ can now be further extended: The algorithm assesses the event of successful completion of the accessing by the stakeholder, followed by eliminating the keys for all the identified instances. The intelligent agreement module reviews the complete record of access Rec, which finally generates a new record *Rec*. The algorithm enforces the stakeholder to request access if their old access record is not found in this *Rec*. The unique access is generated by yielding new key pairs, then applying asymmetric encryption to all the split data blocks and generating a key for encryption. The generation of the unique access is the contribution towards deploying a unique security measure to resist unauthorized data access. The storage system of the SOFS network receives this encoded file as well as the private key of the stakeholder. The file is further encrypted when it arrives within the SOFS network system while the user's private key is shared. All the keys are eliminated once the system records access completion, which makes the scheme high-level secured from intrusive activity on stored data.

VI. Result Analysis

The implementation of the proposed study is carried out on a conventional windows machine with 16 GB RAM and Core-i7 processor. An open-source server environment has been adopted for Java scripting the proposed algorithm. The proposed scheme also uses a high-level object-oriented language to deploy innovative agreements over an Ethereum environment. A standard benchmark test environment of Mocha 6.2.0 is used, while Ganache is considered for the Ethereum platform. The complete assessment is carried out over a standard Kovan testnet. The standard nodes from Amazon Web Services, i.e., AWS nano, are considered for the storage nodes that perform their data transmission over 100mps with NVIDIA GEFORCE GTX as GPU. The performance parameters considered for assessing the proposed system with the existing system (conventional blockchain) are as follows:

- *Time for Data Reposition*: This is the time required to store the data in the distributed cloud servers after being subjected to block operations.
- *Time for Data Retrieval*: This is the time required for the stakeholder to access their stored data from distributed location to their local system.
- *Operational Cost*: This is the cumulative number of resources (in memory and bandwidth) used for overall repositioning and retrieval processing.
- *Delay*: This is latency associated with data transmission from one point to another. The study considers cumulative delay for both repositioning and retrieval.

The proposed system is evaluated based on 100 GB of sample data programmatically generated traffic in IoT. Assessed over 1200 simulation rounds, the sample data is allocated and increased arbitrarily to map with a practical world environment.

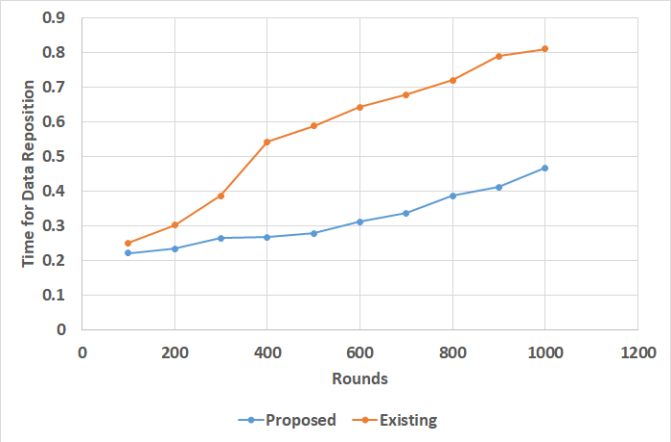

Fig. 2. Analysis of time for data reposition

Fig. 2 highlights the time required to store the data, stating the proposed system offers very little time consumption compared to conventional blockchain technology. The prime reason behind this is the higher dependency on adopting consensus-based mechanisms by traditional blockchain technology, which also induces scalability issues. On the other hand, the proposed scheme doesn't have any such dependencies that result in faster processing. Apart from this, conventional blockchain technology is inherently characterized by a slower process if the size of the network increases. A closer look into the proposed scheme shows that the tree-based structuring of hashed data makes the flow of the encoded blocks of spitted data much faster than the existing scheme.

