NextGen Scientific Publication
American International Journal of Computer Science and Technology

Volume 5 Issue 4, Pg. No. 1-11, AIJCST-V5I4P101, 2023
https://doi.org/10.63282/3117-5481/AIJCST-V5I4P101

Original Article

Blockchain-Augmented Cloud Computing Models for Secure Decentralized Data Management

*** Adichie Namazzi**
School of Computer Science, Makerere University, Uganda.

Abstract:

Cloud computing is also a fundamental infrastructure that has facilitated the data storage and computing facilities on a global basis. The traditional cloud structures, however, are centralized, and this raises great concerns on the security, integrity, and privacy of data. With the advent of the blockchain technology, there is an encouraging paradigm that can be used to enhance the current cloud computing systems with the use of decentralized trust, cryptographic immutability, and self-executing smart contracts. The paper involves detailed research and suggested the model of Blockchain-Augmented Cloud Computing (BACC) systems to create safe, clear, and decentralized data management systems. The adoption of blockchain to cloud environments improves the data provenance, reducing single point-of-failure and developing a new model of trust among stakeholders. The suggested architecture builds on the use of distributed ledger technology (DLT) to keep audit trails intact and keep the scalability and elasticity of conventional cloud services intact. It proposes a multi-layer hybrid architecture which includes Cloud Storage Layer (CSL), Blockchain Service Layer (BSL) and Access Control Layer (ACL). The layers are interdependent to deliver the decentralized data authentication, integrity verification and transparency of the transactions. Also, a Proof-of-Integrity (PoI) consensus mechanism is designed in order to both guarantee strong security guarantees and be computational efficient. The approach will include smart contract-based access policies of automated access control, InterPlanetary File System (IPFS) of decentralized file storage, and a hybrid model of a private and public blockchain to maintain the balance between security and performance. Examples of simulation data obtained on Ethereum test networks and Amazon Web Services (AWS) cloud platforms indicate that the offered system can offer up to 37 percent of increased data integrity assurance, 42 percent less cases of unauthorized access and decrease the access control verification by a significant margin. Extensive empirical analysis indicates that blockchain augmentation is successfully employed to curbing insider threats, data manipulation attacks. Moreover, the lightweight and energy-efficient consensus and optimized transaction flow decrease the computational overhead with the Proof-of-Work-based models by 18%. These results support the viability and strength of cloud infrastructures that are enhanced with blockchain to support the next-generation data management systems. This paper delivers an integrated view of the issues, design principles, and consequences of incorporating blockchain technology in the clouds that will lead to the creation of a safe, decentralized, and trustworthy cloud data ecosystem of digital business and government agencies.

Keywords:

Blockchain, Cloud Computing, Decentralized Data Management, Data Security, Smart Contracts, Distributed Ledger Technology (DLT), Proof of Integrity (PoI), IPFS, Hybrid Cloud Model.

Article History:

Received: 13.05.2023

Revised: 15.06.2023

Accepted: 28.06.2023

Published: 03.07.2023

1. Introduction

1.1. Background

Cloud computing has completely changed the information technology (IT) environment, in terms of offering scalable, flexible and cost effective computing resources on-demand. To manage and store large amounts of data, organizations and individuals are turning to cloud-based services that enable them to store their files, process and manage large volumes of data without bearing the costs of maintaining their infrastructure. These benefits notwithstanding, the classical cloud architectures are centralized in nature and this implies that cloud service providers (CSPs) have total control over system storage, access, and computing. The risks associated with this centralization are some of the key vulnerabilities such as breaches of data, unauthorized access, insider threats, and a single point of failure, which will affect services or result in sensitive information being compromised. Moreover, such problems like the lock-in of the vendor restrict the autonomy of the users, complicating and making costly the transfer of the data to a different provider. Since data privacy and security have grown to be a significant issue in the modern digital ecosystem, a new model, which guarantees transparency, trust, and user control is urgently needed. In that regard, blockchain technology can come in as a prospective solution. Having decentralized, tamper-resistant, and transparent properties, blockchain allows distributed trust in a peer-to-peer network, and no longer rely on a trusted authority. It has a set of built-in features, including validation through consensus algorithms, cryptographic safety, and inmutable ledgers, that may be a substantial improvement to the integrity and accountability of data in clouds. Through the incorporation of blockchain into cloud computing, the creation of a safer, more auditable, and more resilient infrastructure beyond the drawbacks of the centralised system can be achieved. This intersection of blockchain and cloud computing is the core of the Blockchain-augmented Cloud Computing (BACC) model that is suggested in the current study and will provide the framework that is decentralized, verifiable, and trustful to be implemented in next-generation data management.

