A Survey on Data Security in Cloud Computing Using Blockchain: Challenges, Existing State of the Art Methods, and Future Directions

Muhammad Usman Ashraf [1], Maham Iftikhar[2], Munam Ali Shah[2,] and Iqra Ilyas[3]
[1]Department of Computer Science, University of Management and Technology, Sialkot.
[2]Department of Computer Science, COMSATS University Islamabad (CUI), Islamabad, Pakistan
[3] GC Women University, Sialkot, Pakistan
Email: usman.ashraf@skt.umt.edu.pk

(Received: 04 April 2021; Accepted: 05 May 2021 ; Issue Published: 12 September 2021)

Accepted Manuscript

ABSTRACT

Cloud computing is one of the ruling storage solutions. However, the cloud computing centralized storage method is not stable. Blockchain, on the other hand, is a decentralized cloud storage system that ensures data security. Cloud environments are vulnerable to several attacks which compromise the basic confidentiality, integrity, availability, and security of the network. This research focus on decentralized, safe data storage, high data availability, and effective use of storage resources. To properly respond to the situation of the blockchain method, we have conducted a comprehensive survey of the most recent and promising blockchain state-of-the-art methods, the P2P network for data dissemination, hash functions for data authentication, and IPFS (InterPlanetary File System) protocol for data integrity. Furthermore, we have discussed a detailed comparison of consensus algorithms of Blockchain concerning security. Also, we have discussed the future of blockchain and cloud computing. The major focus of this study is to secure the data in Cloud computing using blockchain and ease for researchers for further research work.

Keywords: Cloud Computing, Blockchain, Data Security, Encryption, Decentralized Technology, Hashing.

1. INTRODUCTION

The concept of cloud technology is fundamentally pioneered because a wide variety of resources are needed, including networking, safety, storage, machine intelligence, and standard business applications. Cloud computing can therefore also be defined as software outsourcing. You can access various software and resources from anywhere else in the world funded by a foreign entity called the cloud. Cloud computing provides different advantages [1], such as,

- The self-service framework where users can use various computer tools to fulfill all job requirements.
- The permeability with which the use of data can be increased with increasing demand and decreased data use with declining demand. This reduces the number of high costs.
- CSPS also uses out-of-date services for scalable workloads to guarantee versatility in storage and handle sensitive throughput for users across many regions globally.
- Versatility to transfer data from one cloud to another, where possible.

Cloud is classified into three models [2]

- Infrastructure as a service (IaaS) is a model that provides data security, maintenance, data backup, etc to the cloud hosts critical infrastructures such as servers, applications, storage, etc., [1].
- Service software (SaaS) is a role model that can be used by multiple programs [2].
- Platform as a service is a model wherein users build and run their applications and services without being stuck in code, architecture, and inventory [1].

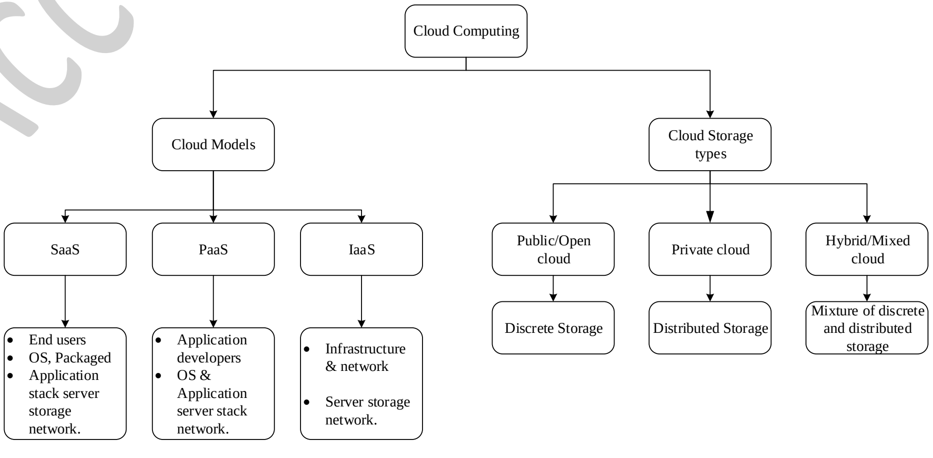

Figure 1: CC Models & Storage types

Generally, the cloud offers services such as security, storage, networking, massively parallel computing [52], artificial intelligence [43], etc. To make use of these facilities, different companies are renting out to cloud service providers [1, 45]. Today, it is the vendor's duty to offer the services to customers in compliance with their specifications. But every coin has two sides, there are various problems, such as data protection, integrity, confidentiality, miss management, etc., with this excellent technology [1]. Distributed storage allows the client to store their information on the network. All data set aside in the cloud is scrambled and cloud management is available. Under the reach of the SLA, which covers integrity and security of information [3]. Numerous companies have shifted their entire data center to the cloud. Acknowledge points of interest such as versatility, load modification, waste, usability, and respectability [4]. It is therefore important to protect an attack vulnerable to constraining devices.

