Cloud-Based Blockchain Technology for Data Storage and Security

Govindaiah Simuni [1,*] and Avinash Reddy Kandlakunta [2]

[1] Vice President and Technology Manager, Bank of America, 100 North Tryon Street, Charlotte, NC 28255, USA.
[2] Software Engineer, Accenture, Texas, USA.

* Corresponding author. Email: simunigovi@gmail.com (G.S.); kandlakuntaavinashreddy@gmail.com (A.R.K.)
Manuscript received March 10, 2025; accepted June 5, 2025; published August 22, 2025.
DOI: 10.18178/IJBTA. 2025.3.2.95-113

Abstract: Cloud computing has revolutionized data storage, offering scalable and flexible solutions for diverse applications. Despite its advantages, significant concerns regarding data security, privacy, and integrity remain. Blockchain technology, renowned for its decentralized, transparent, and tamper evident properties, presents a promising solution to address these challenges. This paper explores the integration of blockchain technology with cloud-based data storage systems to enhance security and trustworthiness. We propose a novel framework that leverages the immutable nature of blockchain to ensure data integrity, confidentiality, and availability in cloud environments. Our research delves into the architectural design, implementation challenges, and potential benefits of the proposed system. Key components include decentralized data management, secure data sharing, and robust access control mechanisms. Additionally, we discuss the integration of smart contracts for automated data governance and compliance. The effectiveness of our approach in safeguarding data against unauthorized access, tampering and data breaches is demonstrated while maintaining high performance and scalability. The proposed framework aims to provide a secure, efficient, and trustworthy solution for data storage in the era of cloud computing.

Keywords: cloud computing, blockchain technology, data security, data storage, smart contracts, decentralized data management, secure data sharing, access control

1. Introduction

Cloud computing has revolutionized the way data is stored, processed, and accessed, offering scalable and flexible solutions that cater to the needs of a diverse range of applications. By leveraging the cloud, organizations can outsource their data storage and computational needs to third- party service providers, thereby reducing the costs associated with maintaining physical infrastructure. The on-demand nature of cloud computing, coupled with its ability to provide virtually unlimited storage and processing power, has made it an indispensable tool in today's data-driven world.

Despite these advantages, cloud computing introduces significant concerns related to data security, privacy, and integrity. The centralized nature of cloud service providers means that users must place a great deal of trust in these entities to manage and protect their data. This centralization poses several risks, including unauthorized access by malicious actors, data breaches, and potential data loss due to infrastructure failures or malicious actions by insiders. Furthermore, the multi-tenant nature of cloud

environments, where multiple users share the same physical resources, amplifies these risks, as vulnerabilities in one tenant's environment can potentially be exploited to gain access to another tenant's data.

Blockchain technology has emerged as a potential solution to many of these challenges, offering a decentralized approach to data management that inherently enhances security and trust. Originally developed to support cryptocurrencies like Bitcoin, blockchain technology has since been recognized for its broader applications across various domains. At its core, blockchain is a distributed ledger that records transactions across multiple nodes in a network. This decentralized structure ensures that no single entity has control over the entire data set, thereby mitigating many of the risks associated with centralized systems.

One of the key features of blockchain technology is its immutability. Once data is recorded on the blockchain, it cannot be altered or deleted without the consensus of the network participants. This property provides a robust mechanism for ensuring data integrity, as any attempt to tamper with the data is immediately evident to all participants. Additionally, blockchain employs cryptographic techniques to secure data, ensuring that it can only be accessed by authorized parties. These features make blockchain an attractive option for enhancing the security and integrity of data stored in cloud environments.

This paper explores the integration of blockchain technology with cloud-based data storage systems to create a secure, efficient, and trustworthy solution for managing data [1]. We propose a novel framework that leverages the strengths of both technologies to address the inherent security vulnerabilities of cloud computing. By incorporating blockchain's decentralized data management capabilities, the framework aims to provide enhanced security, privacy, and data integrity in cloud environments.

The proposed framework consists of several key components, including a decentralized data management system, secure data sharing mechanisms, and robust access control protocols. Additionally, the framework integrates smart contracts to automate data governance and ensure compliance with relevant regulations. Smart contracts are digital contracts that execute on their own once the language of the contract has been coded. They execute and implement the conditions of a contract whenever certain conditions are achieved, making such systems very secure and clear.

As an example of the considerations made while deriving the proposed framework, the authors describe its overall architecture and the relationships between its elements. Some of the questions that this paper seeks to answer encompass, performance enhancement, size of such a system, and compatibility with other systems. An important characteristic is performance, because the application of the blockchain concept can bring several limitations concerning latency and throughput that need to be solved in order for the system to be effective. This is something that is crucial both in the cloud systems and in the blocks — the system's ability to scale, that is to accommodate more data and more transactions as time goes by without slowing down. The system should be interoperable to fit well with the current cloud environment and infrastructure hence make a smooth transition to the organizations that adopts the system.

This research also entails the assessment of the efficiency of the presented framework to determine the framework's ability in preventing the data leakage, unauthorized modifications, and unauthorized access. We also discuss how our solution performs and is secured compared to a regular cloud storage solution and discuss the advantages and drawbacks of utilizing blockchain essence. The analyses presented show that the major contributions of the developed framework increase data protection and reliability and remain in the range of high efficiency and expandability.

Besides the technological features that have been addressed, further, we identify possible sectors and practical purposes that can be applied to the proposed system. For example, in the financial sector the usage of such a framework can increase the security of the transactions in general and prevent frauds while

meeting the requirements of the law. In the healthcare industry, the system can keep the patient's data secure and private and it can also serve as a means of sharing patient's details among various authorized institutions. Supply chain management can also improve using the framework in as much as it provides total track and trace of goods, thus enhancing the efficiency in SCM while minimizing on counterfeits.

This paper is organized as follows: We kick off the paper with the background of prior studies to establish the background and context of our study, which focuses on the previous work performed in terms of combining blockchain and cloud solutions. We then discuss the feature level of the proposed framework and explains what each component of the framework does along with its operations. Security and privacy concerns are then discussed, which presents the threats that are countered by the framework and the approaches used to counter them. Finally, we explain how the process of implementing the system should be carried out and discusses the expected results of the experiments; the aim is to give a detailed picture of the effectiveness and security concerns of the presented system. Lastly, we consider the usability and possible scenarios that can be implemented when working with ICT and outside IT industry job opportunities and prospects of this field, together with strengths and weaknesses, as well as future developments in this area before summarizing key conclusion for practitioners and researchers.