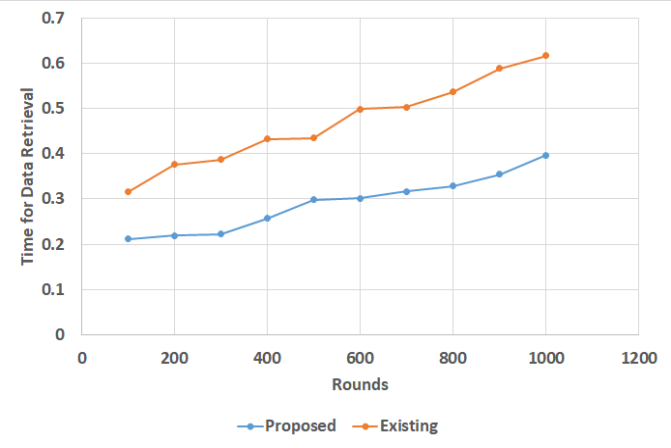

Fig. 3. Analysis of time for data retrieval

Fig. 3 highlights that the proposed system offers much-reduced consumption of time for retrieval of data in comparison to the conventional blockchain. A similar reason for time for repositioning can be stated as its cause. Apart from this, the process of metadata management by the SOFS network system makes the faster process of requestor legitimacy. Although it depends upon the synchronization time of updating, it still offers speedier query processing. Conventional blockchain has a higher dependency on node operation. In contrast, the proposed scheme outsources this dependency towards the Ethereum distributed database system using the SOFS network system, making the retrieval system relatively faster with a speedy auditing process for the information request.

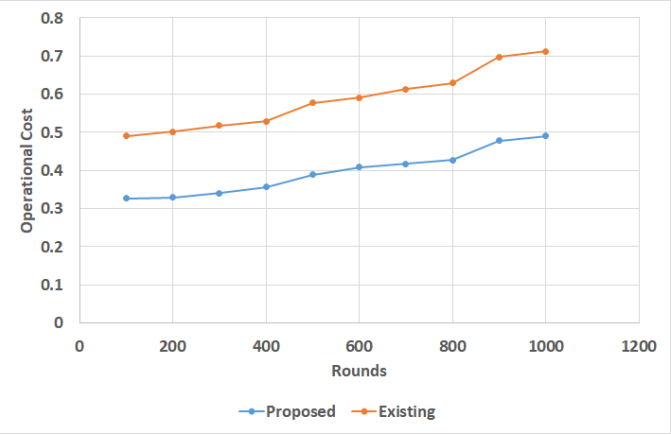

Fig. 4. Analysis of operational cost

Fig. 4 showcases that the proposed system offers reduced operational costs compared to conventional blockchain technology. Operational cost is one of the prime performance parameters to ascertain the applicability of the blockchain process toward data security in a realistic environment. The prime rationale behind this outcome is that traditional blockchain enforces the miners to solve problems with updates of new transactions by the ledger, which consistently increases resource dependencies. On the contrary, the proposed scheme controls its resource inclusion as a preemptive method of computing the entire path of data forwarding to the distributed storage unit, considering all the constraints from a security perspective. This offers a reduced consumption of resources leading to reduced operational costs.

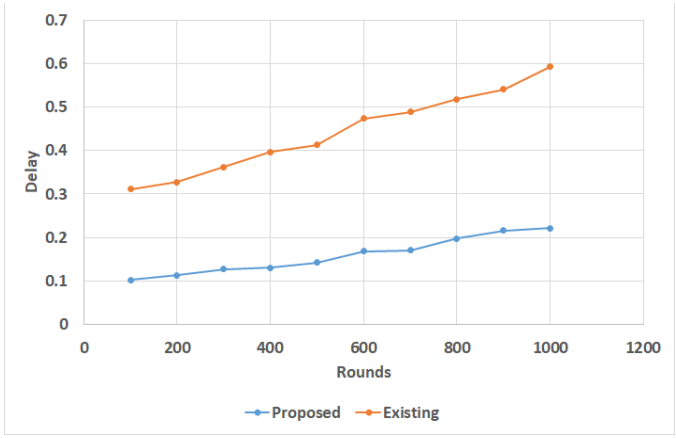

Fig. 5. Analysis of delay

Fig. 5 showcases that the proposed system offers a significantly reduced delay trend compared to conventional blockchain. It is to be noted that traditional blockchain forces the individual to have their key to make it completely decentralized. This process offers a sophisticated key management scheme and increases the information stored and retrieved. This eventually leads to a potential lag in time. However, the proposed system provides innovative agreement management, supporting faster auditing tasks over split encrypted data. Hence, irrespective of the usage of the RSA scheme, there are no complications towards key management both during storing and retrieval. The proposed system offers reduced delay trends to support various online applications over distributed cloud applications and services. Hence, the proposed method provides evidence to show its complete control over reducing time complexity.