Blockchain is a free, transparent, distributed ledger that captures digital records that cannot be meddled. Blockchain offers a transparent yet secure decentralized solution to ensure the system's flow of knowledge and information. With blockchain, the entire path of data flow in the system can be maintained, and information can be traced back to where it originated. Blockchain offers a safe approach that validates the individuals involved in the communication in a distributed and decentralized manner [5]. The technology of Blockchain uses a consensus-based data update system. Every and indeed most nodes should be verified in the public directory of all blockchain nodes, making it extremely difficult to manipulate and forge new generation data [6]. The data of the blockchain system are secured using a general cryptography technology, but all nodes need to validate data before the block is entered, which can be demanded at null post-writing costs to all nodes, reducing the cost of the system node's dependency on confidence and thus minimizing the gain of knowledge [6].

Since some of the underlying capacity blockchain data include integrity, confidentiality, and availability, like other systems, standards and cybersecurity controls need to be implemented to protect organizations.

Using blockchain within their technological infrastructure. Deloitte cyber professionals worldwide recommend that businesses take a safe, vigilant, and resilient (SVR) cyber strategy that helps organizations stay secure and strengthens their vigilance and resilience in response to emerging cyber threats.

To help leaders further drive the productivity of their organizations, we think that embraced this safe, vigilant, and resilient cyber approach is crucial [7].

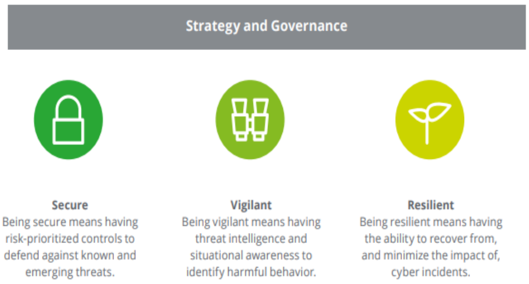
Strategy and Governance
Secure
Being secure means having risk-prioritized controls to defend against known and emerging threats.
Vigilant
Being vigilant means having threat intelligence and situational awareness to identify harmful behavior.
Resilient
Being resilient means having the ability to recover from, and minimize the impact of, cyber incidents.

Figure 2: Blockchain Strategy & Governance [7]

Blockchain distributed storage arrangements take information from the client and break it into tiny lumps. They provide an extra layer of protection at that point, and it's spread all over the device. This is conceivable by using Blockchain highlights such as hashing power, public-private key encryption, and record exchange. Each piece of information is stored in a decentralized area [4]. If gate crashers try to hack into it, they initially get scrambled records, and then only get a lump of information and not a whole record; this ensures that reports are stored in blockchain-based distributed storage [4, 39, 40]. Privacy and confidentiality of data is a problem when third parties process data. Storage can be generated from peers' underutilized resources. Data protection, safety, availability, and usage of resources are the areas protected by the blockchain [8]. Blockchain is the perfect method for transferring data from A to B without stressing that false data is stored in the record, as this would fulfil the entire chain of a large number of cases. Innovation is responsible, as the interactions that are registered are only through various gatherings [3]. Confirmation and no exchange in the record can be changed at a later point by the meetings. Well, Blockchain can provide data protection. The knowledge contained in the blockchain is fully unified [3]. The advantage of blockchain is the interconnection of devices owned by different users who share their computing power and storage reliably and securely. Blockchain-based networks will also replace the cloud by offering a decentralized and secure storage facility that can help process data transmitted across the network. Blockchain technology, however, has pressing problems that occur in a constrained resource setting [2].

2. LITERATURE REVIEW

Deepak Kumar Verma [2] discussed that the key benefit of cloud computing is that consumers do not have to pay for infrastructure, for installation, for manpower to manage those infrastructure and maintenance. The other benefits of using cloud computing are cost savings, versatility, and scalability. The rapid expansion in the "cloud computing" business also poses serious security issues. Cloud storage security privacy and confidence problems are reviewed in the proposed document. In promoting a stable, virtual, and economically viable

Accepted Manuscript

IT solution in the future, cloud computing has the potential to become a frontrunner.

The PDP (Provable Information Ownership) model enables a client to check the first information is given without retrieval on an untrusted server. It generates probability ownership checks by evaluating arbitrary server square arrangements that certainly minimize I/O costs, proposed by Anagha Markandey *et. al.* [1].

[3, 46] discussed that the specifications and concerns of current security and privacy protection approaches have been discussed to resolve the problem of big data security and privacy protection and expose the idea of large data cloud computing and its linkages. On a cloud platform, a reference model is suggested. In a big data security analysis, this model offers the efficient approach for the integration of early alerting and threat-perception of device risk with measures, data layers, interface, and application layers [48]. At the same time, it illustrates a plausible path for research using the blockchain to address cloud protection and privacy.