Therefore, based on the present study and by combining Blockchain with Cloud, we postulate to develop a secure, efficient and reliable solution to solve the current real-world issues of cloud environment. Thus, this research will be beneficial to advance the existing knowledge about such systems and offer useful ideas and solutions to improve the approach to ensuring the security and reliability of data in the context of cloud computing.

2. Preliminaries and Related Work

2.1. Cloud Computing

This framework known as cloud computing has given a new face to IT domain as it has made computing resources accessible over the World Wide Web on demand. This change in perspective enables business organizations to subcontract infrastructure, platform and software solutions in an attempt to cut costs and also increase the versatility of the organizations' systems. The National Institute of Standards and Technology (NIST) defines cloud computing as the ability to access routers, software, storage, and data centers, as well as processing capacity, over the Internet and on a self-service basis, without discernible distinction between the cloud and other IT resources.

Cloud computing services are generally categorized into three main models: IaaS also known as Hardware as a Service, PaaS also known as Software Stacks as a Service and SaaS also known as Applications on Demand.

Infrastructure as a Service also referred "as Hardware as a Service'' offers hardware resources over the internet. It enables consumers to hire Virtual Machines (VMs), storage necessities, and networks under the consumption model. Some of them include, Amazon Web Services (AWS) EC2 and Microsoft Azure.

Platform as a Service (PaaS) provides the physical devices, computer system and application software over the internet, often ones that are necessary for the applications. The application hardware and software are hosted on PaaS supplier's server infrastructure so that users add application code without having to worry about the base hardware. Such as Google App Engine and AWS Elastic Beanstalk.

SaaS refers to the provisioning of software applications through the internet by payments being on a subscription basis. These applications can be accessed through a web browser, thus there is no need for installation and management on the client's systems. Examples include Google workspace and Microsoft Office 365.

Nevertheless, there are many benefits in using the cloud computing, including the scalability, cost-effective, and accessibility, but again it comes with the problems like, security, privacy and data integrity. Since, Cloud Service Provider's (CSPs) facilities are centralized, they are prone to cyber threat's attempts. In addition, due to the multi-tenant nature of cloud environments it is also a concern to others since there can be privacy and data leakage and compromise, if security and isolation is not properly adhered to.

2.2. Blockchain Technology

Blockchain technology, initially conceptualized as the foundation for Bitcoin, has gained significant attention for its potential to provide secure, decentralized, and tamper-evident records of transactions [2]. A blockchain is a distributed ledger that records transactions across multiple nodes in a network. Each block in the chain contains a list of transactions, and blocks are linked together using cryptographic hashes. This structure ensures that once data is recorded in a block, it cannot be altered retroactively without altering all subsequent blocks, which requires the consensus of the network participants (Example article_asiaccs…,).

Key features of blockchain technology include: Decentralization: Unlike traditional databases that are centralized, blockchain operates on a decentralized network of nodes. Each node maintains a copy of the entire blockchain, and transactions are validated through a consensus mechanism.

Immutability: Data once written to a blockchain cannot be modified or deleted. This impossibility of change is well supported by the use of the cryptographic hashing algorithm and the consensus protocol; thus, making blockchain very resistant to any interference.

Transparency and Traceability: Blockchain records all the transaction that is executed and none of these transactions can be forged since they are all tracked. This transparency is desirable for scenarios that must have an audit and/or accountability trail.

Security: It should be noted that using data in the blockchain structure is protected by cryptographic methods. It can be noted that the actual transactions, are simply digital signatures [3] that are verified by the corresponding private keys, which enables the recording of the valid transactions contained in a block, by a consensus mechanism such as PoW or PoS.

Hence, Blockchain is not only limited to cryptocurrencies, but also other domains such as supply chain, healthcare, financial, and many others. However, it must be noted that blockchain also has limitations like scalability, energy consumption especially when it comes to PoW-based blockchain, and the legal questions.

Integration of Blockchain and Cloud Computing Blockchain with cloud computing is the attempt to unite the benefits of the effective cloud services and high security of blockchain. This is a combination of the two where the blockchain is used to help solve basic security problems of cloud systems since it is decentralized and cannot be altered.

A number of researchers have also attempted to examine the different uses of the integration of blockchain with the cloud computing environment. For example, Yue *et al.* [4] designed the blockchain-based data integrity service framework for cloud storage which could guarantee the customers that data stored in the cloud is safe from alteration. This framework uses blockchain as a database where all data storage and access events are recorded in a tamper-proof ledger with unassailable transparency.

Likewise, Yue *et al.* [4] introduced a privacy preserving blockchain-based approach for the integrity of IoT data and cryptographic technique to protect the data stored in the cloud and allow only specific users. Their approach entails the encryption of data before going to cloud and the use of blockchain for the control of encryption keys and access permission.

However, implementing blockchain with cloud computing has some difficulties as follows. These are the performance overhead because of the extra layer of complexity introduced by blockchain, the problem of

increased size of the blockchain, and the communication between different blockchains and between blockchain and the cloud. Research continues to be conducted in order to solve these problems and design effective, practical, and safe solutions of the cloud blockchain system.

2.3. Related Work

A great number of papers exist in the literature about the integration of blockchain and cloud computing to address issues that are related to protection and confidentiality and design aspects.

Particularly, Zhang *et al.* [5] give a survey on blockchain-based public integrity verification for cloud storage against procrastinating auditors, which helps to understand how to apply blockchain in cloud computing by introducing its merits and demerits.

Another similar study done by Ref. [6] is also concerned with the security and privacy threats in cloud computing and how blockchain solves this problem. The authors offer the description of various types of the blockchain consensus and their connection with the cloud security.

In addition, Peng *et al*. [7] developed a theoretical architecture of integrating the private hybrid cloud and the public blockchain system to improve security and confidentiality of information. They also use both the private and public block; private is used for transaction/buying/selling confirmation and collection of data that are sensitive while the public block is used in a faster manner to deal with data that are not sensitive.

In conclusion, the articles establish that the synergy of blockchain and cloud computing can positively affect data security, privacy, and data authenticity. But it also has some weakness that need to be reduced in order to maximize the chances of implementing the given concept. Thus, keeping with the previous papers which review studies, this paper goes on to from the previous literature to build a new conceptual framework advent of cloud-based blockchain technology with a specific focus on decentralized data management, safe data sharing, and the deployment of dependable access control architectures.