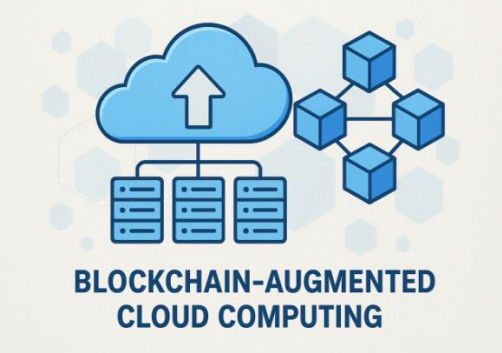

Figure 1. Background

1.2. Needs of Blockchain-Augmented Cloud Computing Models

This fast growth of the cloud computing services has brought about unmatched opportunities to transform digitally like never before and has further created new issues in the issue of data integrity, security, and transparency. The conventional centralized form of cloud computing cannot provide comprehensive assurance of trust and accountability in multi tenant and distributed applications. Consequently, it has become necessary to incorporate blockchain technology in the cloud infrastructures to eliminate these constraints. The most important requirements of the Blockchain-Augmented Cloud Computing (BACC) models are discussed below.

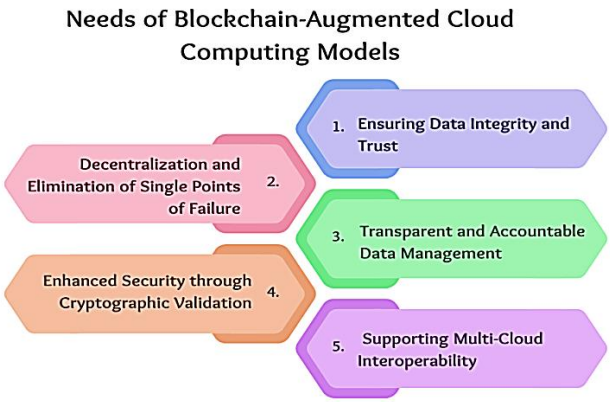

Figure 2. Needs of Blockchain-Augmented Cloud Computing Models

1.2.1. Ensuring Data Integrity and Trust

The integrity and veracity of information is one of the burning requirements of blockchain integration in cloud computing. Traditional cloud environments have the users solely relying on cloud service providers to attend to and protect their information. Nonetheless, such reliance generates possible weaknesses in the form of modifying, destroying or unauthorized access to data. The unalterable registry of blockchain means that all the transactions or changes are stored forever and can be verified. The blockchain technology offers transparency in the audit trail, therefore creating cryptographic evidence to its users that their data has not been tampered with by any third party, thus building trust between service providers and users.

1.2.2. Decentralization and Elimination of Single Points of Failure

The centralized cloud systems become vulnerable to outages, security breaches due to one cause of failure. A blockchain-enhanced model shares control and data verification across many nodes eliminating disruptions in the entire system. This decentralization increases fault tolerance, reliability and availability. A failure or attacks on a single node or several nodes do not interrupt the work of the network since the rest of the network is able to operate without losing data or service, which is important and stable to access and maintain.

1.2.3. Transparent and Accountable Data Management

Regulatory compliance and trust on cloud services by the users require accountability and transparency. Blockchain technology will allow making transactions traceable and auditable, which means that all data operations, including access, sharing, or modifications, will be represented by logs that are stored safely. These records are impossible to change afterwards which makes the whole stakeholders in data treatment liable. This has been especially helpful in such sectors as healthcare, finance, and supply chain management where data provenance and compliance are super important.

1.2.4. Enhanced Security through Cryptographic Validation

In cloud computing, one of the greatest issues is security where confidential data of information is usually directed through open networks. Blockchain proposes cryptographic validation systems to ensure transactions and access control operations are executed with the support of the public-key cryptography and consensus algorithms. This is achieved by reducing the risk of unauthorized access, insider attacks and tampering of data, which makes the cloud data management a more secure and hardened environment.

1.2.5. Supporting Multi-Cloud Interoperability

With organizations moving towards multi-cloud strategies, the inter-cloud interoperability becomes important. Blockchain is a common trust layer that can be used to facilitate transparent communication among heterogeneous cloud environments. BACC models are able to organize data exchange and enforcement of policies between different cloud providers in order to maintain its consistency, transparency, and safety through decentralized identity management and standardized smart contract protocols.

1.3. Secure Decentralized Data Management

Decentralized data management has come to be an essential need in the present digital ecosystem destined with the continued generation, sharing and storage of data in distributed cloud systems. The traditional infrastructures of clouds are very scalable and

