Enhancing the Performance and Data Security of Blockchain Technology for Cloud Computing

Poonam Kumari[1] , Meeta Singh[2]
Pnmdv211@gmail.com, meeta.sangwan@gmail.com
Department of Computer Science and Engineering, Manav Rachna International Institute of Research and Studies,
Faridabad, Haryana, India.

Abstract
Today's fastest-growing IT technology is cloud computing, which is gaining popularity due to its adaptability and user-friendly characteristics. Cloud computing can decrease pay-per-use costs, which also boosts scalability. In cloud computing, any requested resource or service, such as software, hardware, or infrastructure, will be made available. The main issue with cloud computing is data security because the data will be held by a third party and will be readily available online. Since the consumer has limited control over the data, several security risks may occur as a result of its invisibility. As a result, cloud security is required to guarantee the security of user data on the cloud. Utilizing cloud services from a cloud provider who guarantees the security of your data is crucial. The majority of articles focus on creating cloud storage that is safe enough for sensitive information. The Internet of Things (IoT) is now used in a variety of ways to simplify people's lives. The Internet of Things generates enormous amounts of data that need to be processed and stored on the cloud. Data stored on the Blockchain is secure from prying eyes since it is a distributed ledger. Any computational node with internet access can join or establish a peer network, increasing the effectiveness with which resources are employed. Every machine in a peer-to-peer, decentralized network that uses blockchain has its own database. According to our current study, a system's security may be increased by implementing robust data encryption, privacy safeguards, access restrictions, and identity management processes. These measures will secure sensitive data and prevent unauthorized access.

Keywords: Blockchain, Cloud Computing, Privacy, Data Security, Authentication.

1. Introduction

Currently, the "Cloud" is a prominent topic of discussion. People often use the metaphorical term "Cloud" to refer to cloud computing rather than a specific location [1]. Declaring that future apps will stay on the cloud at this time is appropriate. Cloud computing solutions are being used more frequently to meet the demands of several company programmers and clients [2] [43]. Only two examples of cloud service providers are Dell EMC and Amazon since they are regarded as being more economical and technologically sophisticated than conventional data centres [3][4]. However, security is the most pervasive of all of its drawbacks, making it distinct from other storage methods. When business data is moved to the cloud, the cloud provider also takes up data security.

Increased data exposure and overlapping trust boundaries may provide malicious cloud users greater opportunities to exploit IT systems and steal or alter corporate data. To overcome this cloud security issue, a "Distributed Cloud Model" based on blockchain technology can be used [5]. Blockchain technology has attracted a lot of interest because it provides new, secure, and cost-effective choices for storing ever-increasing data sets. Blockchain, which was initially built for the virtual currency Bitcoin [6], eliminates the need for reliable third parties. Additionally, Blockchain data is dispersed across several sites. By doing this, a peer-to-peer network is established that is trackable, auditable, and exceedingly challenging for hackers to compromise [7], [42].

1.1 Traditional cloud storage model

Traditional cloud storage architecture may use a client or mobile device as the front-end platform. The back-end platform is a server or storage; the network might be the internet or an intranet. Google Drive is one such instance of a standard cloud service. All of the files you submit are kept in a safe Google data center [8]. A user can request access to the data from the data center via a computer or mobile device.

Operations in large data centers are expensive. The technology in these data centers has to be upgraded often. There are also operational costs for cooling, maintenance, and upgrades. Safety is still another factor [9].

Despite the strict security precautions that many cloud providers have in place, it is possible that they could be breached and sensitive data will be accessed. The most recent celebrity cloud breach was one such incident [10] various from human error, there are various privacy threats [11]. Large corporations can search non-encrypted files. The many circumstances in which they may legitimately access and share the data are outlined in their privacy regulations [12].

1.2 Cloud computing attributes

The few key characteristics employed in cloud computing is as follows:

1. Multiple tenancies

Sharing resources is multi-tenancy. Because many organizations share data in the cloud with other organizations, multiple tenures are crucial in cloud computing.

2. Exceptional scalability

In the context of cloud computing, massive scalability refers to the power to scale up bandwidth and storage as well as thousands of systems.

3. Flexibility

Depending on their needs, users can scale up and down resources fast thanks to cloud service providers.

4. Buy a Use

Users may only pay for the resources they really use, and frequently they rent resources so they only have to pay for the time they actually utilize them.

5. Providing resources in advance

The user has previously organized the system and the additional resource by providing them in advance.

1.3 Cloud Computing Deployment Model:

Figure 1 depicts a three-part cloud deployment strategy that is dependent on factors including storage capacity, ownership of the infrastructure, and accessibility. The decision on the deployment strategy is heavily influenced by two key factors:

1) who is in charge of the infrastructure, and 2) where it is situated.

There are three different kinds of deployment models:

i. Private Cloud

Only employees of the organization have access to certain systems and services. Third parties may also be managed by it. Users can store data in the cloud using a secure private key under this paradigm, preventing data hacking from the public cloud [15]. Users do not share the resources they purchase with other organizations; they buy them for their own organization. Only those who can be trusted utilize it. Microsoft, VMware, and Ubuntu, for instance.

ii. Public Cloud

In a public cloud, the cloud service providers share the resources openly, or across several organizations. To the numerous users, it offers real cloud hosting and services. Some examples of public clouds include Google, Amazon, and Microsoft. It is offered by a supplier for a fee [13][58].

iii. Hybrid Cloud

Public and private clouds, as well as community and private clouds, can be combined to create a hybrid cloud. We refer to it as a hybrid cloud. Data is protected and takes advantage of the secure application in a hybrid cloud. The combination of two cloud models is what hybrid clouds generally use, as shown in Figure 1.

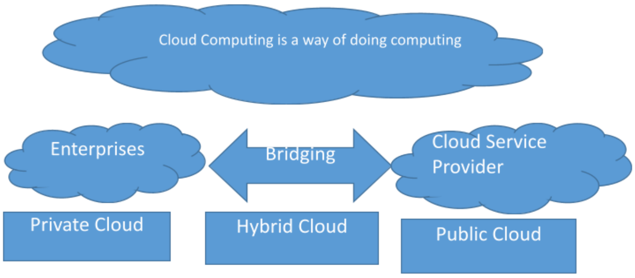

Figure 1: Cloud computing deployment model.