The networks are vulnerable to various security concerns such as intrusion, fishing, hacking, and multiple encryption methods are used to curb the same. Different attacks that compromise the basic CIA triad of network security are vulnerable to IoT environments [47]. To meet the needs of their restricted architecture, lightweight algorithms are built. Blockchain is a technology that helps to achieve safe and tamper-proof data transfer between two objects by a peer-peer. Blockchain will empower the credibility of networks in this way. They focused on blockchain technology's applications and challenges in securing cloud computing and IoT environments. While it allows a secure peer-peer transaction between the node, expanding blockchain technology to IoT environments thus enhanced the security of systems, but it increases the system's complexity. The opposite of engaging blockchain technology in a resource-inhibited setting is doubtful, but the desired protected peer-peer functionality can be realized if the correct balance is maintained between cloud storage, IoT environments, and the benefits of blockchain technology [5, 42, 43, 49].

2.1. Cloud Computing Threats

In figure 3 we have discussed the basic threats of cloud computing. We have discussed technological, human-related and hardware, and software-based threats in this taxonomy diagram [41].

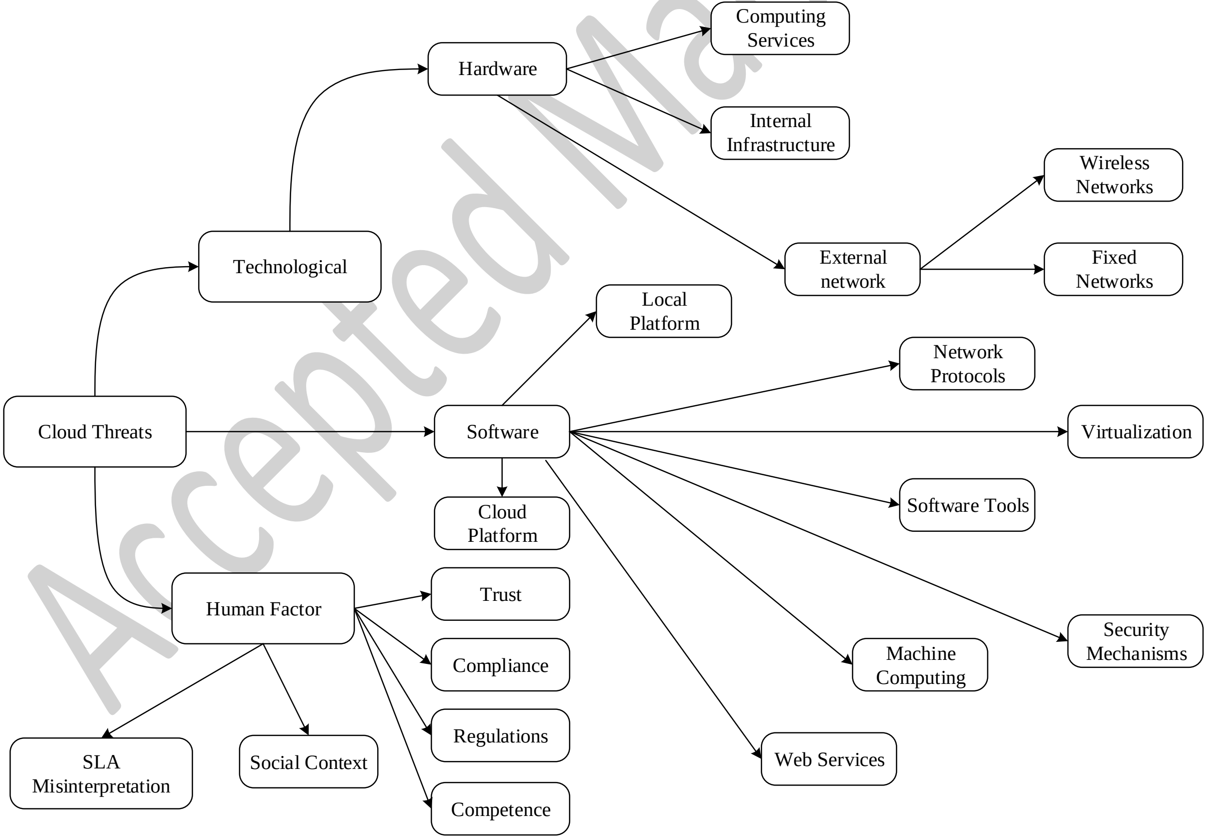

Figure 3: Cloud Threats Taxonomy diagram

Aamir Mughal *et. al.* [4] discussed that, due to the progress of web innovation, the content of data is becoming quite gigantic. The capacity limit of the client terminal must be expanded with the assistance of the cloud stage (platform) to deal with enormous data. The management of information on the cloud platform requires strict security measures. To solve the above issue a Blockchain for cloud storage and protection is proposed. The decentralized and disseminated existence of the blockchain procedure

Accepted Manuscript

guarantees the prerequisites for protection and persuades cloud storage to enhance security. We present the idea of blockchain technology and its hot research developments are discussed. Two key calculations, such as job verification and stake confirmation Blockchain exchanges are often used to guarantee confidentiality. Therefore, by proposing a method of safe blockchain use this study addressed the method of providing protection.

The two aspects of innovation, first to help SaaS services, a centralized cloud-based SaaS service platform includes virtualization, automated deployment and distributing, standardization of data formats, information sharing, and efficient user and operational management functions. A cloud storage platform is essentially the unified support network for the service. Second, to better adapt to the blockchain system, our systems use peer-to-peer networks for data distribution. The findings are satisfactory. The data must be organized to ensure that the flow of information through this mechanism is accurate and rapid. Data normalization specifically involves four aspects: standardization of data components, standardization of database structure, standardization of data storage, and standardization of input and output [6]. The built core platform will assist in developing the robust system.