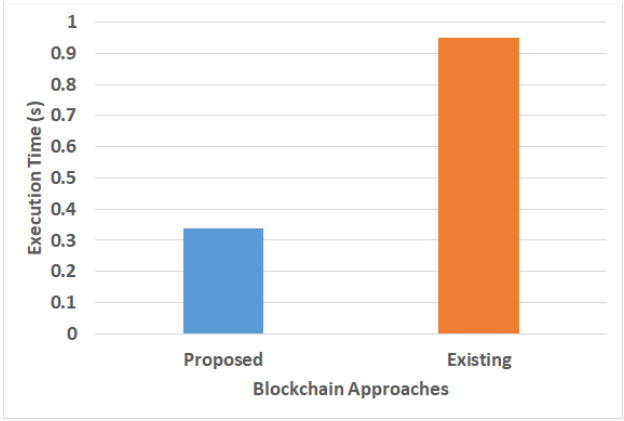

Fig. 6. Analysis of execution time

From the point of benchmarking, the proposed evaluation process considers assessing execution time. It should be noted that an indirect evaluation of memory is analyzed in the operational cost metric exhibited in Fig. 4. The outcome exhibited in Fig. 6 showcases that the proposed blockchain approach offers approximately 61% faster execution time compared to the existing blockchain scheme. A similar reason

stated for preliminary analysis is also to be attributed for this outcome. Hence, it is found that the proposed system can perform cost-effective computational operations in IoT.

VII. DISCUSSION

The graphical outcome highlighted in the prior section shows that the proposed blockchain-based operation offers better performance than conventional blockchain architecture in various respects. One of the prime reasons for the betterment in performance is its non-dependency from any entities associated with a trusted third party as witnessed in existing system [11]. This process is enabled using the proposed smart agreement system incorporated in the system design connected to processing the data over the network. This fact also contributes towards a lesser operational cost score for the proposed system, as noted in Fig. 4. The outcome will also contribute towards an effective large-scale data-sharing process among multiple enterprises. Apart from this, it can be noted that the proposed scheme offers reduced delay (Fig. 5) and time of retrieval (Fig. 3); owing to faster computational speed, the proposed scheme significantly controls the scalability problem in conventional blockchain design. This process is implemented by using the sharding mechanism.

From the perspective of the privacy preservation viewpoint, there is a potential difference between conventional and proposed Ethereum design methodology. The conventional Ethereum experience low processing speed whereas processing speed is much lower for proposed scheme. Apart from this, proposed scheme maintains a novel blockchain network topology with higher control of data and transaction where the compliance is monitored using smart agreement with updates. This offers higher privacy conservation in contrast to existing Ethereum.

Unlike the existing mechanism of secure data sharing [7][8][12][13][16][25], as illustrated in Section II, the proposed system enables the direct accessibility of the data to its owner. The data owner can carry out the associated process of its access policy and its need for amendment or customization. Hence, complete control of data ownership is retained in the proposed scheme in adherence with the smart agreement of laws towards privacy protection. From the perspective of legal authority of General Data Protection Regulation (GDPR), it is known that blockchain system is always considered to possess a data controller (where at least one legal person resides) in order to ensure the correct implementation of law of data protection in EU. Such forms of data controllers are mandatory require to adhere to the protocols of GDPR. Hence, the proposed scheme of Ethereum, in spite of its decentralized scheme, always offers its architecture to be controlled by multiple authorities in order to ensure data privacy as per the algorithm implementation.