1.4 Service Cloud

A broad group of Internet-based services that may be easily accessible by anybody, anywhere in the world, is referred to as "cloud services". These services might save time and money because they don't require any specialized equipment or software to function. Throughout the workday, most employees often utilize cloud services for activities like checking email and collaborating on documents.

The cloud [14] computing vendor or service provider alone is responsible for managing cloud services. Businesses may simply point their consumers to the servers of the service providers instead of having to host apps on their own servers.

1.5. Security and Algorithm

1.5.1. Cloud Security

The practices and policies used to safeguard data, apps, and infrastructure in cloud computing environments are referred to as cloud security [16]. The security of cloud resources is essential as companies and consumers depend more on them for storage, processing power, and application hosting.

i. Following are some crucial elements of cloud security:

ii. Data encryption: Data encryption guarantees that data remains incomprehensible even if it is intercepted or viewed by unauthorized parties. Most cloud service providers offer encryption solutions for both data in transit and at rest.

iii. Access controls: To restrict access to cloud resources, strong access controls are crucial. In order to do this, it is necessary to use robust authentication techniques, such as multi-factor authentication (MFA), and stringent identity and access management (IAM) regulations in order to provide the proper rights [17][59].

iv. Network security: To secure the cloud infrastructure from unauthorized access and assaults, cloud providers frequently include built-in network security mechanisms, such as firewalls, intrusion detection systems, and virtual private networks (VPNs).

v. Patches and upgrades are often released by cloud providers for their systems' security. To safeguard against known vulnerabilities, it's critical to keep these patches up to date.

vi. Secure APIs: Application Programming Interfaces (APIs) make it possible for various cloud services to interact and communicate with one another. For these APIs to remain secure and guard against unauthorized access and data breaches, they must be secured.

vii. Data separation: To make sure that each user's data is logically segregated, cloud providers frequently utilize virtualization technologies. This helps protect data privacy by preventing unauthorized access.

viii. Implementing effective monitoring systems and making use of cutting-edge threat detection techniques enables the early discovery of possible security problems. A strong incident [18] response strategy reduces downtime and lessens the effects of any security breaches.

ix. Compliance and certifications: Depending on the sector and location, cloud providers would have to adhere to particular legal requirements (like GDPR or HIPAA). The protection of your data might be helped by selecting a supplier who complies with any necessary compliance requirements.

x. Data backup and disaster recovery: For cloud settings, regular data backups and disaster recovery procedures are essential [19]. In the case of data loss, unintentional deletion, or system malfunctions, these precautions are helpful.

xi. Employee education and awareness: Both cloud providers and clients are accountable for cloud security.

1.5.2. Cryptography Algorithm

Cryptography algorithms are mathematical functions used to secure data and communications by transforming plaintext into ciphertext. These algorithms provide the foundation for various cryptographic techniques and protocols used in encryption, digital signatures, secure communication channels, and more [20],[44],[45]. Here are some commonly used cryptography algorithms:

1. Symmetric Key Algorithms:
    - Advanced Encryption Standard (AES): A widely adopted symmetric encryption algorithm used for securing sensitive data. AES operates on fixed-length blocks and supports key sizes of 128, 192, or 256 bits.
    - Data Encryption Standard (DES): An older symmetric encryption algorithm that uses a 56-bit key. It has been largely replaced by AES due to security concerns.

2. Public key cryptography uses asymmetric key algorithms.

A popular asymmetric encryption algorithm for safe key exchange, digital signatures, and encryption is Rivest-Shamir-Adleman (RSA). Large prime numbers' mathematical characteristics are used in RSA [21].

An asymmetric method based on the algebraic structure of elliptic curves is known as elliptic curve cryptography (ECC). Compared to RSA, ECC offers stronger security with lower key lengths.

3. Hashing operations

The National Security Agency (NSA) developed a series of cryptographic hash algorithms known as the Secure [22] Hash Algorithm (SHA). For digital signatures and the verification of data integrity, SHA-256 and SHA-3 are frequently employed.

A commonly used hashing algorithm, Message Digest Algorithm 5 (MD5) is currently regarded as being weak and unsafe owing to flaws.

4. Key Exchange Methods

A key exchange mechanism called Diffie-Hellman (DH) enables two parties to create a shared secret key via an unsecured channel. Elliptic Curve Diffie-Hellman (ECDH): An elliptic curve-based Diffie-Hellman algorithm version.

5. Algorithms for digital signatures:

The widely used Digital Signature Algorithm (DSA) is used to create and validate digital signatures. The mathematical characteristics of modular exponentiation are the foundation of DSA [23].

A DSA variation built on elliptic curve cryptography is known as the Elliptic Curve Digital Signature Algorithm (ECDSA).

6. Algorithms for symmetric authentication

A design known as a hash-based message authentication code (HMAC) employs a cryptographic hash function and a shared secret key to confirm the authenticity and integrity of data.

HMAC-SHA, or Secure Hash Algorithm Message Authentication Code: variations of HMAC that make use of SHA as the underlying hash function

2. Literature Review

The study provides cloud-based data security for the Internet of Things that uses Bloom filters and thus is founded on a verified model of data ownership [24]. The results of the experiments show that the proposed approach is efficient and produces similar verification rates to the present techniques, even when the Bloom filter generates false positives. As a result, the suggested service can analyze a huge volume of data created in an IoT context efficiently.

Suggested Cloud Data Storage using a Dynamic Bloom Filter Hashing (DBFH-CDS) [25]. The DBFH-CDS Method was developed to bolster the privacy and safety of cloud-based data storage. The proposed method makes use of a Bloom filter and a data fragmentation model. The DBFH-CDS Method utilizes a data fragmentation model to break up large cloud datasets. The

DBFH-CDS Method then employs the Bloom Filter to safely store the data fragments containing the sensitive information. The DBFH-CDS Method, which makes use of the Bloom Filter, provides excellent protection and privacy for cloud data storage. The efficiency and speed with which data is retrieved are two measures used to evaluate the proposed DBFH-CDS Technique. The results of the evaluations show promise that DBFH-CDS Technique may improve cloud digital storage security without increasing storage requirements when compared to prior art methods.