Meet Shah *et. al.* [8] Cloud storage was proposed as a pioneering alternative to storage, but a centralized cloud storage strategy was not effective. On the other hand, Blockchain is a distributed ledger cloud storage system that ensures data protection. Blockchain is a decentralized peer-to-peer framework that preserves a blockchain version, ensuring it immutable for each network node. The recommended system is that the IPFS (Interplanetary File System) protocol encrypts and processes a user file through multiple peers in a network [50]. IPFS defines a hash value. The hash value defines the file path and is stored in the blockchain. The emphasis is placed on decentralizing secure storage of data, high data access, and open storage.

[9] said that, Cloud storage is a technology in which multiple users store a vast volume of data that is pooled. The knowledge that is stored comes from different organizations, people and cultures, etc. Therefore, the protection and privacy of data is a big concern in terms of the existence of the stored data. We'll combine the two most reliable algorithms to boost data protection. AES and RSA data encryption and decryption algorithms. Multilevel encryption is, therefore, not very easy to crack [44].

The Blockchain is an extremely powerful way of enforcing the protection and integrity of cloud platform data. We addressed the Blockchain types along with their implementations. Blockchain platforms comparative analysis: Ethereum, Hyperledger, and R3 Corda. In the fields of Fintech, wealth management, the insurance sector, payment gateways, and many more, blockchain is rapidly evolving. We agree that the continued incorporation of Blockchain into applications to directly enhance the availability and integrity of cloud data for protection is yet to be explored. In order to suggest a more robust and reliable framework solution, this paper encourages researchers to manipulate the platforms in extreme circumstances and analyze them to improve data availability over the distributed ledger using Blockchain technology [10].

Amel Ben Lazreg *et. al.* [11] discussed the cloudlet technology. Further discussed that, recently, Blockchain technology has gained considerable interest, especially in providing distributed applications with scalable, safe solutions. On the basis of this groundbreaking technology, their paper proposes the implementation of the Blockchain-based security solution to ensure a variety of security services, including transaction traceability and secure transactions between cloud users and cloud servers. Moreover, a super-agent component was introduced to track and fix crashes between the Cloud and Cloudlets caused by the lack of protection and data synchronization problems in cloud systems, which resulted in some deadlock situations. In an industrial environment, the proposed blockchain-based solution was introduced and experimented with. The first is the handling of a variety of critical impasse situations in cloudlet. The second relates to the reliability of the entire system when Blockchain is implemented. Our model gives promising experimental results.

Cloud computing has huge advantages, but the security of cloud data is increasingly threatened. They conducted a safety survey to show the safety effectiveness of the types of cloud computing and blockchain technology. The survey provides a detailed understanding of a blockchain-based POW (Proof-of-Work) model with blockchain technology [12, 44, 45]. They also recognized that blockchain technology is one of the growing technologies with maximum privacy guarantees.

A detailed survey on cloud computing integration with blockchain. Further discussed, blockchain technology is an evolving topic that is well known for its immutability and the information protection it offers. They said that we would solve some of the approaches to cloud computing problems with the help of Blockchain Technology.

They suggested a protocol for safely using and eliminating the blockchain [13]. It would seem that, in addition to protection, efficacy trials are also required, given the sense in which a large amount of information is transmitted.

Accepted Manuscript

2.2. CC Security challenges and Attacks

Figure 4 has discussed different types of cloud computing challenges and attacks. These attacks are network-based, models based i.e., SaaS, IaaS, PaaS, and cloud storage types based i.e. Public, Private and hybrid. The well-known attacks on the cloud are DDoS, Flooding attacks, SQL Injections, MITM attacks, Phishing attacks, malicious insiders, authentication attacks, unencrypted data, and incomplete data deletion, etc.