2.4. Applications of Blockchain in Cloud Computing

Thus, from this article, we can conclude that blockchain is wide in many business areas that interact with cloud computing. As applied to the implementation of cloud computing with the help of the blockchain, several crucial issues related to the storage of sensitive information and the level of trust in such data can be addressed.

Data Integrity and Verification: The first and probably the most significant application area of the blockchain in cloud computing is the validation of the data and that data's contents. This characteristic makes blockchain very appropriate in circumstances that demands record generation and protection in a manner that makes it nearly impossible to alter or manipulate them. For instance in the health sector the patient records which are stored in the cloud can be verified and the data that is more sensitive can be certified by blockchain in order to show that it was not altered. By applying this, one will be able to enhance the level of confidence of users in cloud storage systems not forgetting the fact that it would help in preventing sensitive information from interference.

Secure Data Sharing: Cloud system can benefit from the application of block chain since it has the ability to share more than one party data. It is particularly useful in industries such as financial where there is sensitive data that require to be transferred between organizations and without the concern of interferences. Permissions addressing the capability of managing data access can also be issued within smart contracts, which means that access to the necessary data will be possible only after receiving the relevant permission. This capability can improve the use of the organization resources, reduce incidences of data leakage and conform to the legal provisions on data protection.

Decentralized Storage Solutions: Blockchain effectively sets the basis for distributed storage which may be decentralized supplementary to centralized cloud storing. Modern storing systems including the following are of the type that doesn't centralize data; IPFS (InterPlanetary File System), Filecoin, and more. This further opens up data availability and permanence and at the same expands data security. Hence, when the decentralized storage solutions are integrated with the cloud services, the organizations get the benefits from the two concepts.

Supply Chain Management: Based on the findings Blockchain provides good solutions for managing supply chains since it creates end-to-end visibility and traceability. Cloud-based supply chain systems can benefit from the technical features of the blockchain to record all the transactions and the movement of products, so that, all the involved actors have access to one single and authentic record. Some of these are to support minimization of fraud and an optimization of efficiency so that there is an improved trust among the users of the SCM platform.

Identity and Access Management: Blockchain can complement IAM systems in the cloud environment, which can be described as cloud IAM. Old-fashioned IAM systems depend on directories, and these are very much prone to attacks. That is why, IAM systems can have decentralized existence by the usage of blockchain systems, which will make them less vulnerable to various threats. For instance, decentralized identity platforms such as blockchain can enhance and deliver smooth identity services such as identity management, while the users are in possession of their identity without involving a central authority.

Compliance and Auditing: Adherence to the regulations which include GDPR and HIPAA are a major issue when working with cloud services [8]. By using smart contracts, many compliance can be attained through blockchain where the smart contract and all the compliance information will be visible for audits. This automation can also eliminate the overload in relating with the organizations and make sure they are in compliance at all times.

2.5. Challenges in Integrating Blockchain with Cloud Computing

As evident from the above-discussed areas, there are opportunities that can be accrued from a harmonized blockchain and cloud computing environment; however, there are issues that need to be solved to support the efficient integration of both solutions.

Scalability: Different types of blocks in decentralized systems, especially the ones utilising the PoW protocol, may experience the problem with scalability. In relation to the number of transactions, it can be said that as the number of transactions increases the time to complete the transaction and their complexity in terms of computational requirements also grows. This limitation can prejudicially affect the functioning of cloud-based applications that utilize blockchain for carrying out transactions. Challenges like these are that blockchain-based solutions need to scale, and the majority of existing implementations lack both horizontal and vertical scalability; sharding, layer 2 solutions, and other consensus algorithm approaches (for example, Proof of Stake).

Performance Overhead: At the same time, the implementation of blockchain with cloud computing may add complexity of extra work load when performing consensus and cryptographic solutions. This overhead which is incurred by users can affect the response time as well as the bandwidth of applications hosted in the cloud. The adjustment of blockchain activity performance and the reduction of its influence to the general work of the system is critical for achieving a real-world and efficient integration.

Interoperability: This implies that there must be compatibility between blockchain platforms and the conventional cloud services to enhance the integration process. Each of the blockchain platforms may have their own protocols, standards and API, which adds to the level of integration complexity. Despite the numerous use cases and applications of blockchain cloud integration, there are limitations in the

communication interfaces, which demands standard interfaces/protocol between blockchain and cloud to occur, to ensure compatibility and effective interaction between the two systems.

Regulatory and Compliance Issues: The legal framework of the blockchain technology is rather new as the governments and countries are yet to come up with an appropriate regulatory measures. Adhering to such regulations while applying blockchain together with the cloud can sometimes be risky. Some examples of dynamic compliance drivers include new laws and rules that are constantly being drafted and enacted which organizations have to follow to ensure that the systems they implement do not offer shortcuts to breaking them while at the same time fulfilling their purpose and providing security.

Energy Consumption: The consensus algorithms, especially the PoW, are associated with very high-power consumption by blockchain networks. An issue that is gaining importance concerning blockchain operations is the environmental effect, as organizations cut down on emissions. The consensus algorithms efficient in terms of energy consumption and the optimization of the energy consumption of blockchain activities are vital for the effective integration with the Cloud computing.

Security Risks: Although blockchain improves security in many aspects, its security has its own risks. There is a risk of what is called 51% attacks where one party is able to gain control of the majority of say, hashing power, of a given blockchain. Also, there are weaknesses that can be traced in the code of smart contracts that are developed and implemented to address certain transactions. To minimize the risks it is necessary to have strong security measures and regularly audit the system and processes.

2.6. Future Research Directions

Therefore, the combined use of blockchain and cloud computing is a growing research area with many opportunities for advancement. Some potential research directions include the below possible areas of research: Optimizing Blockchain Performance: Researches on New consensus models including the POS, POA and combined models are perusing to provide solution to scalability and performance issues. Similarly, other factors, such as the type of network, an option to shard, and applying off-chain transactions, enhance the outcomes of the blockchain.

Enhancing Interoperability: This indicates that there are ways through which one could plan for the accomplishment of the various goal and objectives that include the following, The development of consistent etiquette and schematic for the blockchain-cloud can assist in integration. More analysis and innovation in communication and the connectivity of different domains of blockchain, the different entities in the platform of blockchain can be connected hence enhancing the proficiency of blockchain.