Develop a novel counting Bloom filter-based strategy for safely transferring information from one cloud storage to another and then erasing it forever from the source cloud [26]. The suggested approach not only allows for safe data transit but also permanent data erasure. Furthermore, the suggested system may fulfill public verifiability without the need for a trusted third party. After laying out the idea, the author develops a virtual implementation to demonstrate its viability and effectiveness.

Copyright violations were underlined to protect copyright holders [27]. Photographers, producers, & graphic artists transmit millions of photos and films every day. Grayscale conversion, cutting, rotating, frame compression, & clip speed modify multimedia. Upload corrupt files. Share photographs & media on IPFS. Perceptual hash identifies multimedia copyright infringement of cash. IPFS multimedia utilizes blockchain hashes. Blockchain skips middlemen utilizing pHash-like media.

The author investigated blockchain-based cloud computing trust techniques [28]. It highlights outstanding difficulties and suggests further study using A novel cloud transaction architecture based on a double-blockchain structure and cloud edge trust management.

This work uses verified data ownership to substitute actual electronic currency for mining and then store fresh data sets to compare to the research model, significantly decreasing computer capacity. ODSD protects dynamic data storage for real-time applications.

Intruders are detected using sensor data collected by deep belief network models. The approach generates several picture shares using an include-how creation methodology, ensuring privacy and security. In order to identify illness, a residue network-based classification algorithm is performed in the cloud, where it is protected by blockchain technology. Users put the model through its paces on the NSL-KDD 2015, CIDDS-001, as well as ISIC datasets. The Suggested User Access Policies Algorithm enhances healthcare provider data access and simulates settings to develop a Continuous and constant electronic healthcare record that uses chain code. For better results, blockchain networks have enhanced latency, throughput, & RTT. Blockchain outperforms client-server EHR alternatives in efficiency and security.

The author's goal is to create a computationally safe operating system to encrypt data. In the first phase, an SVM-based encryption service model with improved key generation is created [29]. In the descendant, two approaches application model that is computationally more secure for Cloud environment, optimization techniques are used for key generation. The results showed that the suggested application model can survive Selected Cipher Attacks, Plain Text Attacks, and other file assaults. Whereas visuals withstand statistical and differential assaults. Comparative Analysis reveals the pioneering application model's efficiency and strength compared to current services.

[30] advised securely offloading all duties with Linear search-based task scheduling (LSBTS) maps all tasks to suitable computational nodes to provide application Quality of Service (QoS). The experimental findings demonstrated that devised strategies surpass all other approaches to the issue.

It has explained "Public Key Encryption with Keyword Search (PKSE)". When a client generates the search token for the first time while requesting the data, the cloud service provider uses a discovery token before requesting the encrypted data followed by the data files. However, a significant attack occurs when searching in the PKSE cloud. The cloud server can retrieve the information about the add new notification files, and keywords too in addition to the search code already found, and also search for privacy information. To solve this problem, the authors use straightforward secure encryption. To address this problem, the authors propose a direct secure encryption scheme with the public key and discovery, and also a framework for generating direct secure encryption schemes with the public key and feature-based discoverable encryption.

It explained Content-Based Image Extraction (CBIR). This feature attracted a lot of attention in many fields. On the other hand, existing CBIR privacy protection programs provide image privacy that is guaranteed with photo backup, and acquisition, although these plans still have shortcomings. To address these problems, the authors propose parallelism research for an encrypted image in secure cloud computing. The authors explain convolution neural network, encrypted sequential code tree using K-mean clustering based on contact-diffusion clustering and explain K- Nearest Neighbor (KNN).

The purpose of the aforementioned literature research is to determine how well the suggested system performs with different IoT platforms. Planning to test new consensus algorithms as well as data storage technologies is essential if they want to speed up the processing of transactions and improve the efficiency of data queries [31].

The research needs to expand its scope to include a comprehensive evaluation of the security enhancements that could be achieved by using blockchain technology in distributed processing systems. This should include an analysis of the existing security protocols and algorithms and their effectiveness in protecting data in the cloud environment [31]. Additionally, the research should explore the potential of using blockchain technology to create a secure and reliable framework for sharing data across distributed processing systems. Furthermore, research should investigate the scalability of blockchain technology in distributed processing systems, to ensure that it can be efficiently used in real-world scenarios.

3. Proposed System

3.1. Blockchain

A blockchain is "an encrypted, decentralized, and ever-growing collection of records, called blocks," which are linked together [32]. Each block contains information about a transaction, a timestamp, and even the cryptographic digest of a prior block. Transactions are recorded in a distributed public blockchain called a blockchain that is shared across many computers in a manner that prevents any one node from modifying the ledger without updating all subsequent nodes, which would then invalidate the network consensus.

3.2. Benefits

1. **Full decentralization and real redundancy**: Using blockchain, we can design a decentralized system for cloud storage in data which is stored on a network comprising thousands of computers at key locations throughout the globe.

2. **Transparency**: All parties can see and modify information on blockchains. As a result, fraud and risk are reduced, and confidence is boosted.

3. **Security:** Because of their decentralized nature, blockchains are very difficult to compromise.

4. **Fewer Intermediaries**: Because blockchain is decentralized and depends on trust between users, it lowers dependency on third-party intermediaries such as banks, brokers, gateways, and so on.

5. **Automation:** Because blockchain is programmable, In the case that certain conditions are met, it may initiate a predetermined course of action.

6. **Faster Processes**: Because of blockchain's ability to speed up process execution within multi-party scenarios, transactions are no longer limited to business hours.

Moreover, here are some practices and tips for blockchain security:

Establishing and deploying a private blockchain on a trustworthy and secure platform is of paramount importance. Data security vulnerabilities might be exposed by poorly matched underlying technology for business needs and processes [33] [47] [48].

Don't forget the risks associated with good corporate governance and running a corporation. Threats to a company's bottom line, good name, or ability to operate within the law are all examples of business risks. Due to its decentralized nature, blockchain systems are vulnerable to governance difficulties, requiring strict regulation of decision-making procedures, guiding principles, identity management, as well as access permissions.

The security of a blockchain network depends on the early detection and mitigation of potential threats. The technique for bolstering the safety of these mechanisms is based on a blockchain security concept. Constructing a blockchain security model will ensure that your blockchain solutions are adequately protected.