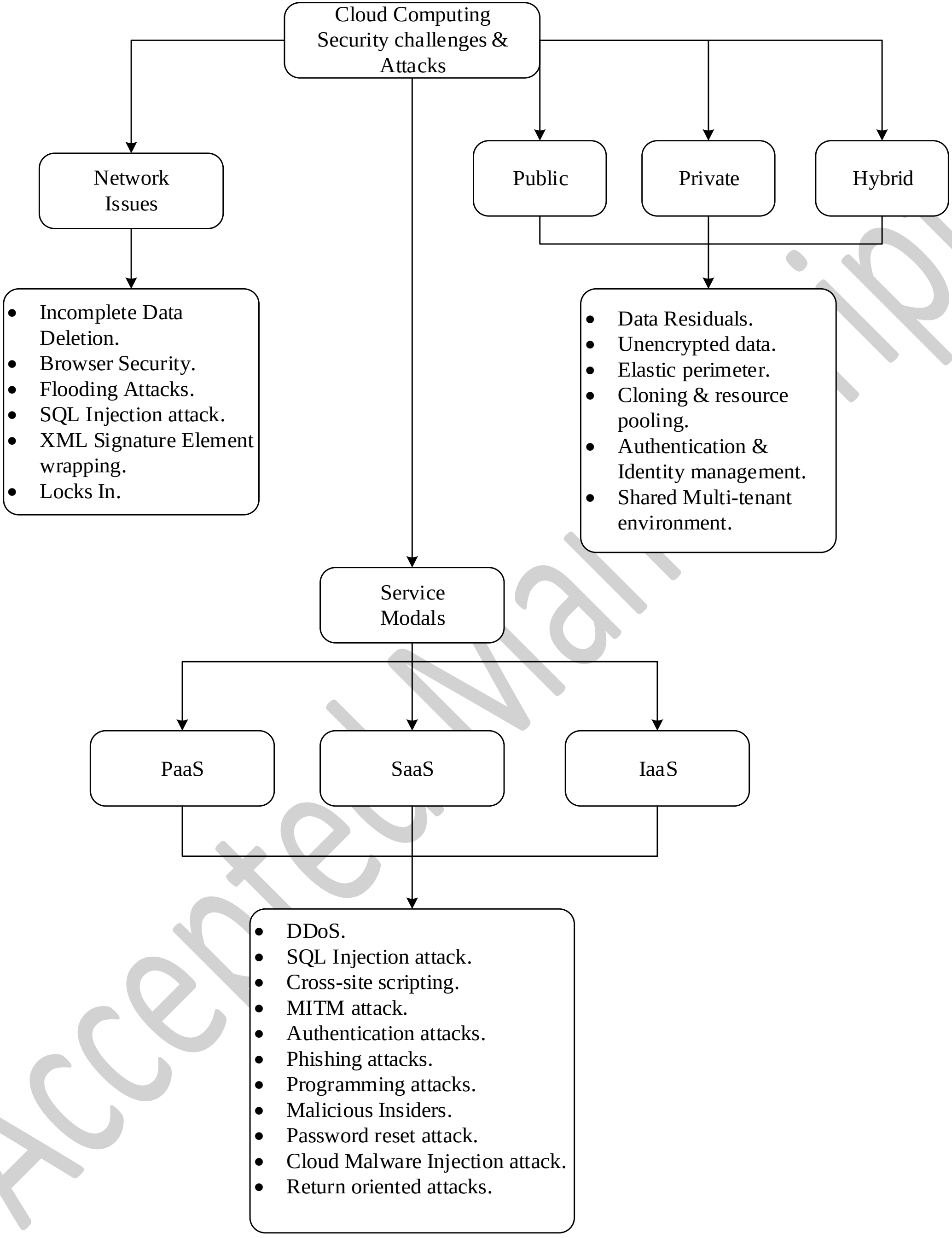

Figure 4: Cloud Computing Security attacks and challenges

[14] proposed a new decentralized, lightweight encrypted, Yugula cloud storage framework to preserve files' confidentiality, avoid central data replication, and boost blockchain completeness. Two approaches for data deduplication confidentiality files are discussed: one is using dual hacking and the other uses symmetrical encryption. The proposed architecture has been implemented and its implications for high transaction data output requirements to demonstrate reliability and usability for IoT data management in the cloud.

Shahzaib Tahir *et. al.* [15] Proposed a new privacy-preserving method to scan the keyword on the blockchain network for encrypted data. SE (Search Encryption) is studied for the first time over a licensed blockchain network, that is Hyperledger-

Accepted Manuscript

Fabric. The SE approach preserves confidentiality since it is focused on probabilistic trapdoors. Consequently, major protection and privacy benefits are assured by the system. The security review results in higher standards of security and privacy protections being guaranteed by the system.

[16] discussed that, one feature of Blockchain that is applied to hospital data is to use concepts of data division in chunks and the development of a connection between the chunks as a heritage of blockchain mechanics. The benefits of using this mechanism to secure patient reporting and how it increases trust in stored data have also been discussed.

Three stages of authentication using hash and anti-hash functions to resolve data security issues. Cloud end auto encryption-using RSA and AES hybrid cryptography framework or some other acceptable encryption tool. Due to auto encryption and three-step authentication, the proposed solution would provide extra protection, as if any hacker gets user credentials [17], he can enter the cloud environment, but he cannot access his files or data.

Jaideep Kaur Mudhar [18] The proposed Framework for secure Fog-enabled IoT devices access to user authentication was proposed for blockchain-based purposes. The proposed scheme utilizes the smart contract of Ethereum. We have built and tested our intelligent Remix-IDE Agreement in two test networks using Structural rigidity language, Test RPC and Rinkeby Test Network. Security vulnerabilities of the chain security analysis tool in our intelligent contract have also been investigated. This scheme is also secured against replays, threats, on- and off-chain interactions.

Caixia Yang *et. al.* [19] Proposed a blockchain-based system of privacy control called AuthPrivacyChain. Firstly, you use the account node address as the identifier in the blockchain when redefining the cloud access control authorization, which is encrypted and stored in the blockchain. We then create processes for access control, permission, and revocation authorization in AuthPrivacyChain. In addition, they are implementing AuthPrivacyChain based on the Enterprise Operating System (EOS). The results show that AuthPrivacyChain can prevent unauthorized access by hackers and administrators to resources and also to resources protect authorized privacy. Usage of this scheme only users with rights of access can access services. This approach, therefore, satisfies confidentiality, openness, accessibility, honesty, and accountability, preventing external users from attacking and preventing internal management from attacking.