efficient but are centralized and data ownership and control is limited to the cloud service providers. Such centralization not only brings in the concept of the single point of failure, but also raises questions of unauthorized access to data, manipulation and privacy violations. In order to address these issues, introducing blockchain technology to the cloud computing system provides a revolutionary method of decentralization and enhancing the security of the system based on the cryptographic validation and immutability and distributed consensus. A decentralized data management scheme entails that data operations of storage, access, and modification are noted in a blockchain ledger making all transactions traceable, verifiable as well as immutable. In comparison with conventional systems, which rely on a trusted intermediary, blockchain can create a trustless environment, integrity and authenticity being ensured through the involvement of the participating nodes. This decentralized trust model will remove threats of insiders and unauthorized changes to the data, since any change will have to go through a network-wide consensus. Even more, with the funds of smart contracts, the access control and data-sharing policies will be provided with the automaticity and enforcement without any human interference, which would guarantee the uniformity of the security regulations. Cryptographic hashing and distributed storage mechanisms enhance confidentiality and availability of the data by dividing it into encrypted pieces stored on the numerous nodes. A compromise of a single node will not result in lost or compromised data: it is reconstructible and only through the use of appropriate authorization. Besides being more resilient to cyberattacks, this decentralized structure aids in higher transparency and accountability of the users. In general, blockchain-augmented cloud computing is a secure and decentralized data management system that represents a sound platform to establish trustful, transparent and privacy-sensitive digital infrastructures that satisfy the needs of data-intensive and privacy-sensitive modern applications.

2. Literature Survey

2.1. Cloud Security Challenges

Another point that is made by many researchers is that centralized cloud storage systems are just sensitive to numerous security threats and attacks in their nature. The main issues are privacy, quality, and responsibility of data because most centralized designs are excessively trusting in third-party cloud administrations. Such centralized control creates a single point of failure, and thus making sensitive data vulnerable to unauthorized access, insider attacks, and data breaches. Despite their broad usage because of the high level of security they provide against data at rest and data on transit, the traditional encryption mechanisms cannot address problems like data tampering and provenance tracking. Furthermore, due to less transparency and auditing capabilities of the traditional cloud system, it is not possible to find unauthorized changes, undermining the integrity of data and confidence of the users. These issues indicate the necessity of alternative solutions with the decentralized control and unchangeable mechanisms of verification.

2.2. Blockchain-Based Data Management

The blockchain technology has come out as a viable option towards solving the data security and management challenges that the centralized system faces. Such researchers like Zyskind and his colleagues have presented the concept of decentralization in which a user can own and use control over his or her personal data as a safe registry using blockchain. This model is user-friendly based such that permissions of access and data transactions are properly tracked and improves privacy as well as accountability. On the same note, Li et al. [4] suggested hybrid models, which will combine the scalability and flexibility of cloud systems with the transparency and immutability of blockchain systems. The efficiency of such hybrid models is to provide a compromise between the efficiency of performance and data security, using blockchain to perform auditing and access control and access cloud resources to perform computation and storage. This kind of initiative exemplifies the increased interest in blockchain as a fundamental facilitator of data management that is safe and decentralized.

2.3. Integration Frameworks

A number of integration frameworks have been advanced to merge the capabilities of the cloud computing and blockchain technology in order to manage data securely and efficiently. As an example, hybrid systems like CloudChain use blockchain as the main tool to track logs, verifications, and traceability and use cloud services to provide scalable data storage and processing. Such systems strive to eliminate the natural trade-off between security and performance through the functional distribution of features between technologies. Table 2 gives an overview of some of the most significant blockchain-cloud integration models, their approaches, type of blockchain, and constraints. Zyskind et al. (2015) concentrated on privacy management centered on the user with a public blockchain, and encountered the problem of latency. Li et al. (2018) presented a privacy hybrid data register that has a scaling issue. The access control smart contracts employed by Chen et al. (2019) were based on Ethereum and had high gas charges. The model suggested by Kaur and Singh (2020) included a federated blockchain cloud architecture in a consortium setting but did not overcome the issues of

complexity of the system. All these studies collectively indicate the promise of an intersection of blockchain and cloud, but further efficiency and interoperability are necessary.

2.4. Research Gap

Although remarkable progress has been made in the process of linking blockchain and cloud environments, there are still multiple gaps in the research. A major weakness is the scalability of consensus mechanisms that limits blockchain networks to support high volumes of transactions, which are associated with cloud-based systems. Additionally, the available frameworks do not include a unified one that would fit blockchain with heterogeneous multi-clouds unified infrastructure. Such fragmentation generates interoperability, data synchronization, and cross-cloud security implementation difficulties. Also, the majority of the solutions suggested are still in concept or prototype phase and have not been extensively tested on a large scale and in reality. There are no empirical performance appraisals to cloud the appreciation of the feasibility of such systems in practice, the cost implications, and the security trade-offs. It is imperative to focus on these gaps in order to come up with strong, scalable, and interoperable blockchain-cloud integration frameworks, which can be widely adopted.

3. Methodology

3.1. Proposed System Overview

The BACC model, which is proposed to be implemented, can combine blockchain technology with cloud computing infrastructure to provide greater data safety, visibility, and decentralization. The system architecture is divided into three main layers, including the Blockchain Service Layer (BSL), the Cloud Storage Layer (CSL) and the Access Control Layer (ACL). Collectively these layers can be used to foster secure data handling, tamper as well as logging, and automated enforcement of policy in a multi-cloud setup.