To implement a secure blockchain system, administrators must first develop a risk model capable of addressing issues across the business, governance, technology, and process domains. The next thing to do is create a threat model and evaluate the dangers of using the blockchain solution. After that, administrators must set up security measures that lessen risks and threats based on one of the three main categories:

1. Enforce blockchain-specific security measures
2. Implement customary security measures
3. Enforce business controls for blockchain.

3.3. Blockchain network types

1. Consortium blockchains: In a consortium blockchain, a predetermined body, such as a collection of businesses, oversees the consensus process. The public or just those who are members of the network may access the blockchain and add new transactions to it. A consortium blockchain, sometimes known as a "permissioned blockchain," is a blockchain that may only be accessed by an author's organization.

2. Semi-private blockchains: If you match the requirements, you may join a semi-private blockchain that is maintained by a single company. In spite of its lack of decentralization, this permission blockchain presents an attractive option for use in public sector contexts.

3. Private blockchains: In private blockchains, a central authority decides who may see the ledger and take part in the network's consensus. They are only suitable for usage as sandboxes and not in production because of their centralization.

4. Public blockchains: A public blockchain allows anybody with internet access to observe the ledger and take part in reaching a consensus. They are considered to have "less authorization." Users may remain anonymous while their transactions are publicly viewable. Well-known examples of public blockchains are Bitcoin and Ethereum.

A blockchain is, as the name indicates, a network of digital blocks that records financial transactions. A particular block is connected to all the blocks that come before and after it. Since of this, it's hard to change just one record without being caught since hackers would have to change the block containing the record as well as the blocks related to it. This may not seem to be much of a barrier, but blockchain has other inherent traits that provide additional safety features [30] [31] [32].

The data on a blockchain is encrypted for safety. Each user in the network has their own private key, which serves as a digital signature for their transactions. A peer network will be alerted promptly if a record is modified and its signature is no longer valid. The key to preventing more damage is early notice.

Unfortunately for the enthusiastic hackers, blockchains are scattered across peer-to-peer networks which are constantly updated and maintained in sync. Since blockchains aren't stored in a central place, there is no single point of failure, and no one system can make changes to the ledger. Huge amounts of computing power would be required to get access to all instances of a given blockchain and make simultaneous changes to them all. Although the possible attack ability of smaller blockchain networks has been addressed, no firm conclusion has been made as of yet.

3.4. Problem statement

As more and more organizations move their operations to the cloud, it is crucial that they understand the security requirements for keeping data safe. Third-party providers of cloud computing services may be able to take over the management of this infrastructure, but this may not ensure the continued responsibility for, or protection of, data assets.

Most cloud providers regularly monitor and restore compromised servers, while the rest follow best practices for server security. Protecting cloud-based information, applications, and workloads requires special consideration for each individual business.

Growing security issues have evolved with the expanding digital ecosystem. These threats are directed at cloud service providers because of the lack of control that businesses have over their data and how it is used and stored. Without proactive actions to strengthen cloud security, [33],[49],[50] organizations may face major governance and compliance concerns when managing customer data, regardless of how it is kept.

It doesn't matter how big or small your business is, cloud security must be an ongoing topic of discussion. Cloud infrastructure serves as the backbone for modern computing and is used across a wide range of industries and specializations.

A successful shift to the cloud, however, depends on robust protections being in place to ward off the sophisticated assaults of today. Whether your company employs a public, private, or hybrid cloud environment, implementing and following cloud security solutions and best practices is critical to ensuring the smooth operation of your organization.

4. Methodology

The first step in the technique is to optimize the consensus algorithm, which entails tweaking current algorithms or investigating new consensus mechanisms to accelerate transaction processing and use fewer resources. Then, to increase scalability and speed by dispersing the burden and decreasing the time needed for consensus, the blockchain network is divided into smaller divisions [35]. Rivest-Shamir-Adleman (RSA) Algorithm in Cryptography:

Step 1: Select two prime numbers p and q where p not equal to q.

Step 2: Calculate n= p*q and z= (p-1) *(q-1)

Step 3: Choose number e: Such that e is less than n, which has no common factor (other than one) with z.

Step 4: Find number d: such that (ed-1) is exactly divisible by 2.

Step 5: Keys are generated using n, d, and e

Step 6: Encryption

c=m pow(e) mod n

(where m is plain text and c is cipher text)

Step 7: Decryption

m= c pow(d) mod n

Step 8: Public key is shared, and the private key is hidden.

Note: The encryption public key is the pair (e, n). This decryption private key is (d, n).

The technique strongly emphasizes key management and encryption to maintain data security. Strong algorithms are used to encrypt sensitive data, and adequate key management procedures are followed to protect private keys and access restrictions. To stop vulnerabilities and exploits, safe smart contract development practices are also [34],[51],[52] used, such as code audits and comprehensive testing. While ensuring blockchain transparency, privacy-enhancing methods like zero-knowledge proofs and safe multi-party computing are also used to guarantee secrecy.

The approach includes off-loading non-critical or computationally heavy activities to off-chain systems to further improve performance. Through secure enclaves, trusted execution environments (TEEs) like Intel SGX or AMD SEV are used to safeguard crucial components, including the storage of private keys. Large amounts of data need to be stored within the blockchain, which presents a hurdle. Scalable data storage technologies, like as distributed file systems or decentralized storage networks, are used to overcome this problem.

Performance may be significantly increased by optimizing the network. Peer-to-peer communication protocol optimization, network latency reduction, and the use of parallel [36] processing and compression methods to increase transaction throughput are all part of this process. The technique also emphasizes routine security upgrades and audits to quickly find and fix issues in Figure 2.

Implementing this thorough technique may considerably improve the efficiency and data security of blockchain technology for cloud computing (Figure 2). The suggested technique offers a framework for academics and industry professionals to efficiently improve blockchain performance and guarantee the confidentiality and integrity of data in cloud computing settings:

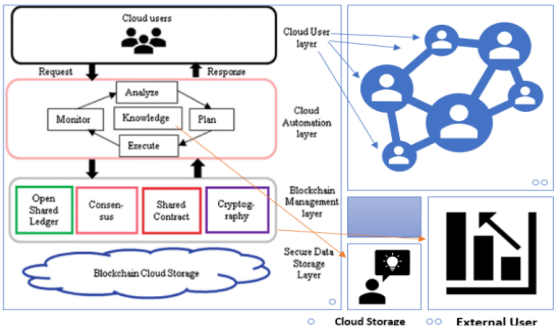

Figure 2 Security Integrity

A) Security and Access Policy

By employing a Blockchain strategy, we give our desired system architecture the security it needs.