A blockchain network, called cloud@blockchain, secures cloud computing services that benefit from the blockchain's privacy and immutability. The creation and anonymous file sharing and inspection of files improperly loaded are two functions on cloud@blockchain. Cloud users can access data on cloud@blockchain via smart contracts and identify all users in the app layer. It evaluated the performance of three different architectures: a pure blockchain and a hybrid blockchain. The results show the hybrid blockchain superiority over the pure blockchain and the traditional cache databases, which outperforms it respectively by 500% and 53.19% [20].

2.3. Comparative table

In this table, we analyze and compare different techniques and solutions. We also discuss the reliability, cost-effectiveness of well-known blockchain techniques and CIA i.e., confidentiality, integrity, availability.

[21] proposed a detailed survey that using blockchain to examine and compare different issues in the cloud environment and security problems. They further proposed a model in which, all data is transmitted inside the groups in file format, those files are encrypted using the AES algorithm and the integrity of the MD5 or SHA algorithm is maintained. To search for changes in the data being stored in the cloud storage, the MD5 or SHA algorithm is used. To provide safe data transfer and storage in the cloud, the individual user who makes changes can be eliminated. Furthermore, Blockchain increases the security challenges of cloud computing.

A decentralized, privacy-saving public auditing (DBPA) blockchain system in which a blockchain is an unpredictable source for (random) difficult data generation, and the auditor is expected to record the blockchain audit process. Users may publicly review the audit results because of the characteristics of the blockchain.

Accepted Manuscript

Table1. Comparative table of cloud security using blockchain techniques

Ref	Decentralized Service	Integrity	Availability	Confidentiality	Reliability	Cost-effective	Affected Technology				
							PoW	Ethereum	Permissioned BC	IPFS	Cryptography
[2]	✘	✓	✓	✘	✘	✓	✓	✘	✘	✘	✓
[1]	✘	✓	✓	✓	✓	✓	✓	✘	✓	✘	✘
[3]	✓	✓	✓	✓	✓	✘	✓	✓	✓	✘	✘
[4]	✘	✓	✓	✓	✓	✓	✓	✘	✓	✘	✓
[5]	✓	✓	✓	✘	✘	✘	✓	✓	✓	✓	✓
[6]	✓	✓	✓	✓	✓	✓	✘	✘	✘	✓	✓
[8]	✓	✓	✓	✓	✓	✓	✓	✘	✓	✓	✘
[9]	✓	✓	✓	✓	✘	✘	✘	✘	✓	✘	✓
[10]	✘	✓	✓	✘	✘	✘	✓	✘	✘	✓	✓
[11]	✘	✓	✓	✓	✓	✓	✓	✓	✘	✓	✘
[12]	✓	✓	✓	✓	✓	✓	✓	✘	✓	✓	✓
[13]	✘	✓	✓	✓	✓	✓	✓	✘	✓	✓	✓
[14]	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘
[15]	✓	✓	✓	✓	✓	✘	✘	✘	✓	✘	✓
[16]	✓	✓	✓	✓	✓	✓	✓	✓	✘	✓	✘
[17]	✘	✓	✓	✓	✓	✘	✓	✓	✘	✓	✘
[18]	✓	✓	✓	✓	✓	✘	✓	✓	✘	✓	✘
[19]	✓	✓	✓	✓	✓	✓	✘	✘	✓	✓	✓
[20]	✓	✓	✓	✓	✓	✘	✓	✓	✓	✘	✘
[21]	✘	✓	✓	✓	✓	✘	✓	✘	✓	✓	✘
[22]	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✓
[23]	✓	✓	✓	✓	✓	✓	✓	✘	✓	✘	✘
[24]	✓	✓	✓	✓	✓	✘	✓	✘	✓	✘	✘
[25]	✘	✘	✓	✘	✘	✓	✓	✓	✘	✓	✘
[26]	✓	✓	✘	✓	✓	✘	✓	✘	✓	✘	✘
[27]	✓	✓	✓	✘	✓	✘	✘	✘	✓	✓	✘

Furthermore, DBPA uses zero-knowledge proof during the audit process to protect users' privacy to prevent the CS reply data from discharging user data information [22]. Safety analysis and performance evaluation demonstrate that DBPA is safe and effective.

Keke Gai *et. al.* [23] investigated the recent efforts of clouds and blockchain in technical fusion. In this work, approximately three technical dimensions are discussed. First, they discussed the service model and analyze an evolving Blockchain-as-a-Service (BaaS) cloud-relevant blockchain service model; second, Protection is regarded in this work as a crucial technical dimension, and access control and searchable encryption systems are assessed; finally, we analyze the efficacy of the cloud data center with support/participation for hardware and software blockchain.

The main findings of this work are a theoretical reference for potential work in the field of blockchain-enabled cloud reengineering.