Privacy-Preserving Techniques: To ensure privacy it means that blockchain-cloud system must employ the ideas like zero-knowledge-proof, homomorphic encryption and etc., These techniques can help to process and verify the data and at the same time do not reveal the information.

Energy-Efficient Blockchain: Studying prospects for energy-efficient consensus mechanisms as well as further research on the efficient energy utilization of the activities linked to the blockchain are important to avoid problems with sustainable integration into the application of cloud computing. Researches being carried out around the world on the kinds of energy that are relatively renewable and available for use in the management of blockchain, and also the refining of the hardware that is used in the management of a blockchain will go a long way in mitigating the negative effects.

Decentralized Applications (DApps): Thus, it can be stated that the emergence of new possibilities and business models based on the analysis of the autonomy of blockchain and the scalability and efficiency of cloud for Building D Apps can be obtained. It would also be useful to study how to deal with architectures of DApps, for the main point, as it was already mentioned, DApp applications might benefit users, and their introduction is rather essential for the most part.

Security Enhancements: Additional investigations on higher tiers of security, for example, of smart contracts themselves, and of secure multi-party computations will enhance the quality of the security of the Blockchain-Cloud systems. Thus, efforts like building the proper procedures for putting in practice a safe solution minimizes the threat level.

3. Proposed Framework

3.1. Design Principles

In the headings of advancing cloud computing security, the combination of blockchain technology and cloud computing seeks to build on each other's strength to mitigate the insecurity that is innate to cloud settings. There are several axioms the proposed framework is built with to meet the requirements of efficient and scalable security. These are decentralization, non-adjustability through modification, openness, safe exchange of data, and self-executing rules.

Decentralization: Hence, the framework decentralizes the aspects of data management by storing data in multiple nodes in a blockchain network. The fact of decentralization excludes the possibility of hacking and modification of the data by individuals or groups of individuals.

Immutability: As a result, by using the property of blockchain in which data can be recorded but not edited or removed, the framework guarantees the integrity of data. This property affords a solid means of ensuring the credibility of collected and processed data.

Transparency: Since all the transactions and data changes take place on the blockchain, it is easy to track any activity that occurs on the business's database. This openness increases the degree of responsibility from members and it simplifies the validation process of data authenticity.

Secure Data Sharing: The framework uses various cryptographic methods to ensure that information that is exchanged between users is and applications is safe. Data security measures that are put in place entails that data shall not be accessed by unauthorized personnel.

Automated Governance: Smart contracts are employed for the intelligent management and compliance with the data governance task as well. These smart contracts automatically execute rules and conditions, guaranteeing compliance with the regulations and the company's policies when dealing with data.

3.2. System Architecture

The following are the main elements of the given framework that have contributed towards the formation of a more secure cloud data storage solution that is also more efficient and at the same time scalable. The system architecture includes the following components.

3.1.1. Blockchain network

The core of the proposed framework is defined in the blockchain network within which the transactions and changes to any data are registered in a secure and distributed environment. The nodes are many and each of them has the complete chain showing the state of the blockchain. The Consensus algorithm like, PoS or PBFT helps in reaching a consensus on the state of the blockchain between all the nodes.

3.1.1.1. Cloud infrastructure

The core and the support services of the cloud are used in this case to deliver the computational and storage resources required by the framework. It comprises VMs, storage service, and networking components. The cloud services are employed for hosting nodes of the blockchain and storing the encrypted information. CSPs provide on-demand virtualized resources, which are self-service and elastic in that they can be used to achieve different levels of usage.

3.1.1.2. Integration layer

The integration layer functions as a connector between the block chain network and cloud structure

where the message of each layer is interchanged. It is used for encrypting and decrypting the information, it is used to control data storage and requested items, and it is also aimed at providing communication between clouds services and blockchain systems. It is also responsible for smart contract's transaction and the application of access control rules.

3.1.1.3. Data management module

The data management module entails the methods and protocols for storing, accessing, and distributing data in an efficient manner within the computational framework laid down. It is responsible for encrypting data before storing it in the cloud and also keeps a record of the reference between encrypted data and the entries in the Blockchain. To specialized and secure processes of storing the data, it is only revealed to the authorized people within the module.

3.1.1.4. Access control module

Anti-abortion activists claim that women seeking abortions are irresponsible and contrast it to cases where women go through strict undersea training to become divers. It employs the principles of cryptography when determining the level of authorization of a certain user. To regulate the access rights, the module interacts with the blockchain to authenticate the users and filter the access according to the smart contracts specifications.

3.1.1.5. Smart contracts

Smart contracts are contractual obligations which are automated hence when the contractual terms are coded, they run on their own. They adapt and govern data and compliance processes by running predefined rules or conditions. They are employed for the regulation of access rights to data, data sharing, and satisfaction of compliance specifications.

3.1.2. Data flow

The specific processes with regards data within the proposed framework include creation, storage, access, and verification. To achieve appropriate data protection, at the same time, data authenticity, and accessibility, throughout the given procedure, one must follow specific guidelines.

3.1.2.1. Data creation and encryption

As and when a user creates or uploads his data, the data management module incorporates a secure algorithm to encrypt the data. The encrypted data is then distributed to the cloud environment of the solution. An entry is made in the blockchain with the metadata and the hash of the encrypted data in it. This entry justifies the data's existence and credibility as an on-going documentary record.

3.1.2.2. Data storage

It means that the encrypted data is placed to the cloud infrastructure interacting with the scalable storage resources of the CSP. The cloud storage service also guarantee the data accessibility and the actual data permanency. The integration layer is responsible for handling the storage operations and it keeps the relation of encrypted data to the entry in the blockchain.

3.1.2.3. Data access and decryption

Another step is the actual checking of a user who wants to obtain the access to the data by access control module. And if the user is authorized the module for managing the data gets the data from the cloud storage encrypted and decrypts it. A user, in turn, receives the decrypted data as the result of the procedure described above. Every input and output access request and alike operation occur on the blockchain and are recorded as such.