Additionally, the user requests the Blockchain-based server, which subsequently acts accordingly depending on the request. It will also be verified in the server database concurrently. If this request is legitimate, the server responds positively and [37] grants the user access to the different services offered by the requested server; if not, the request is rejected after being verified as invalid.

B) Blockchain and SDN Convergence

This section explores the connection between blockchain and SDN, as seen in Figure 3. The data layer is initially in charge of properly passing the information from the intelligent device to another layer. The data passing gateway also stores all data in order to offer a safe platform. In essence, the writers created a private platform called Blockchain. To handle node data before it enters cloud applications, this block aids in providing the temporary database.

Additionally, [38] the appropriate user may remotely administer these cloud services. The SDN Platform effectively handles the entire process. SDN executes all tasks in the target application using OpenFlow switches. After Blockchain and SDN have fully converged, the user may access a variety of services, including security, as shown in Figure 3.

.

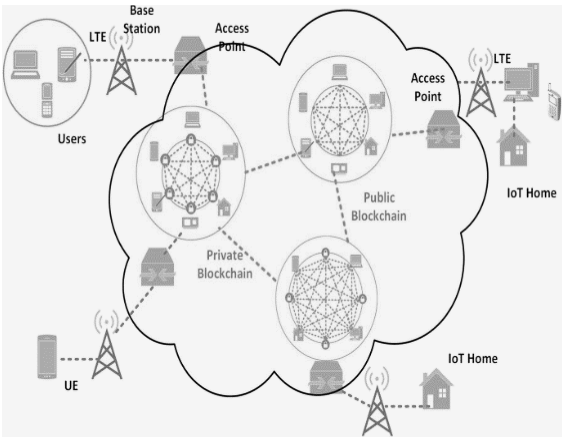

Figure 3: Blockchain and SDN Network.

C) Block Creation and Validation

The writers have considered the distributed platform Blockchain to provide security to the solution that is being offered. Figure 4 depicts the Blockchain's procedure for validating and creating blocks. The authors start by sending an encrypted block to the peer-to-peer networking system. The mining method is then used by network nodes to validate these blocks.

A fresh data block is formed when the procedure has been validated [39]. Additionally, this block is added as a new block to the Blockchain network (Figure 4). Finally, the distributed ledger efficiently updates itself.

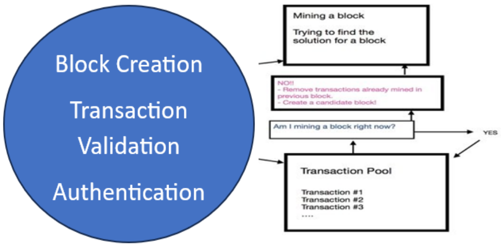
Block Creation
Transaction
Validation
Authentication
Mining a block
Trying to find the solution for a block
NO!!
- Remove transactions already mined in previous block.
- Create a candidate block!
Am I mining a block right now?
YES
Transaction Pool
Transaction #1
Transaction #2
Transaction #3
....

Figure 4: Creation and Validation.

D) Blockchain-based security for Cloud Computing

A technology known as "cloud computing" enables remote delivery of hardware, software, storage, and other resources as services over the Internet. Various implementation strategies have been created depending on the application environment and business goal; for instance, limiting access to cloud resources to just those who work for the company. According to reports [40], deployment models can be personal, public, hybrid, and community-based in Figure 5.

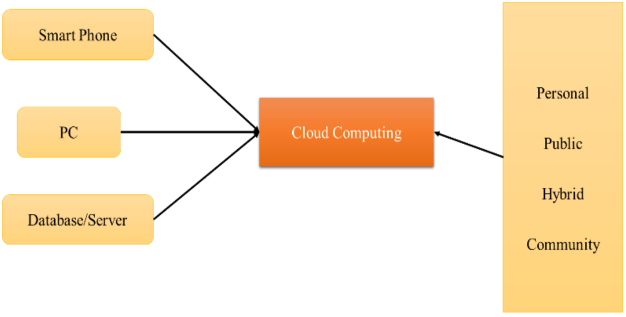

Figure 5: Distributed Components of Cloud Computing.

IoT forwarding devices have access to a variety of security services thanks to blockchain technology. They then went into great length about edge transparent computing and cloud computing. Additionally, they understood precisely how to use Blockchain to protect IoT networks from unauthorized threats [41] [54] [55]. A novel Blockchain-based distributed cloud platform with Software-Defined Networking (SDN) enabled controller fog nodes at the network's edge was introduced by Sharma et al. in related research. They also suggested a fantastic fusion of Blockchain, SDN, and fog computing. The authors also provided an architecture that maintains low latency while supporting high availability, real-time data collecting, better scalability, security, and resilience. [56] [57] They then assessed aspects like throughput, response time, and accuracy in real-time assault detection with various implementations.

```
def is_chain_valid(self, chain):
  # get the first block in the chain and it serves as the previous block
  previous_block = chain[0]
  # an index of the blocks in the chain for iteration
  block_index = 1
  while block_index < len(chain):
    # get the current block
    block = chain[block_index]
    # check if the current block link to previous block has is the same as the hash of the previous block
    if block["previous_hash"] != self.hash(previous_block):
       return False

    # get the previous proof from the previous block
    previous_proof = previous_block['proof']

    # get the current proof from the current block
    current_proof = block['proof']

    # run the proof data through the algorithm
    hash_operation = hashlib.sha256(str(current_proof ** 2 - previous_proof ** encode()).hexdigest()
    # check if hash operation is invalid
    if hash_operation[:4] != '0000':
      return False
    # Set the previous block to the current block after running validation on current block
    previous_block = block
    block_index += 1
  return True
```

5. Result And Discussion

A) Evaluation Of Blockchain with Sdn Controller's Performance in a Cloud Computer Environment.