[24] Proposes a stable collaborative model of smart contracting information, consisting of the three types of participants, including the owners of data, miners, and third parties. These participants can generally acquire and store data sharing through their private or public clouds. We analyze the topological relationships between stakeholders in the distribution mechanism and create some Single valued models from simple to complex. They also assess the motivational effects of exchanging security data and the rationality of the proposed solution by reviewing delivery legislation.

In order to develop a cost-benefit relationship, available models were suggested and evaluated for blockchain supplies of cloud computing infrastructure and their respective operating costs. We provide two case studies that consider blockchain implementation over a simple framework and three other complementary alternatives to demonstrate the feasibility of these models [25].

E. Angelin Kanimozhi *et. al.* [26] Suggested blockchain integration architecture and job model in cloud storage. The suggested model has been tested and proven efficient by comparison with the existing protocols with respect to costs and times. This can be applied in the future to obtain other data security properties, too. In the upcoming study, data recovery may also be discussed. The architecture proposed would be suitable for all immutable documents, such as the data of a government regarding its people. In order to allow data modifications, this design can be further changed, so that it fits potential muable data storage.

[27] Blockchain, which facilitates the audits between tenants and cloud providers, has implemented clear integrity in the log transactions. They also introduce the intelligent contract to simulate the allocation process, policy management, and other functions between cloud providers and citizens, so that the cloud computing platform of Blockchain can be easily integrated. Our expected result is that cloud computing can be applied on Blockchain along with other functional features of cloud computing. Besides Blockchain, Smart Contract is used to monitor data transactions and also to help integrate Cloud computing into the Blockchain network via a truffle framework. The underlying mechanisms and efficiency in terms of the average deployment time have been defined in this paper.

2.4. Blockchain-based Security Solutions

The following taxonomy diagrams (Fig.5.1 & Fig.5.2) show different blockchain-based security solutions of cloud computing i.e., PoW, CEM, Ethereum, PDP, Hashing, IPFS, hybrid encryption techniques, and Remix-IDE. Furthermore, it shows the contributions of different cloud-based solutions i.e., CIA, reliability, verification of data, authenticity, cost-effectiveness, high performance, trust enhancement, management of critical deadlocks, functional solutions, enhancement of data security, validity, and complexity.