VIII. CONCLUSION

The proposed concept presents a discussion about a novel computational framework that harnesses the potential of the Ethereum distributed database system for facilitating a secure validation of the data or any participating nodes towards storing and retrieving the data from distributed cloud servers. The novelty of the proposed scheme is as follows:

1. The model presents a duplication module for evidence to offer an assurance of the legitimacy of each transaction being carried out by the Ethereum-based distributed database system
2. The proposed scheme introduces a novel image data-sharing process and associated access policy management using a unique intelligent agreement system.
3. The complete assessment is carried out over Amazon Web Service nano nodes for standardizing its outcome using the SOFS network system and Ethereum client
4. The proposed scheme can control all the problems that impede decentralization using distributed storage units organized by the SOFS network system. At the same time, the complexity associated with data security and scalability is addressed using the presented splitting of data followed by encryption on every split data.
5. The proposed system offers approximately i) 42.5% of reduction in time for data repositioning, ii) 41.1% of reduction in time for data retrieval, iii) 34.8% of reduction in operational cost, and iv) 73.9% of reduction in delay trend in comparison to conventional blockchain method.

The possible shortcoming of the paper is that it is further required to be evaluated on real ground and find a similar consistency in its outcome. More test environments are further required to ensure this. From the above outcomes assessed on a standard benchmarked testbed, it can be stated that the proposed scheme offers better control over time complexity and high-end data privacy. Future work will further extend the present model toward more optimization-based processing. For this purpose, various bio-inspired approaches will be investigated to improve the blockchain operation further. The major emphasis will also be given to the impact of the massive peak and concurrent bottleneck conditions on the performance of blockchain operations. Further in order to offer higher privacy preservation over proposed scheme, the future work direction will be to extract the stochastic trends of dynamic attacker considering the network attributes to develop a novel attack map. This distributed attack map can be used for sandboxing any form of illegitimate or suspicious data request to further confirm the legitimacy of the request. Improving upon encryption protocol over such distributed attack map is anticipated to offer higher degree of privacy preservation.

REFERENCES

[1] H. Li, J. Liu, and X. Zhou, "Intelligent Map Reader: A Framework for Topographic Map Understanding With Deep Learning and Gazetteer," in IEEE Access, vol. 6, pp. 25363-25376, 2018, doi: 10.1109/ACCESS.2018.2823501

[2] Y. Zheng et al., "Histopathological Whole Slide Image Analysis Using Context-Based CBIR," in IEEE Transactions on Medical Imaging, vol. 37, no. 7, pp. 1641-1652, July 2018, doi: 10.1109/TMI.2018.2796130

[3] I. Z. Hong, D. Ming, K. Zhou, Y. Guo, and T. Lu, "Road Extraction From a High Spatial Resolution Remote Sensing Image Based on Richer Convolutional Features," in IEEE Access, vol. 6, pp. 46988-47000, 2018, doi: 10.1109/ACCESS.2018.2867210.

[4] B. Jiang, M. Seif, R. Tandon, and M. Li, "Context-Aware Local Information Privacy," in IEEE Transactions on Information Forensics

and Security, vol. 16, pp. 3694-3708, 2021, doi: 10.1109/TIFS.2021.3087350.

[5] J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy Preserving Social Network Data Publication," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1974-1997, third quarter 2016, doi: 10.1109/COMST.2016.2533668.

[6] A. K. Sandhu, "Big data with cloud computing: Discussions and challenges," in Big Data Mining and Analytics, vol. 5, no. 1, pp. 32-40, March 2022.

[7] G. Akkuzu, B. Aziz and M. Adda, "Towards Consensus-Based Group Decision Making for Co-Owned Data Sharing in Online Social Networks," in IEEE Access, vol. 8, pp. 91311-91325, 2020, doi: 10.1109/ACCESS.2020.2994408.

[8] L. Dong et al., "A Hierarchical Distributed Processing Framework for Big Image Data," in IEEE Transactions on Big Data, vol. 2, no. 4, pp. 297-309, 1 December 2016, doi: 10.1109/TBDATA.2016.2613992.

[9] R. G. Sonkamble, S. P. Phansalkar, V. M. Potdar, and A. M. Bongale, "Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR," in IEEE Access, vol. 9, pp. 158367-158401, 2021, doi: 10.1109/ACCESS.2021.3129284.