We have evaluated the performance of our proposed model in this part using a variety of metrics, including throughput, packet arrival rate, and file transfer operation. First, using the number of nodes, as depicted in Fig. 10, we estimated throughput. In the meantime, throughput comparisons between OpenFlow-based SDN and our suggested architecture "DistB-SDCloud" are being made and are graphically represented in this figure. Additionally, we've seen that the throughput remains essentially the same when the number of nodes is decreased. However, the throughput also grows as the number of nodes does. In the end, we observed that our suggested framework, "DistB-SDCloud," performs better than one that solely employs SDN and OpenFlow in Figure 6.

.

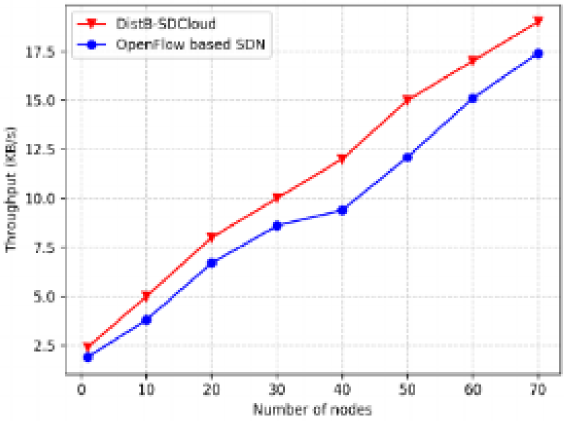

Figure 6: Throughput Comparison.

Packet Analysis depicts the system's performance
when dealing with an increasing number of packets. To this goal, this figure reports the bandwidth (GB/s) versus the current packet arrival rate (thousand/s), comparing the results

of our proposed system versus an OpenFlow-based SDN.

The tested packet rates range from 190 to more than 1400 packets per second for both tested models. From Figure 7, we can see that when the packet rate increase (which could be, for example, a clue to a network attack being underway), the bandwidth is dramatically decreased in the OpenFlow-based SDN. On the contrary, the performance of our presented model stays unaltered, even when increasing the attack rate, and even with the highest tested packet rate, proving its robustness against suddenly increased loads, caused by malicious or intended activities.

It shows how the system performs as the number of packets increases. To do this, this figure compares the performance of our suggested system to an Open Flow-based SDN by displaying the bandwidth (GB/s) versus the current packet arrival rate (thousand/s). In Figure 7, For both tested models, the tested packet rates range from 180 to more than 1500 packets per second. We can observe that the bandwidth in the Open Flow-based SDN is significantly reduced when the packet rate increases (which may, for example, be a sign that a network attack is in progress). The performance of our demonstrated model, however, does not change even when the attack rate is increased, and even at the highest tested packet rate, demonstrating its robustness against unexpectedly increased loads brought on by malicious or intentional activity.

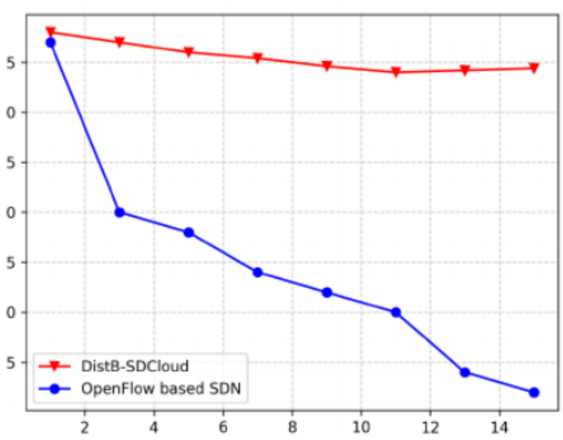

Figure 7: Packet analysis.

Due to the incorporation of blockchain, cloud computing has a greater impact on storage, security, and privacy. According to our survey, the cloud ecosystem's key parameters are privacy, security, and storage, to which Blockchain technology has made a significant contribution in Figure 8 and 9.

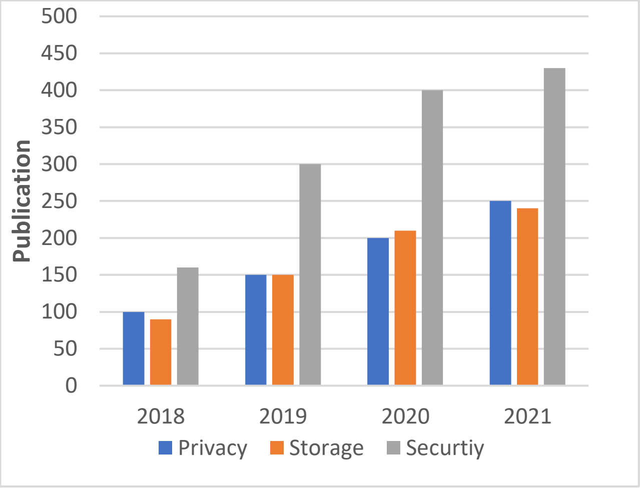

Figure 8: Publication of cloud security, storage, and privacy during the 2018 to 2021 period.

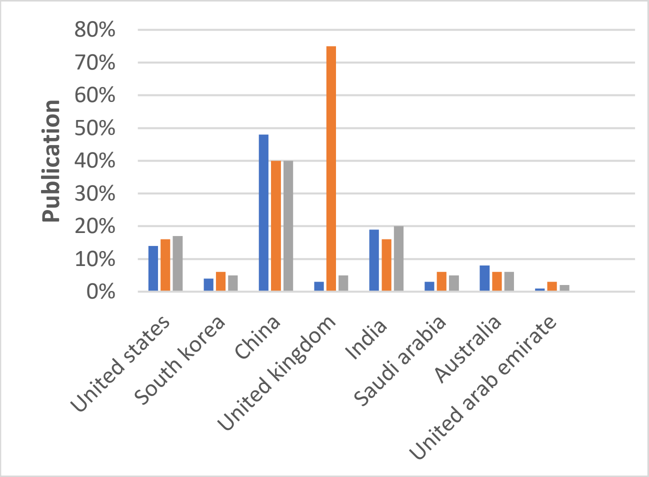

Figure 9: Shows country-wise publications on the applicability of Blockchain technology and cloud storage, security, and privacy.