3.1.2.4. Data sharing

There is a secure way of sharing data between the users and the applications through the framework. Smart contracts are employed to set out and execute the conditions pertaining to the sharing of data, as well as the extent to and the manner in which data sharing can be done. During a Data sharing request, the access control module checks on the conditions and permissions that have been hard coded in the smart

contract. If those conditions are fulfilled, the data management module enables the communication of encrypted data safely.

3.1.2.5. Data verification

Based on this strategy, the users can compare the hash of the data obtained with the hash stored on the blockchain. In this case, if hashes are matching, therefore it assures that data is intact and has not been interfered. This verification process helps to made sure that the data is still reliable and still have its original form.

3.1.3. Security and privacy

To minimize the risk of accessing private/protected/sensitive data by unauthorized personnel, and other security/privacy concerns, the proposed framework of reference embraces numerous security/privacy layers. These measures include:

3.1.3.1. Encryption

Data is converted into a format that secured by using the most effective encryption algorithms then stored in the cloud. This ensures that irrespective of who gets to analyze it, the data will still be in a form that can hardly be read and is safe. The framework is also good on the management of the encryption keys where they are safeguarded to avoid access by unauthorized personnel.

3.1.3.2. Access control

The access control module limits the manner in which data can be accessed to the fact that only certain users can be allowed to access certain data as per the set security measures. The techniques commonly employed are used to authenticate the user and control their level of access. Regarding access control, smart contracts self-execute the rules of access functions hence enforcing access control policies in the usage of data.

3.1.3.3. Immutability

The concept of the blockchain makes it impossible to tweak or erase data that has been written into it without the approval of a consensus of the participants in the network. This property offers a reliable means by which the trustworthiness of data can effectively be achieved.

3.1.3.4. Transparency and auditability

Any form of data access and modifying operation is done and recorded into the blockchain database, allowing transparency. This increases accountability and makes it very easy to check the accuracy of the claims that are being made.

3.1.3.5. Secure Data sharing

Smart contracts act as the terms for the exchange of data in the agreed-upon manner and in a secure and authorized manner in this case. The integration layer also ensures that passing on of data is secure through encryption and encourages the privacy of the clients.

3.1.4. Proposed implementation and experimental results

In this paper, the proposed framework must be adopted through integrating blockchain and cloud. The process turns into the creation of the blockchain network, the installation of the cloud environment and building of the integration layer and modules.

3.1.4.1. Blockchain network setup

A blockchain network is created on an appropriate blockchain environment that can be Ethereum or Hyperledger Fabric. Nodes run on many cloud instances to make them dispersed and backup. The consensus mechanism is set to make sure the transaction throughput and data verification is well made.

3.1.4.2. Cloud infrastructure deployment

The cloud infrastructure is set-up from services which are offered by a cloud service providers, whether it be Amazon Web Services or Microsoft Azure among others. The virtual machines, the storage services, and the networking components are set up to host the blockchain nodes and to store the encrypted data.

The general architecture of the underlying structure is able to grow in a tightly coupled manner to the requirements of the workloads assigned.

3.1.4.3. Integration layer development

Integration layer is formed to provide a clear interface between the blockchain network as well as the cloud environment. Components such as data encryption/decryption, storage management, and smart contract using this system are also incorporated. The structure of APIs and interfaces is used for interaction with the blockchain and cloud facilities.

3.1.4.4. Module implementation

The data management and access control modules are used to store and control access to the data and the data operations. This is due to the fact that the operating system relies on cryptographic mechanisms to protect the data and also in the administration of the permissions. Smart contracts are created to work on the data management that is carried out in accordance with the set provisions.

3.1.4.5. Experimental setup

The implemented framework must be examined in a number of experiments with regard to its functionality, security and performance as well as the number of users. Some of the parameters of experimentations include; stressing the framework on various workloads and analysing the outcome in terms of recovery time, number of operations per unit time, and other relevant cost such as amount of resource consumed. Validation of Security Enforcement is aimed at the assessment of encryption, access control and data integrity methods.

3.1.4.6. Results and analysis

The findings from the experiments will prove that the proposed framework achieves consistent enhancements to the data safety and security compared to regular cloud storages.

Blockchain technology improves the credibility of the data and makes it transparent and trustworthy, smart contracts, on the other hand, makes data management and compliance with the governing rules automated. Measures of productivity reveal that the framework is capable of processing large numbers of data and several transactions without straining resources and system's productivity.

Overall, with the proposed framework incorporate the advantages of blockchain and cloud computing to support the storage of the data securely, intelligently and with high credibility. Through implementing the framework that minimizes the drawbacks of cloudy environments, it introduces higher levels of data security, as well as accuracy and confidentiality; thus, it became significant for various organizations of various industries. The paper also proposes the detailed design, implementation, and experimental analysis of the proposed framework to outline the future possible uses.

4. Security and Privacy

The symbiosis of blockchain with the cloud computing concept adds the following benefits in terms of security and privacy [9]. However, it also arises some specific issues that have to be solved to maximize the benefits of both the technologies. This section presents the analysis of the security and privacy threats and their solutions to protect the confidentiality, integrity, and availability of data within the proposed framework.

4.1. Security Concerns

4.1.1. Data breaches and unauthorized access

Security is a top consideration in cloud computing because in situations where a business places data in the cloud service, leakage of this data can have extreme implications that include: loss and compromise of reputation, and legal liability. This is a factor that the above developed framework targets to address by

applying the highest levels of encryption to the information during storage as well as during transit. The information that is sent to a cloud is encrypted using secure and very efficient ways of cryptography so that even if an intruder wish to have a look at the materials, he/she will not have the ability to decipher them. Others are elements of the access control mechanisms that are built on blockchain technology and similarly enhance the security of the stored data in that only those who are supposed to have access to the certain given data can have access to it. Smart contracts assist in the implementation of the access control policies and therefore seal the security layer.

4.1.2. Data integrity and tampering

Information data accuracy may be regarded as the contingency and, thus, to ensure the implementation of system integrity, it is essential to increase accuracy. Current cloud back up techniques are vulnerable to the changes of the data either by third party interferences, or mishaps whereby one corrects the other person mistake. The properties of the blockchain technology are immutable, and that is why it is a solution to this kind of issue. The users who add data in the blockchain cannot tamper with or delete the same without the permission of other users of the specific distributed network. This characteristic Also, it preserves data in transit from alteration because to change a record in any block, all succeeding blocks need to be changed, which is practically inexistent. As the idea of blockchain, it explains how the users of the framework can develop the proof of one or multiple data's integrities and track the records to verify the alterations made by the third parties.