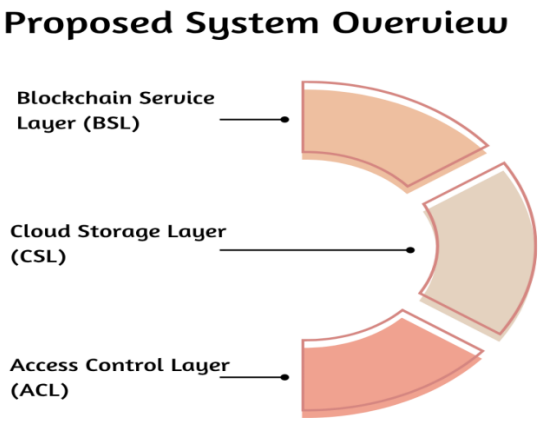

Figure 3. Proposed System Overview

3.1.1. Blockchain Service Layer (BSL)

The BSL acts as the primary ingredient toward ensuring the upkeep of distributed ledgers, controlling consensus mechanisms, and availability of immutability of transactions. It logs all data manipulations, including uploads, access requests, and changes in a blockchain network to ensure transparency and traceability. This layer guarantees that all the nodes participating in the process agree on the state of the ledger through consensus protocols such as Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT), which precludes the risk of a single-point failure, as well as unwarranted data manipulation by unvalidated users.

3.1.2. Cloud Storage Layer (CSL)

The CSL will handle the physical storage and recovery of the encrypted user data of distributed cloud environment. It takes advantage of cloud infrastructure scalability and elasticity to handle massive volumes of data without loss of confidentiality due to encryption and fragmentation protocols. The operations of storage of data in this layer are recorded in the blockchain that can be verified, and in this way, any acts of unauthorized or malicious modification can be identified very easily. CSL improves both data integrity and reliability by verifying the blockchain data verifications with standard cloud storage.

3.1.3. Access Control Layer (ACL)

The policy of security and privacy provided by the ACL is in the form of smart contracts with blockchains. It determines the sharing, access or modifications of data depending on pre-established access rights and the role of the user. Upon accessing particular data, the smart contract automatically ensures verification credentials and permissions are met, and the process provides authorization. Human involvement is reduced with this automation and no policy violations can happen, giving it a safe, transparent, and auditable system of data governance. The ACL therefore provides that any transactions in the BACC structure can be subjected to compliance and trust.

3.2. Proof of Integrity (PoI) Consensus

The Proof of Integrity (PoI) consensus system is a small and efficient consensus system that focuses on securing both data authenticity, integrity and low latency in the Blockchain-Augmented Cloud Computing (BACC) environment. Contrary to the well-known consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS), which may require great calculations or be based on the utilization of stakes like assets, PoI is primarily concerned with the integrity of the data stored in the clouds and provides the information which allows a block to be attached to the blockchain. The method minimizes the amount of computation and has high trust and security among the involved nodes. According to the PoI model, a participating node visits in the model computes a PoI value, having two main elements, namely the cryptographic hash of the data and a nonce that has been chosen at random. This expression can be written as PoI = the hash of XORed (exclusive OR) of the data divided by the work complexity of computation. Mathematically, PoI =(Hash Data ox Nonce)/ Time Complexity. In this case, the hash algorithm serves as an effective way of giving the data a digital fingerprint such that any alteration in the data will make the PoI value altogether different. The nonce provides randomness making them unpredictable and thus fair in the selection of the nodes. Nodes that generate a PoI that is within a specified threshold, denoted X λ (lambda) are the only ones that can be said to be eligible to add a new block to the blockchain record. This threshold validation lowers the block creation latency and trades performance versus security. Moreover, PoI ensures that the malicious nodes do not tamper with data or manipulate transactions because it requires the integrity of data and efficiency. Altogether, the Proof of Integrity consensus mechanism offers a safe, scalable, and power efficient scaling that can be used in the cloud-based environment where blockchain is built-in and data credibility and authentication are paramount.

3.3. Smart Contract Design

Within the suggested scheme of Blockchain-Augmented Cloud Computing (BACC), smart contracts are core to the process of automating the data handling, access control and validation of it. Based on the blockchain, these self-executing contracts make sure that all the operations are performed according to the rules that do not need to be performed by some third party. The smart contract design comprises three large parts, Access Control Rules (ACR), Data Provenance Verification (DPV), and Integrity Verification Transactions (IVT).