[10] S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park, and R. Sandhu, "Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future," in IEEE Access, vol. 9, pp. 107200-107223, 2021, doi: 10.1109/ACCESS.2021.3101218.

[11] W. Fang, N. Cui, W. Chen, W. Zhang, and Y. Chen, "A Trust-Based Security System for Data Collection in Smart City," in IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4131-4140, June 2021, doi: 10.1109/TII.2020.3006137.

[12] H. R. Hasan et al., "A Blockchain-Based Approach for the Creation of Digital Twins," in IEEE Access, vol. 8, pp. 34113-34126, 2020, doi: 10.1109/ACCESS.2020.2974810.

[13] M. Zichichi, S. Ferretti and G. D'Angelo, "A Framework Based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems," in IEEE Access, vol. 8, pp. 100384-100402, 2020, doi: 10.1109/ACCESS.2020.2998012.

[14] S. Jiang and J. Wu, "A Blockchain-Powered Data Market for Multi-User Cooperative Search," in IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 203-215, March 2022. doi: 10.1109/TNSM.2021.3125604

[15] M. Debe, K. Salah, M. H. Ur Rehman and D. Svetinovic, "Monetization of Services Provided by Public Fog Nodes Using Blockchain and Smart Contracts," in IEEE Access, vol. 8, pp. 20118-20128, 2020. doi: 10.1109/ACCESS.2020.2968573

[16] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar and S. Ellahham, "Blockchain-Enabled Telehealth Services Using Smart - Contracts," in IEEE Access, vol. 9, pp. 151944-151959, 2021. doi: 10.1109/ACCESS.2021.3126025

[17] B. Podgorelec, M. Heričko and M. Turkanović, "State Channel as a Service Based on a Distributed and Decentralized Web," in IEEE Access, vol. 8, pp. 64678-64691, 2020. doi: 10.1109/ACCESS.2020.2984378

[18] [18] M. M. Madine et al., "Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records," in IEEE Access, vol. 8, pp. 225777-225791, 2020. doi: 10.1109/ACCESS.2020.3045048

[19] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O. -Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," in IEEE Access, vol. 8, pp. 111223-111238, 2020. doi: 10.1109/ACCESS.2020.2999468

[20] C. Lin, D. He, X. Huang, X. Xie, and K. -K. R. Choo, "PPChain: A Privacy-Preserving Permissioned Blockchain Architecture for Cryptocurrency and Other Regulated Applications," in IEEE Systems Journal, vol. 15, no. 3, pp. 4367-4378, Sept. 2021. doi: 10.1109/JSYST.2020.3019923

[21] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, "A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes," in IEEE Access, vol. 8, pp. 118433-118471, 2020. doi: 10.1109/ACCESS.2020.3004790

[22] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," in IEEE Access, vol. 10, pp. 36978-36994, 2022.doi: 10.1109/ACCESS.2022.3164081

[23] X. Yan, X. Yuan, Q. Ye, and Y. Tang, "Blockchain-Based Searchable Encryption Scheme With Fair Payment," in IEEE Access, vol. 8, pp. 109687-109706, 2020. doi: 10.1109/ACCESS.2020.3002264

[24] W. Xiong and L. Xiong, "Smart Contract Based Data Trading Mode Using Blockchain and Machine Learning," in IEEE Access, vol. 7, pp. 102331-102344, 2019. doi: 10.1109/ACCESS.2019.2928325

[25] M. Debe, K. Salah, M. H. U. Rehman and D. Svetinovic, "IoT Public Fog Nodes Reputation System: A Decentralized Solution Using Ethereum Blockchain," in IEEE Access, vol. 7, pp. 178082-178093, 2019. doi: 10.1109/ACCESS.2019.2958355

[26] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic and M. Omar, "Trustworthy IoT Data Streaming Using Blockchain and IPFS," in IEEE Access, vol. 10, pp. 17707-17721, 2022. doi: 10.1109/ACCESS.2022.3149312