4.1.3. Distributed Denial of Service (DDoS) attacks

Cyber threats and risks that affect internet-based businesses include Distributed Denial of Service (DDoS) Attacks.

While DDoS attacks are direct in nature and target cloud services, the particularity is to send a high number of requests that the system cannot handle, thus denying the services to users. Due to the distributed architecture of blockchain systems, there is improvement against the threat of DDoS attacks as no node/cluster can be said to be central. In the proposed framework, data is distributed in various nodes so that even if the attackers decide to go ahead and offer a certain node a very big traffic to block the system, they cannot do it. Yet in this type of attack, metrics like PoS or, PBFT provide ample coverage as this means that, regardless of syndrome nodes within the network, the consensus instrument can still work, and the network carries on to have consensus.

4.2. Privacy Issues

4.2.1. Data privacy and confidentiality

Preservation of data privacy and data confidentiality is another major concern with reference to clouds. Employers must believe that their information or records are not disclosed to other unauthorized personnel. This issue is considered in the proposed framework by applying end to end encryption on data passed and stored in the system. The data is protected by a cryptographic method before it is stored in the cloud while access keys are stored in a blockchain. This makes sure that only the personnel with the right decryption keys is able to unlock the data and thus freedom from exposure. Also, smart contracts enable the organization of the access control policies that guarantee data privacy by regulating permissions for accessing data based on the set rules.

4.2.2. Anonymity and pseudonymity

In some of the cases like in banking and fiscal operations, or in the case of medical records, user identification is important in ensuring privacy is upheld. Pseudonymity is facilitated in blockchain as the user only needs to engage the system using keys and not actual personal details. This feature is incorporated into the proposed framework to ensure that users' identity is either anonymous or

pseudonymous as the situation may warrant. For instance, in a healthcare system, the patient can conveniently forward his/her electronic medical records with the use of pseudonyms; thus, enhancing the privacy of the patient while at the same time the patient shares his/her records with the healthcare providers.

4.2.3. Data ownership and control

It's undefined to share the information with unauthorized individuals once the data is stored in the third-party server, one of the emerging problems with cloud computing. Because users entrust data to cloud service providers for storage and protection, issues related to ownership, and control of such data arise. The above work calls for improved data management to enable the users to have better control through decentralization. The ownership of data can be unalterably kept and controlled by the owner with the help of blockchain technology that offers the proofs of ownership. Other novel applications of Blockchain technology include data usage policies where smart contracts are created to dictate how data can be accessed and used by others in compliance with the owner's wish. This brings the power of control of data back to the users even when it is stored in the cloud.

4.3. Mitigation Strategies

4.3.1. Encryption

Encryption is one of the most commonly used methods of data security and can be regarded as the basic level of protection. Through integrating the proposed framework, the use of high encryption algorithms in keeping data secure when stored and when in transit is observed. In case of storage of data in the cloud, data is encrypted, while the encryption keys are managed through the use of block chain. Further, end-toend encryption also implies that data gets protected from the time it is generated, stored and even while it gets retrieved.

4.3.2. Access control

Security controls particularly for access and modes of access are necessary to control the access of a particular data by various people. With reference to the proposed framework, the privacy and access control are secured by a blockchain based system that gives strict security policies. Smart contracts contain access rules, which determines who can access information and under what circumstances. Automation of the access control policies eliminates the chances of intrusion and makes certain that only those who are permitted to access a given data will do so.

4.3.3. Immutability and transparency

The intrinsic feature of the blockchain structure can effectively offer means for preserving and enhancing the data authenticity and openness. Basically, once a data set is written to the block chain, it cannot be changed or removed without the consent of the block chain participants. This immutability helps to make the data reliable and provable always. Furthermore, all the data and changes to the data sets are stored in the transaction to append the transparency of the records. The above transparency also serves to boost or increase the level of accountability as well as the audibility of data verity.

4.3.4. Decentralization

Decentralization is one of the main recommendations towards the improvement of the security and reliability of the proposed framework. With the concept of data fragmentation across nodes of the framework, there is no isolated point that is vulnerable to be attacked by malicious structures such as DDoS. The distributed structure of the blockchain network serves as an advantage in this case to guarantee that the system will still continue to run despite the malicious nodes or the cyber-attacks.

4.3.5. Smart contracts

Smart contracts can also be used to automate the aspects that are related to data management and compliance. These smart contracts execute themselves based on the set parameters and are used to

monitor and standardize the compliance of data management with the laid down rules and regulations. Smart contracts also handle access control of policies, data sharing, and other security aspects with great security and transparency.

4.4. Experimental Evaluation

In order to evaluate how the proposed framework can help solve the identified security and privacy problems, a set of experiments must be performed. With reference to the experimental evaluation, the main concentrations should be the efficacy, security, and adaptability of the framework under different circumstances.

4.4.1. Experimental setup

The actual experimental factor is to implement the above-mentioned proposed framework on the cloud platform of an established cloud computing services supplier. While the blockchain nodes are hosted on virtual machines the storage services are set to encrypt the data. The integration layer, data management module, and access control module should be developed and tested with the data from the real application.

4.4.2. Performance metrics

Other quantitative measures like the latency, the throughput as well as the resource usage must be taken to compare as well as quantify the efficiency and the scalability

of the framework that was implemented. To cover these aspects, the workloads that are used in the experiments should include different to determine how the system would perform given different usage patterns.

4.4.3. Security tests

Simple security tests are performed to assess the framework's defenses against data leakage, corruption, and invitations. Such tests involve testing the ability to attempt to read encrypted data that they have no rights to read, to try and modify the blocks in the blockchain and also to perform DDOS attacks on the actual system. As for these threats to security, the response of the framework must be determined and quantized.

4.4.4. Results and analysis

Based on the proposed experimental results, we will be able to ascertain that the concepts elaborated in the paper's framework offer much better security and privacy than that offered by innovative cloud storage systems. The encryption procedures confer confidentiality to data because the data cannot be easily accessed by unauthorized parties and, in addition to that the block chain property of data prevents modification or deletion of information. The proposed framework decentralized processes will make the system more resistant to DDoS attacks, and because of smart contracts, access control and data handling will become more efficient. Performance measures will also show that the framework is capable to assimilate large volumes of data and transactions with relative overhead making it sustainable and adaptable to large organizations.