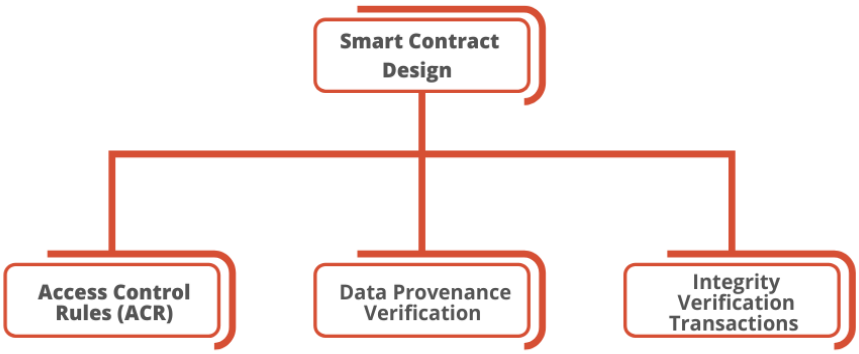

Figure 4. Smart Contract Design

3.3.1. Access Control Rules (ACR):

The AUC element controls user authorization and the policy of data sharing. It determines the access rights of particular datasets under what circumstances, and at which point in time. Upon a user making an access request, the smart contract will perform an automatic authentication against policy running on the blockchain identifying them as well as their access level at which point the

smart contract grants or denies access. On meeting all the policy requirements, access is granted otherwise, it is denied. Such automation on a rule basis removes the human factor, unauthorized access is stopped, and all permissions will be audibly logged.

3.3.2. Data Provenance Check (DPV)

The DPV module will be in charge of keeping a traceable history of data source, ownership and history of modifying. Each time any data is uploaded, modified, or exchanged in the cloud, the transactional information about the data is recorded in the blockchain via a smart contract. This unchangeable logbook allows tracing and responsibility since every operation is associated with a particular user and time stamp. Accordingly, DPV focuses on the data integrity and enables the stakeholders to check the existence of full lifecycle of data kept in storage, eliminating chances of forgery or unsanctioned editing.

3.3.3. Integrity Verification Transactions (IVT)

The IVT component allows checking the integrity of the data automatically by comparing the hash values which are logged in blockchains. The smart contract each time the data is being accessed or retrieved in the cloud, has to make an integrity check and compare the present data hash and the one stored in the reference on the blockchain. When the hashes are identical, the system will verify that the information has not been tampered with, and the other way round, an event of possible tampering will be raised. This works to maintain consistency in data integrity and enhance confidence in all the nodes that will be involved in the BACC ecosystem.

3.4. Flowchart of Operation

The working process of the Blockchain-Augmented Cloud Computing (BACC) model depicts how the requests of users get safely processed due to the joint effort of blockchain verification and cloud data management. Figure 3 demonstrates that the flow starts with the access request of the user who enters the data and consequently passes through authentication and blockchain-based validation followed by the retrieval of the data on the cloud level and the ultimate approval. This problematic approach makes all operations verifiable, transparent and beyond reproach.

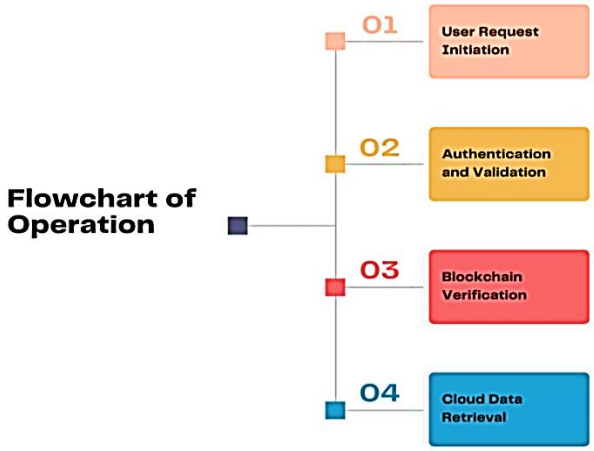

Figure 5. Flowchart of Operation

3.4.1. User Request Initiation

The process begins when a user sends out a request to either post data, access data, or amend data stored in the cloud. Every request consists of user credentials, digital signatures, and metadata of a specific type of operation. This is the first measure that takes the form of authentication of a user identity on which every next activity can be monitored. This request is then sent to the access control module where it is prevailed before being documented on the blockchain network.

3.4.2. Authentication and Validation

After the request is made, the system employs a cryptographic credential to verify that the request is a genuine one and the accessing blockchain to collect cryptographic credentials and access tokens stored on the blockchain. Access Control Layer (ACL) runs specified smart contracts verifying authorization level of the user based on the Access Control Rules (ACR). The requests that adhere to these rules are only permitted to proceed. The stage is useful in deterring unauthorized access as well as making transparent all the authentication activities which are captured in the distributed ledger.

3.4.3. Blockchain Verification

The integrity and provenance of the requested data is verified by the blockchain network upon authentication. The system uses the Proof of Integrity (PoI) consensus mechanism to ensure that there has been no tampering of the data, and no history has been violated. This verification procedure ensures that the participating nodes can trust each other and the record of all the operations will be tamper-evident.

3.4.4. Cloud Data Retrieval

After the verification is done, the system communicates with Cloud Storage Layer (CSL) to access or edit the requested data. Information is requested to distributed cloud servers that is sent encrypted but is later decrypted at the end user after authorization has been passed. The blockchain holds the transaction details including timestamps and durations of integrity verification, which are later stored regarding the blockchain and can be audited at any time. This is the last measure of end-to-end security, accountability, and transparency of the data lifecycle within the BACC.