[27] H. Yang, J. Yuan, H. Yao, Q. Yao, A. Yu, and J. Zhang, "Blockchain-Based Hierarchical Trust Networking for JointCloud," in IEEE Internet of Things Journal, vol. 7, no. 3, pp. 1667-1677, March 2020. doi: 10.1109/JIOT.2019.2961187

[28] T. Chen et al., "GasChecker: Scalable Analysis for Discovering Gas-Inefficient Smart Contracts," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 3, pp. 1433-1448, 1 July-Sept. 2021. doi: 10.1109/TETC.2020.2979019

[29] Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao and Y. Zhang, "A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5914-5925, 1 April 1, 2021. doi: 10.1109/JIOT.2020.3032997

[30] M. Debe, K. Salah, M. H. U. Rehman and D. Svetinovic, "Blockchain-Based Decentralized Reverse Bidding in Fog Computing," in IEEE Access, vol. 8, pp. 81686-81697, 2020. doi: 10.1109/ACCESS.2020.2991261

[31] B. Kaynak, S. Kaynak and Ö. Uygun, "Cloud Manufacturing Architecture Based on Public Blockchain Technology," in IEEE Access, vol. 8, pp. 2163-2177, 2020. doi: 10.1109/ACCESS.2019.2962232

[32] Y. Zhang, C. Xu, J. Ni, H. Li, and X. S. Shen, "Blockchain-Assisted Public-Key Encryption with Keyword Search Against Keyword Guessing Attacks for Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1335-1348, 1 Oct.-Dec. 2021. doi: 10.1109/TCC.2019.2923222

[33] R. Akkaoui, X. Hei and W. Cheng, "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange," in IEEE Access, vol. 8, pp. 113467-113486, 2020. doi: 10.1109/ACCESS.2020.3003575

[34] S. Wang, R. Pei and Y. Zhang, "EIDM: A Ethereum-Based Cloud User Identity Management Protocol," in IEEE Access, vol. 7, pp. 115281-115291, 2019. doi: 10.1109/ACCESS.2019.2933989

[35] O. Alkadi, N. Moustafa, B. Turnbull, and K. -K. R. Choo, "A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9463-9472, 15 June 15, 2021. doi: 10.1109/JIOT.2020.2996590

[36] S. Wang, X. Wang and Y. Zhang, "A Secure Cloud Storage Framework With Access Control Based on Blockchain," in IEEE Access, vol. 7, pp. 112713-112725, 2019. doi: 10.1109/ACCESS.2019.2929205

[37] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Outsourcing Service Fair Payment Based on Blockchain and Its Applications in Cloud Computing," in IEEE Transactions on Services Computing, vol. 14, no. 4, pp. 1152-1166, 1 July-Aug. 2021. doi: 10.1109/TSC.2018.2864191

[38] Y. Yang, H. Lin, X. Liu, W. Guo, X. Zheng, and Z. Liu, "Blockchain-Based Verifiable Multi-Keyword Ranked Search on Encrypted Cloud With Fair Payment," in IEEE Access, vol. 7, pp. 140818-140832, 2019. doi: 10.1109/ACCESS.2019.2943356

[39] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health

Systems," in IEEE Access, vol. 7, pp. 66792-66806, 2019. doi: 10.1109/ACCESS.2019.2917555

[40] Y. Wang, A. Zhang, P. Zhang and H. Wang, "Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain," in IEEE Access, vol. 7, pp. 136704-136719, 2019. doi: 10.1109/ACCESS.2019.2943153

[41] X. Zhang, J. Zhao, C. Xu, H. Li, H. Wang, and Y. Zhang, "CIPPPA: Conditional Identity Privacy-Preserving Public Auditing for Cloud-Based WBANs Against Malicious Auditors," in IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1362-1375, 1 Oct.-Dec. 2021. doi: 10.1109/TCC.2019.2927219

[42] R. Awadallah, A. Samsudin, J. S. Teh, and M. Almazrooie, "An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain," in IEEE Access, vol. 9, pp. 69513-69526, 2021. doi: 10.1109/ACCESS.2021.3077123.