The subsequent framework proposed adopts the properties of the blockchain and cloud computing to meet these peculiar issues that affect cloud environments. Using the incorporation of encryption, decentralization of data, and auto-governance, the framework becomes an effective, efficient, and reliable means of data storage. The results of the proposed experimental assessment of the framework will prove its capability to provide data security against violations, modifications, and leaks with high performance and scalability.

5. Implementation of Security

The described solution of the proposed framework is to combine the blockchain technology with cloud

computing, accordingly the key benefits are as follows. This section describes the procedures to be followed and the outcome of the assessment of the framework accompanied by the configuration details and application structure of the experiment.

5.1. Implementation Details

Some of the components of the implementation include the blockchain network, the cloud architecture, integration layer, data management component, access control component, and smart contracts [10]. All the components are used with an aim of making the security, privacy and performance of the system efficient.

5.1.1. Blockchain network

The deployment of the blockchain network is done with Ethereum as a popular platform that excels in smart contract execution. Ethereum create a Decentralised environment where Transactions or changes of data are — recorded on the Blockchain. In this architecture, various nodes that exist in the Ethereum network are actually hosted on virtual machines which exist on the cloud environment. These nodes take part in the consensus process so that they can validate transaction and at the same time contribute to making of blockchain.

5.1.2. Cloud infrastructure

The cloud infrastructure is provisioned through the Amazon Web Services without which it is hard to get good cloud services. AWS provides elasticity and available services to host the nodes such as EC2 instances, and blockchains are stored with efficiently encrypted data S3. Availability and reliability of the system is provided by the cloud infrastructure.

5.1.3. Integration layer

The integration layer has a mediator role and ensures synergy between blockchain network and the cloud structure. Encryption and decryption of data, and storage management is performed by it besides providing the interface to interface with both cloud and block chain services. The integration layer is developed using Node. js is a preferred runtime environment used to create large-scale network applications.

5.1.4. Data management module

It is the data management module that handles issues to do with the encryption of data the moment the data is to be stored and deciphering of data the moment it is to be retrieved. AES with the key of 256 bits is used for protection of data, which guarantees the security of data. It also keeps track of the association of the encrypted data and the entry in the blockchain to provide data security.

5.1.5. Access control module

The access control module is used to make sure that only certain people can come across certain pieces of information. It has the functionality of public key distribution for the authorization of the clients. The access control rules are automatically implemented or enforced through smart contract in Ethereum block chain that makes the data access conform to predefined policies [11].

5.1.6. Smart contracts

Smart contracts are digital contracts in the form of code that executes itself whereby the obligations of the contract are coded. In this framework, smart contracts deal with data access rights, data sharing agreements and ensure compliance to the law. These are developed in Solidity, a language based on the Ethereum Virtual Machine for deploying smart contracts.

5.2. Experimental Setup

The practical aspect involves deploying the implemented framework to into an environment in the AWS

cloud environment as well as testing it through a number of tests that intends to determine its efficiency, security and scalability. The tests for the evaluation of operational efficiency should be conducted under the conditions which are as close to real life as possible.

5.2.1. Deployment

Blockchain Nodes: Ethereum nodes which are also known as clients can be hosted on AWS EC2 instances and this can be done using instances that have different parameters in order to assess the performance.

Data Storage: encrypt the data and it is then loaded into an S3 bucket in AWS so as to act as an archive for the data while at the same time serving as a readily available source of it.

Integration Layer: The middle layer that is included for system integration is implemented at AWS Lambda so that serverless computing can take place.

5.2.2. Test scenarios

Performance Testing: This may entail evaluating system response time and the business's throughput of work per unit of time while measuring the consumption of available resources at different levels of load.

Security Testing: This assesses the global performance of the encryption schemes, the access measures, and the integrity of the data. Sims: Such as IT unauthorized, data tampering and DoS attacks.

Scalability Testing: Determines the ability of the systems to handle large volumes of the load where the load may refer to such things as; large volume of data or many transactions.

5.2.3. Metrics

Latency: Processing time required to authenticate and verify the transactions carried out through the blockchain system.

Throughput: Hearths per second, directly showing the efficiency of a certain payment system.

Resource Utilization: During operation the parameters such as CPU usage, memory usage, and the network usage is important.

Security Incidents: Newspaper data: number of attacks that were successful and failed.

Scalability: Application of the aspects to systematic measures, such as how it performs under different data volumes and user requests.

5.3. Results and Analysis

The results of experiments will help in understanding the effectiveness, protection and expandability of the proposed framework. The evaluation of these outcomes will prove that a combination of blockchain with cloud computing enhances the idea of secure data storage.

5.3.1. Performance evaluation

Latency: The average latencies of processing the transactions in the blockchain must be within the acceptable limit of most of the applications. Because of the Ethereum PoS consensus mechanism, the latencies will be lower as compared to PoW.

Throughput: It is possible to understand a high concentration of transactions per second. This performance is for application with moderate to high transaction rates.

Resource Utilization: Available resources must be effectively consumed with the CPU and the memory usage being within the required levels. AWS Lambda must be used to implement the integration layer where by scaling has automatic capability to accommodate likely high traffic without degrading the system's performance.

5.3.2. Security evaluation

Encryption Effectiveness: AES-256 encryption proves to be reliable for data protection, which meant that all attempts to enter are unauthorized are returned as incomprehensible. As mentioned earlier, the decryption will be nil where the right keys were not used.

Access Control: The measures that ensuring permissions will work properly, which is based on the

blockchain technology. Smart contracts effectively implement the access control policies to keep the unauthorized peoples away from the data.

Data Integrity: In the blockchain structure, data remains secure because the records could not be altered; no one attempts to change data throughout the study period. Any modification made on the data will be easily recorded on the hub or the blockchain as noticed by the researchers.

5.3.3. Scalability evaluation

Handling Increased Workloads: It will prove that the system is expansible to accommodate large volumes of data and high transaction volumes without degrading performance. AWS offered the anytime, anywhere scalability for blockchain, which brought about strong scalability grant.

Automatic Scaling: AWS Lambda, the integration layer will be scale-able, and the system is capable of scaling up when a massive load will be applied to it without requiring human interference.