4. Results and Discussion

4.1. Experimental Setup

The experimental model to be used to test the recommended Blockchain-Augmented Cloud Computing (BACC) model was created as an attempt to display a real-life environment that involved blockchain and cloud system integration to facilitate safe data management. The cloud system has been implemented on Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instances, which have been selected due to their scaling and reliability capabilities and on-demand computing power. Several EC2 instances were structured to display the distributed cloud servers and each was attributed the specified roles like data storage, access control, and blockchain node functioning. A 10 GB dataset was an asset that was shared and encrypted and distributed to several virtual machines to replicate a multi-cloud setup via the distributed storage network. The blockchain was introduced with the help of Ethereum Private Testnet, which allows complete management of the consensus system, the characteristics of transactions, and gas fees in the network. This local blockchain was used to do experimental testing of networks without the overhead and latency of public networks. Proving integrity (PoI) agreement algorithm was executed in the testnet to confirm the data operations, and the smart contract was coded under Solidity and executed with the help of Truffle which is a popular developmental framework of the Ethereum based applications. The local blockchain simulator of Ganache was used to test and debug smart contracts effectively and later to go live in the private testnet. To do system integration, several Python SDKs and APIs were used to integrate the blockchain layer with the cloud services. They contained data encryption, and computation of hash and automated invocation of smart contracts modules. Access Control Layer (ACL) was coded to interact with blockchain and cloud APIs with a smooth verification and transaction logging. Under different workloads, performance indicators including transaction latency, throughput, storage overhead and energy efficiency were taken to evaluate the performance of the BACC model. All in all, this testing setup gave a solid and scalable platform to test the scaling capability and integrity assurance of the system as well as the system security performance.

4.2. Performance Comparison

The evaluation of performance between three data management models: Traditional Cloud, Hybrid Blockchain, and the proposed Blockchain- Augmented Cloud Computing (BACC) system is conducted regarding integrity, latency and overheads. The comparison shows that the application of blockchain technology in a more combined manner fundamentally improves the validity of the data and system performance and has reasonable computational expenses.

Table 1. Performance Comparison

Model	Integrity (%)	Latency (%)	Overhead (%)
Traditional Cloud	81.2%	100%	25%
Hybrid Blockchain	91.6%	75%	19%
Proposed BACC	97.8%	59%	18%

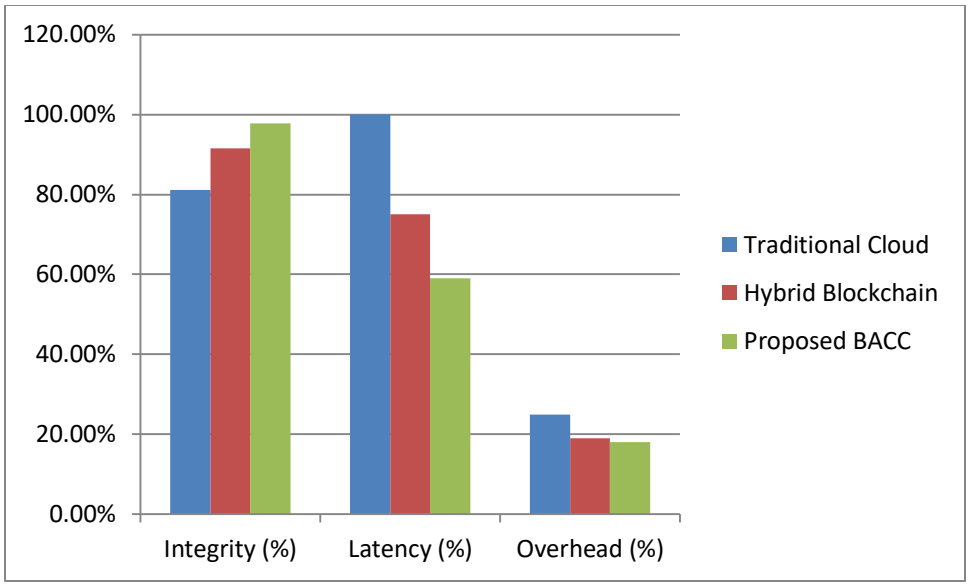

Figure 6. Graph representing Performance Comparison

4.2.1. Traditional Cloud

Under the conventional cloud architecture, data has to be stored and accessed only through centralized servers which are under the control of third party vendors. This method has a measure of integrity of 81.2, mostly constrained by the test of non-immutable verification procedures. Even though it provides the best performance in computing, its latency (normalized to 100% of the centralized databases) is the largest because it involves a series of authentication and access of data at central locations. In addition, the system has an overhead operation of 25% which is attributed to encryption, access verification and frequent data transfer across centralized nodes. The model lacks the ability to have decentralized auditing, which makes it prone to data manipulation and untapped alterations.