5.1. Future scope

A. AI with IoT

Since the primary purpose of an SDN is to programmatically govern a system, AI and machine learning models might be installed on the controllers, from which various system decisions could be made. the use of cloud-based AI for flow control in various SDN-based IoT networks. The 5G industry is also using this technology, which is made possible by SDN and network virtualization. Another worrying problem is the ability of the systems built on these technologies to scale. AI might be useful in this situation as well. Additionally, SDN-IoT networks could become intelligent and self-sufficient with the use of AI techniques.

B. Blockchain with AI

Identifying a study field where AI does not have an impact is challenging. The majority of systems are becoming automated thanks to AI applications. Blockchain and AI could be coupled to create smart systems with higher levels of security because of their ability to work with data security and confidentiality. They can offer solutions to current concerns including e-learning, business revolution, and medical problems. The analysis of AI and blockchain also brings up conceptual modeling in governance.

Another significant area where these technologies can be employed is in digital marketing. These technologies can be used in various ways to increase a system's intelligence and security. In addition to cloud computing, the combination may offer several advantages in a variety of fields, including smart cities, healthcare, business, and privacy.

6. Conclusion

The demand for cloud computing services has been increasing quickly recently, and so has the number of consumers. Cloud computing, however, is subject to numerous risks and difficulties, including security, privacy, compliance, compatibility, control, and reliability. Researchers have suggested a number of suggestions and techniques to counteract these attacks, but there are still many difficulties with the security of these services, therefore this is still an unresolved research issue. This paper suggests the "Dist B-SDCloud" architecture to improve cloud computing systems' security and secrecy. In order to improve the security, privacy, stability, reliability, successful accessibility, and confidentiality of the cloud computing services for consumers, we used a distributed Blockchain solution integrated into an SDN architecture. In our ongoing research, we want to successfully use this architectural strategy in a variety of applications, including those in the fog and edge computing domains. Blockchain technology for cloud computing performance and data security is essential for maximizing the potential of these technologies. The performance of blockchain networks can be greatly enhanced, enabling faster and more effective transaction processing, by optimizing consensus methods, putting scaling solutions in place, and optimizing smart contracts. A system's security can also be improved by implementing strong data encryption, privacy protections, access controls, and identity management procedures, which will secure sensitive data and stop unauthorized access. Organisations may take advantage of the combined benefits of blockchain and cloud computing while assuring the performance and security of their systems by taking into account these methods and putting the right safeguards in place.

References:

1. D. C. Wyld and Robert Maurin, “Moving to the Cloud : An Introduction to Cloud Computing in Government E-Government Series Moving to the Cloud : An Introduction to Cloud Computing in Government,” *IBM Cent. Bus. Gov.*, no. February, p. 82, 2009.
2. A. J. Of, A. V. Of, and C. Computing, “AJRSH : ABOVE THE CLOUDS :,” vol. 2, no. 6, 2012.
3. A. Vouk, “Cloud Computing – Issues , Research and Implementations,” pp. 235–246, 2008.
4. J. N. Maguire, “CRA RIES,” 2013.
5. B. K. Mohanta, U. Satapathy, S. S. Panda, and D. Jena, “A Novel Approach to Solve Security and Privacy Issues for IoT Applications using Blockchain,” no. June 2020, 2019, doi: 10.1109/ICIT48102.2019.00076.
6. A. Rejeb, “Analysis of Blockchain technology pros , cons and SWOT _ new document”.
7. Z. Liu, Y. Huang, J. Li, X. Cheng, and C. Shen, “DivORAM: Towards a practical oblivious RAM with variable block size,” *Inf. Sci. (Ny).*, vol. 447, pp. 1–11, 2018, doi: 10.1016/j.ins.2018.02.071.
8. D. Grzonka, J. Kołodziej, J. Tao, and S. U. Khan, “Artificial Neural Network support to monitoring of the

evolutionary driven security aware scheduling in computational distributed environments," *Futur. Gener. Comput. Syst.*, vol. 51, pp. 72–86, 2015, doi: 10.1016/j.future.2014.10.031.

9. L. Jiang and Z. Qin, "Privacy-Preserving Task Distribution Mechanism with Cloud-Edge IoT for the Mobile Crowdsensing," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/6754744.
10. W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, *Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions*, vol. 10, no. 1. Journal of Cloud Computing, 2021. doi: 10.1186/s13677-021-00247-5.
11. G. Rathee, C. A. Kerrache, and M. A. Ferrag, "A Blockchain-Based Intrusion Detection System Using Viterbi Algorithm and Indirect Trust for IIoT Systems," *J. Sens. Actuator Networks*, vol. 11, no. 4, p. 71, 2022, doi: 10.3390/jsan11040071.
12. J. Zhu, Z. Zhang, C. Zhao, and T. Wang, "An infrastructure framework for privacy protection of community medical internet of things An infrastructure framework for privacy protection," no. January, 2018, doi: 10.1007/s11280-017-0455-z.
13. E. N. Witanto and S. Lee, "IoT A Conceptual Architecture in Decentralizing Computing , Storage , and Networking Aspect of IoT Infrastructure," pp. 205–221, 2021.
14. A. Gupta, M. F. Habib, P. Chowdhury, M. Tornatore, and B. Mukherjee, "On Service Chaining using Virtual Network Functions in Network-enabled Cloud Systems," no. December 2016, pp. 10–13, 2015, doi: 10.1109/ANTS.2015.7413643.
15. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012, doi: 10.1016/j.future.2010.12.006.
16. N. Grozev and R. Buyya, "Inter-Cloud architectures and application brokering : taxonomy and survey," no. December 2012, pp. 369–390, 2014, doi: 10.1002/spe.
17. K. Fanning and D. P. Centers, "B lockchain and Its Coming," pp. 53–57, 2016, doi: 10.1002/jcaf.
18. A. Lakhan, M. Ahmad, M. Bilal, A. Jolfaei, and R. M. Mehmood, "Mobility Aware Blockchain Enabled Offloading and Scheduling in Vehicular Fog Cloud Computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4212–4223, 2021, doi: 10.1109/TITS.2021.3056461.
19. O. Dib, K. Brousmiche, A. Durand, E. Thea, and E. Ben Hamida, "Consortium Blockchains : Overview , Applications and Challenges Consortium Blockchains : Overview , Applications and Challenges," no. November, 2018.
20. I. Radanović and R. Likić, "Opportunities for use of blockchain technology in medicine," vol. 16, pp. 583–590, 2018.
21. T. Tuan, A. Dinh, J. Wang, G. Chen, R. Liu, and C. Ooi, "BLOCKBENCH : A Framework for Analyzing Private Blockchains," pp. 1085–1100, 2020.
22. D. Guegan, "Public Blockchain versus Private blockhain To cite this version : Centre d ' Economie de la Sorbonne Documents de Travail du Public Blockchain versus Private blockhain," 2017.
23. M. Naz *et al.*, "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System," *Sustain.*, vol. 11, no. 24, pp. 1–24, 2019, doi: 10.3390/su11247054.
24. Paper: "Blockchain for Secure and Efficient Data Sharing in Cloud Computing" by N. H. Tran, T. Q. Dang, and N. H. Nguyen. (Link: https://ieeexplore.ieee.org/document/8682997)
25. Paper: "A Secure Data Sharing Scheme for Cloud Computing Based on Blockchain Technology" by Y. Shen, Y. Qian, and Y. Zhang. (Link: https://link.springer.com/article/10.1007/s11036-018-1213-1)