5.3.4. Comparative analysis

Static comparison of the proposed framework with the traditional security solutions to the cloud storage is made to bring out its benefits. It should be seen that by incorporating the concept of blockchain security and data integrity will be increased dramatically, at the same time the overall performance will not differ much. Previous solutions in this paradigm did not incorporate the decentralized and immutability characteristics of the blockchain which rendered them insecure and open to vandalism.

5.3.5. Use case scenarios

It is proposed to consider several use case scenarios to show how the identified framework can be used in practice. These scenarios are health information exchange for patient care, payments and other financial transactions in banking, and supply chain management. In each case, the framework offers better security, privacy, and trust; thus, it could be concluded that it is suitable for practical implementation.

5.4. Discussion

It can be said that the introduction of the proposed framework enhances the degree of data security and privacy over the cloud. In this way, the corresponding meaningful security features are initiated that are associated with unauthorized access, corrupt data, and DDoS attack within the framework. The employment of smart contract in an organization impacts the automation of data governance and compliance for the management of data in the organization in as much as it regards the legal requisites of the institution.

5.4.1. Strengths

Enhanced Security: Hence, the data placed in the cloud storage are offered adequate protection, provided they are backed with the encryption, access control, and data unchangeability of the blockchain system.

Scalability: Scalability of the concept enables the framework to cope up with the enlarging loads of work or tasks which could have an impact on the efficiency of the framework.

Transparency: The structure of the system and the method of record-keeping used in the blockchain makes the system more responsible and trust worthy.

5.4.2. Limitations

Performance Overhead: In integration of the system with the help of the blockchain, one of the concerns that is experienced is the one which relates to the performance overhead which particularly affects the time which is taken in completing a transaction. However, this overhead is justified by the gain acquired through the reinforcement of security in data operations.

Complexity: The introduction and management of blockchain system might be complex since this require adequate knowledge in managing block chain systems. This is still an issue and narrowing down the deployment and management procedures may help in this regard.

5.4.3. Future work

The future works are to enhance the performance of the blockchain network, to study the heuristic algorithms for incorporating the cloud-computing with the blockchain framework, and to incorporate more features of privacy protection in the mentioned framework. Furthermore, the discussions like how one can extend the presented framework with even more consensus algorithms, or how the researcher can identify energy-efficient blockchain techniques are not irrelevant.

Thus, due to the framework suggested, successful integration of BCT with CC is maintained for a secure, sustainable, and efficient system for data storage is realized.

The peremptoriness of the proposed experimental assessment in relation to serious security and privacy threats is investigated in this research work to establish the importance of the instrument for organizations that are interested in enhancing their strategies in data handling on cloud.

6. Conclusion

In conclusion, applying blockchain technology in the cloud computing environment is a promising strategy in tackling some of the most critical issues in data protection and confidentiality. Hence, this paper has proposed a framework that aligns itself with the capabilities of both technologies for cloud-based data storage; a solution that is secure, scalable, and effective. The principles of encryption, disintegration of data through decentralization and automated management through smart contracts considerably reduce hacking risks, data forgery, and DDoS attacks. The case study therefore shows that the proposed framework can indeed improve data confidentiality and privacy and at the same time achieve high performance and scalability.

This proposed system makes it possible to prevent unauthorized access to data placed in the cloud and proves the correct data storage by using the features of a blockchain. The integration of smart contracts for controlling and regulating access to resources and handling compliance requirements also contributes to security by configuring the rights of data access and sharing. Also, the decentralization of the blockchain network increases system security by not allowing the enemy to target specific critical points within the system, thus allowing uninterrupted operations in any unfavorable circumstances.

However, the usage of blockchain technology in the context of the cloud environment enhances performance overhead and complicates the system design. The future research directions that should be addressed further are the improvement of throughput for the blockchain activities, the integration of blockchain platforms with the cloud services, and the use of more environmentally friendly consensus algorithms. Moreover, it will be essential to study the privacy preservation methods and the standard practices of the integration of blockchain and cloud environments to improve the prospects of using such a converged system.

In sum, this research does expand the existing literature on the CBBSs and unveils the useful insights and feasible solutions that can be employed to improve the performance of data protection and assurance. The elements proposed in this paper seem to be rather promising and can be easily scaled for other industries, including healthcare, finance, supply chain, and many others. Since the importance of security and reliability of the data management systems is constantly increasing, the development of the use of blockchain and cloud computing has a very high potential to fundamentally change the existing framework of data management in the context of contemporary digital landscape.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Govindaiah Simuni conducted the research; Avinash Reddy Kandlakunta analyzed the data; both authors had approved the final version.

References

[1] J. Wang, J. Chen, and X. Li, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.
[2] S. Nakamoto. (2008). Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[3] F. Zhang, R. S. Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," *Public Key Cryptography*, vol. 2947, pp. 277–290, 2021.
[4] D. Yue, R. Li, Y. Zhang, W. Tian, and Y. Huang, "Blockchain-based verification framework for data integrity in edge cloud storage," *Journal of Parallel and Distributed Computing*, vol. 146, pp. 1–14, 2020.
[5] Y. Zhang, C. Xu, X. Lin, and X. Xuemin, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," *IEEE Transactions on Cloud Computing*, vol. 9, no. 3, pp. 923–937, 2021.
[6] C. Chen, S. Lee, and P. Wang, "Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation," *IEEE Transactions on Reliability*, vol. 64, no. 3, pp. 840–851, 2021.
[7] C. Peng, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Journal of Future Generation Computer Systems*, vol. 102, pp. 902–911, 2020.
[8] H. Shafagh, L. Burkhalter, M. H. Grossmann, and W. J. Huber, "Towards blockchain-based auditing of cloud service providers," *IEEE Transactions on Cloud Computing*, 2020.
[9] H. Zhang, Z. Zang, and B. Muthu, "Knowledge-based systems for blockchain-based cognitive cloud computing model for security purposes," *International Journal of Modeling and Simulation in Science and Computing*, 2241002, 2021.
[10] L. Ismail, H. Materwala, and A. Hennebelle, "A scoping review of integrated Blockchain-Cloud (BcC) architecture for healthcare: Applications, challenges and solutions," *Sensors*, vol. 21, no. 3753, 2021.
[11] A. Lakhan, M. Mohammed, A. Rashid, S. Kadry, T. Panityakul, K. Abdulkareem, and O. Thinnukool, "Smart-contract aware ethereum and client-fog-cloud healthcare system," *Sensors*, vol. 21, no. 4093, 2021.