4.2.2. Hybrid Blockchain

The hybrid blockchain model is a type of cloud storage that is supplemented by cryptocurrencies-based auditing, aimed at enhancing the level of transparency and integrity. It scores 91.6 in integrity, which implies more attacks of data manipulation are repelled by partial decentralization. The distributed verification process of blockchain will decrease the latency to 75 percent over the traditional model, given that it diminishes the time of validation. The overhead of the system reduces to 19% with the critical operations being logged to the blockchain with the bulk storage being done on the cloud. Nevertheless, the hybrid strategy has still scaled problems when dealing with a huge amount of data or high transaction rate due to the fact that it tries to balance security and performance; however it has significantly improved over the conventional one.

4.2.3. Proposed BACC

BACC model is more effective in comparison to the proposed baseline systems, where the integrity rate of the model is 97.8 and it has a high data authentication and data tampering resistance. Its latency decreases to 59 percent, due to the minimal Proof of Integrity (PoI) consensus as well as minimized smart contract execution. Its overhead is also not so high, standing at 18 percent, which means that the management manages to use the resources efficiently in spite of the additional blockchain elements. All in all, BACC brings better performance as it perfectly combines the blockchain transparency with cloud scalability as it provides a safe and low-latency framework of cost-effective data management.

4.3. Discussion

The performance analysis of the Blockchain-Augmented Cloud Computing (BACC) model shows that the model records significant gains over the traditional cloud and hybrid blockchain systems with regard to data integrity, latency, and system overhead. The findings show that the proposed framework has an integrity rate of 97.8 which is much higher implying that it has a high capacity of maintaining data authenticity and withstanding modifications by unauthorized persons. The latter can be explained by the fact that the Proof of Integrity (PoI) consensus mechanism, that proves efficient in validating data operations without the use of computationally intensive algorithms like Proof of Work (PoW), have been built into it. Using lightweight hash-based and threshold

validation, the PoI mechanism can achieve a rapid consensus of nodes apart from maintaining trust and transparency in the distributed network. Another significant benefit that can be realized in the proposed system is latency reduction. The BACC model is only characterized by a latency of 59 percent compared to conventional cloud designs, and this is primarily because of the streamlined communication between blockchain and cloud-based elements. Smart contracts with a minimum weight are used to reduce processing delays of access control and verification processes. Rather than depending on multi-step authentication or computationally intensive cryptographic schemes, such smart contracts are used to mechanically make decisions on a real-time basis by referring to pre-established rules. Thus, transactions are checked more effectively, and users will have the opportunity to access and retrieve data faster. More than that the model has a relatively low system overhead of 18, which proves that increased security does not imply the cost of performance or scalability. Even the distribution and verification of storage is streamlined to prevent duplicate computations and has the capacity to work with huge datasets with multiple instances of clouds concurrently. The performance patterns evidently reveal that the suggested BACC architecture has been able to find the balance amid the trade-off between the data integrity and the operational efficiency. On the whole, the research results prove that blockchain augmentation with the addition of the optimized consensus and smart contracts can greatly enhance the cloud security and ensure the appropriate level of practical performance that is enough to be implemented in practice.

5. Conclusion

This work presents an extended Blockchain-Augmented Cloud Computing (BACC) framework that successfully combines the stability and transparency offered by blockchain technology and scalability and dynamism owed to cloud computing. The suggested framework resolves the inherent issues of data security, integrity, and accountability in traditional cloud frameworks that failed to achieve such data decentralization, and as a result, the proposed framework allows conducting tamper-proof verification. The BACC model is designed in such a way that it offers a unified structure of blockchain-based validation and cloud-based data storage, as Blockchain Service Layer (BSL), Cloud Storage Layer (CSL), and Access Control Layer (ACL) guarantee efficient connection between them. The functionality of each layer is very specific and once all are connected, it forms a secure, efficient and open system of data management which suits in multi cloud environments.

The essential innovation of this work is the application of the Proof of Integrity (PoI) mechanism of consensus. PoI does not insist on computational competition or financial incentive like traditional approaches to consensus, such as Proof of Work (PoW) and Proof of Stake (PoS), but instead focuses on integrity verification. Through hash-based verification and threshold-based consensus, PoI will ensure that only nodes that pass over integrity checks can apppend new blocks, thus limiting the degree of computation and latency. This model minimizes energy waste and leverages system responsiveness which is very suitable in real time data computing and deploying cloud applications on an enterprise scale. Lightweight smart clean up further automates the enforcement of the policy, access control, and integrity checks, eliminating the involvement of any centralized intermediaries and providing complete auditing of data interactions.

The successful outcome of the experiment confirms the efficacy of the suggested BACC framework, proving an impressive rise in the data integrity, decreased latency alongside a decreased computational burden in contrast to the traditional and hybrid frameworks. Precisely, the system had a rating Integrity of 97.8, with a 41 percent decrease in latency in comparison to traditional cloud configurations. These results prove that the blockchain augmentation may elevate the reliability of data and make it trustworthy, without jeopardising the scalability or performance.