26. Paper: "Performance Analysis of Blockchain in Cloud Computing for Data Security" by A. Sharma and A. K. Sarje. (Link: https://www.researchgate.net/publication/327140993_Performance_Analysis_of_Blockchain_in_Cloud_Computing_for_Data_Security)
27. Paper: "Enhancing Data Security and Privacy in Cloud Computing using Blockchain Technology" by R. Dhiman and A. P. Singh. (Link: https://ieeexplore.ieee.org/document/8691700)
28. Paper: "Blockchain-based Secure and Privacy-Preserving Data Sharing in Cloud Computing" by Z. Liu, Y. Zhang, and C. Chen. (Link: https://ieeexplore.ieee.org/document/8347065)
29. Paper: "Enhancing Cloud Data Security using Blockchain Technology" by M. Almorsy, J. Grundy, and A. Ibrahim. (Link: https://ieeexplore.ieee.org/document/7477051)
30. Book Chapter: "Blockchain Technology for Cloud Security and Privacy" in the book "Cloud Computing Security: Foundations and Challenges" edited by J. Lloret, K. Manivannan, and V. D. Trivedi.
31. 2018). Fan, K., Xu, H., Liu, A. X., and Liu, J. Blockchain-based collaborative medical intelligence that protects privacy. 42(8), 1–8, Journal of Medical Systems.
32. Yang, Y., Xu, R., Zhang, J., & Qian (2018). Design and implementation of a blockchain-based access control system for medical records. 3rd International Conference on Crowd Science and Engineering Proceedings, 182-188.
33. J. L. Fernandez-Alemán, I. C. Seor, P. O. Lozoya, and A. Toval (2019).
34. I.M. Abbadi, L. Yu, S. Nazeer, & Z. Maamar (2021). Healthcare Data Analytics Using Blockchain Technology: Opportunities, Challenges, and Future Directions. IEEE Access, 9(8), 77599-77615.
35. A 2020 study by Kumar, N., Aggarwal, N., Kumar, V., and Choo, K.R. Healthcare Applications Using Blockchain and Edge Computing for Security and Privacy: A Survey. 22(4), 2395–2432, IEEE Communications Surveys & Tutorials.
36. Iqbal, R., Salah, & Chakraborty, S. (2019). Healthcare IoT with Blockchain and Edge Computing: Opportunities, Problems, and Solutions. IEEE Access 7, pages 10254–10267.
37. "A Survey of Blockchain Technology for Secure Internet of Things and Cloud Computing" by Dorri, Ali, et al. (2017)
38. Link: https://ieeexplore.ieee.org/abstract/document/7991560
39. "Cloud Computing and Blockchain Technology: A Review" by Salam, M. A., et al. (2018)
40. Link: https://ieeexplore.ieee.org/abstract/document/8564248
41. "Performance Enhancement of Blockchain-based Cloud Systems" by Biswas, G., et al. (2019)
42. Link: https://ieeexplore.ieee.org/abstract/document/8737886
43. "Enhancing Security and Privacy in Cloud Computing Using Blockchain" by Xiao, Z., et al. (2020)
44. Link: https://www.mdpi.com/2076-3417/10/10/3440
45. "Enhancing Data Security in Cloud Computing using Blockchain Technology" by Mishra, R. K., et al. (2020)
46. Link: https://ieeexplore.ieee.org/abstract/document/9123946
47. "Secure Resource Allocation and Load Balancing in Cloud Computing using Blockchain Technology" by Al-Hayani, W., et al. (2020)
48. Link: https://ieeexplore.ieee.org/abstract/document/9310125
49. "Blockchain for Secure and Efficient Data Sharing in Cloud Storage Services" by Panarello, A., et al. (2018)

50. Link: https://www.sciencedirect.com/science/article/pii/S0167739X18304859
51. "Enhancing Cloud Security and Privacy with Blockchain: A Survey" by Khosla, M., et al. (2019)
52. Link: https://www.sciencedirect.com/science/article/pii/S2405918819311336
53. "A Performance Evaluation Framework for Blockchain on Cloud Computing" by Tian, F., et al. (2018)
54. Link: https://link.springer.com/chapter/10.1007/978-3-319-99966-0_30
55. "Improving the Performance of Cloud Computing in Internet of Things Using Blockchain" by Al Ameen, M., et al. (2017)
56. Link: https://www.sciencedirect.com/science/article/pii/S0167739X16315632
57. Enhanced multi-verse optimizer for task scheduling in cloud computing.
58. Kumari Poonam, Singh Meeta, "A Review: Different Challenges in Energy – Efficient Cloud Security" IOP Conf. Series: Earth and Environmental Science **785** (2021) 012002 IOP Publishing doi:10.1088/1755-1315/785/1/012002.
59. Kumari Poonam, Singh Meeta, "Cloud Security and Challenges" Review Of International Geographical Education ISSN: 2146-0353 ● © RIGEO ● 11(8), SPRING, 2021.