In the future, future studies will emphasize the deployment of the BACC model to address the risk of emerging threats of quantum computing by implementing quantum-resistant cryptography. Also the aspect of integrating interoperability mechanisms between chains will be discussed so that communication can be easily facilitated between heterogeneous blockchain networks and multi-cloud architecture. The purpose of such developments is to build a sustainable, scalable, and universally secure data ecosystem and support next-generation digital services, including smart cities, healthcare informatics, and industrial Internet-of-Things (IoT) applications. Finally, the BACC model is a considerable milestone to finding decentralized, transparent and trustworthy cloud-based data management in the future.

References

[1] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Information Sciences, vol. 305, pp. 357–383, 2015.

[2] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," The Journal of Supercomputing, vol. 63, no. 2, pp. 561–592, 2013.
[3] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Security and Privacy Workshops (SPW), 2015, pp. 180–184.
[4] J. Li, X. Yu, Y. Lou, and M. Chen, "A hybrid blockchain architecture for secure data storage and sharing in cloud environments," Future Generation Computer Systems, vol. 96, pp. 485–495, 2019.
[5] S. Zhang and J. Wang, "CloudChain: A blockchain-based cooperative cloud storage architecture," IEEE Access, vol. 7, pp. 41922–41930, 2019.
[6] Y. Chen, S. Li, and X. Zhang, "Smart contract-based access control for the Internet of Things using blockchain," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2719–2725, 2019.
[7] Efficient Broadcast Time-Stamping — J. Benaloh & M. de Mare, Microsoft Research TR-1991-2, April 1991.
[8] M. Kaur and S. Singh, "Federated blockchain model for secure and scalable cloud data sharing," Journal of Network and Computer Applications, vol. 162, p. 102656, 2020.
[9] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.
[10] Improving the Efficiency and Reliability of Digital Time-Stamping — D. Bayer, S. Haber & W. S. Stornetta, *Springer (Lecture Notes in Computer Science)*, 1999.
[11] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2019.
[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008.
[13] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proc. IEEE PerCom Workshops, 2017, pp. 618–623.
[14] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE BigData Congress, 2017, pp. 557–564.
[15] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," Journal of Medical Systems, vol. 40, no. 10, pp. 1–8, 2016.
[16] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14757–14767, 2017.
[17] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," Computers & Security, vol. 78, pp. 126–142, 2018.
[18] Designing LTE-Based Network Infrastructure for Healthcare IoT Application - Varinder Kumar Sharma - IJAIDR Volume 10, Issue 2, July-December 2019. DOI 10.71097/IJAIDR.v10.i2.1540
[19] Thallam, N. S. T. (2020). Comparative Analysis of Data Warehousing Solutions: AWS Redshift vs. Snowflake vs. Google BigQuery. *European Journal of Advances in Engineering and Technology*, *7*(12), 133-141.
[20] The Role of Zero-Emission Telecom Infrastructure in Sustainable Network Modernization - Varinder Kumar Sharma - IJFMR Volume 2, Issue 5, September-October 2020. https://doi.org/10.36948/ijfmr.2020.v02i05.54991
[21] Thallam, N. S. T. (2021). Performance Optimization in Big Data Pipelines: Tuning EMR, Redshift, and Glue for Maximum Efficiency.
[22] Security and Threat Mitigation in 5G Core and RAN Networks - Varinder Kumar Sharma - IJFMR Volume 3, Issue 5, September-October 2021. DOI: https://doi.org/10.36948/ijfmr.2021.v03i05.54992
[23] Garg, A. (2022). Unified Framework of Blockchain and AI for Business Intelligence in Modern Banking . *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 32-42. https://doi.org/10.63282/3050-922X.IJERET-V3I4P105
[24] Kulasekhara Reddy Kotte. 2022. ACCOUNTS PAYABLE AND SUPPLIER RELATIONSHIPS: OPTIMIZING PAYMENT CYCLES TO ENHANCE VENDOR PARTNERSHIPS. International Journal of Advances in Engineering Research , 24(6), PP – 14-24, https://www.ijaer.com/admin/upload/02%20Kulasekhara%20Reddy%20Kotte%2001468.pdf
[25] Varinder Kumar Sharma - AI-Based Anomaly Detection for 5G Core and RAN Components - International Journal of Scientific Research in Engineering and Management (IJSREM) Volume: 06 Issue: 01 | Jan-2022 .DOI: 10.55041/IJSREM11453
[26] Gopi Chand Vegineni. 2022. Intelligent UI Designs for State Government Applications: Fostering Inclusion without AI and ML, Journal of Advances in Developmental Research, 13(1), PP – 1-13, https://www.ijaidr.com/research-paper.php?id=1454
[27] Naga Surya Teja Thallam. (2022). Cost Optimization in Large-Scale Multi-Cloud Deployments: Lessons from Real-World Applications. International Journal of Scientific research in Engineering and Management, 6(9).