Accepted Manuscript

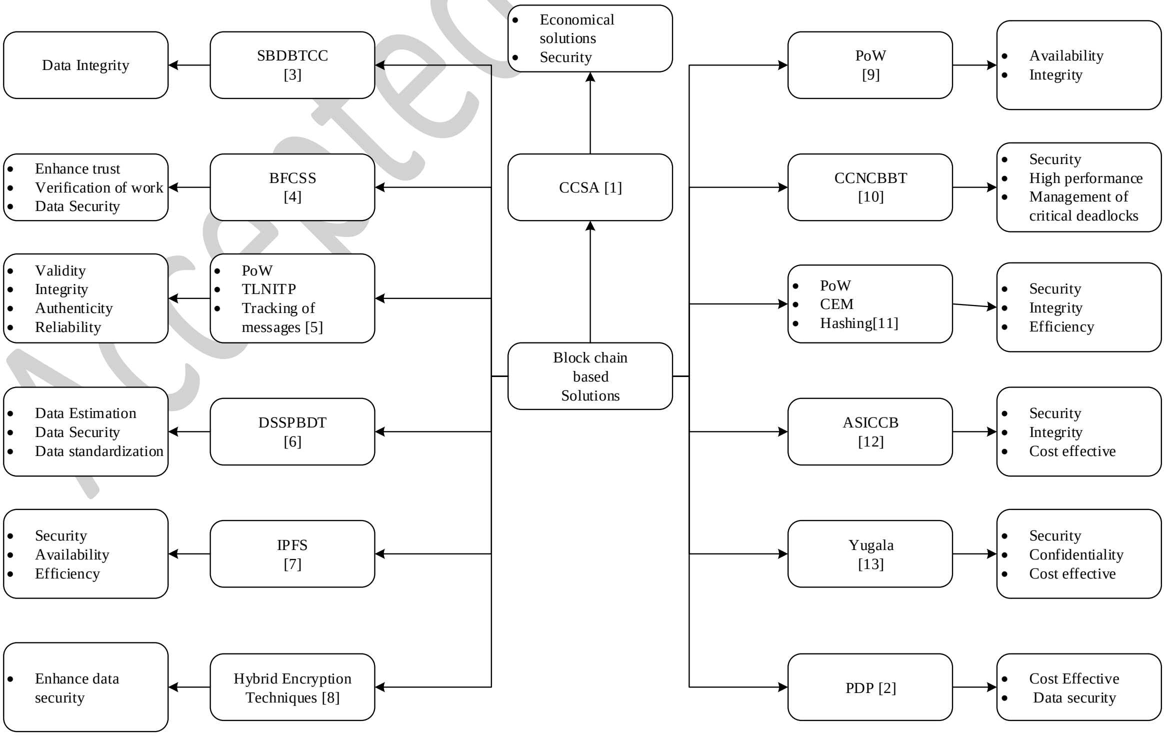

Figure 5: Blockchain-based security solutions

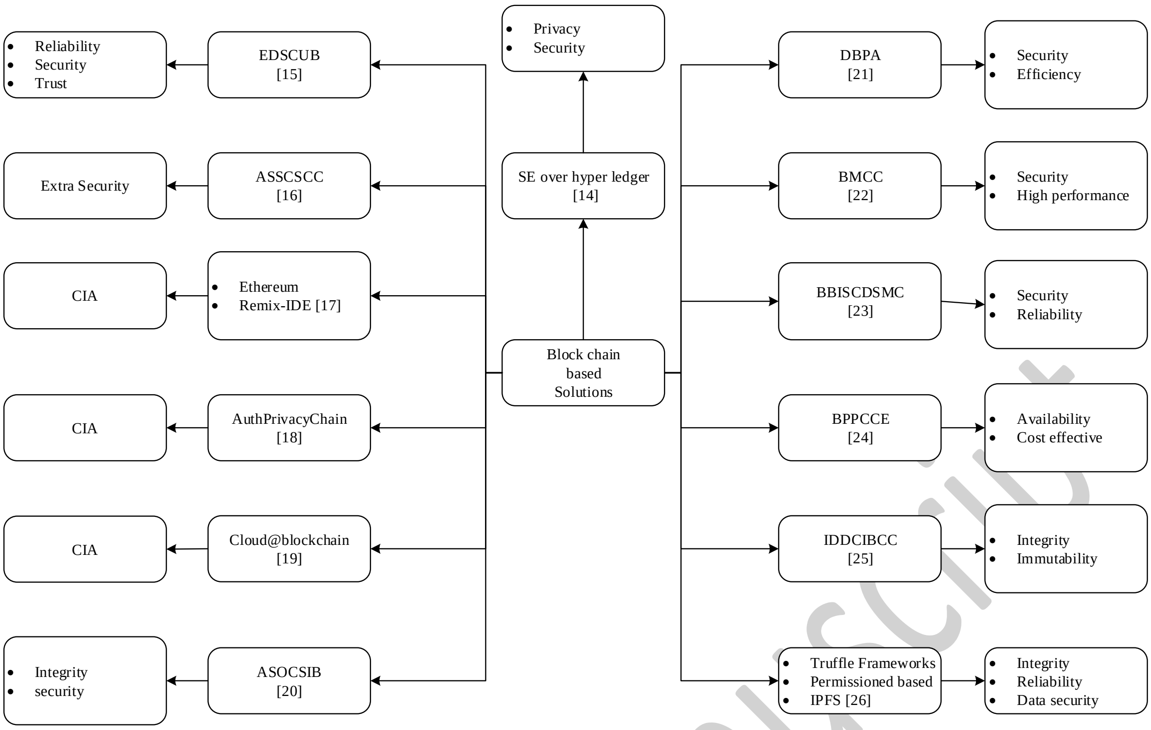

Figure 6: Blockchain-based security solutions

2.5. Benefits of Blockchain technology in Cloud computing [28]

One of the most troubling trends in the increasingly emerging use of blockchain in cloud computing. Most companies use cloud storage and use cloud technology. The opportunities to disrupt whole sectors as blockchain power is used for the mix. Most media interest is collected by crypto-monetary, rendered with blockchain technology. But blockchain technology is much more important in practice in cloud computing because of the ability to transform vast amounts of cost-efficient and stable data processing as well as documentary power.

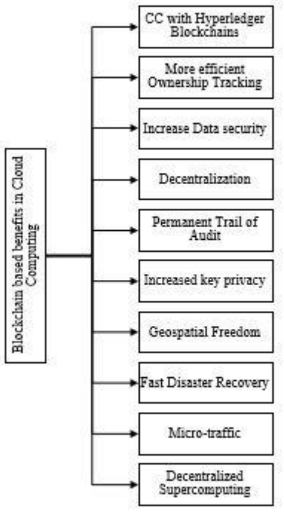
Blockchain based benefits in Cloud Computing
CC with Hyperledger Blockchains
More efficient Ownership Tracking
Increase Data security
Decentralization
Permanent Trail of Audit
Increased key privacy
Geospatial Freedom
Fast Disaster Recovery
Micro-traffic
Decentralized Supercomputing

Figure 7: Cloud computing benefits from the use of Blockchain

3. FINDINGS

3.1. Comparison of Consensus Algorithms

Consensus is the cornerstone of a blockchain and therefore, an optional method called mining decentralizes power. The consensus algorithm is also controlled by the form of blockchain used; that is, not all consensus mechanisms are appropriate for all blockchains. For instance, in publicly unauthorized blockchains, it would make sense to use PoW instead of a simple agreement process that could be based on evidence of authority [31]. Consequently, a suitable consensus algorithm for a specific blockchain project is necessary.

Both consensus mechanisms are designed to resolve flaws in a distributed system and help the distributed systems achieve a final consensus [32]. These groups address all sorts of defects (fail-stop type or arbitrary).

A decision-making process based on consensus is an attempt in which affected parties (stakeholders) aim to find agreement on a course of action to tackle a problem or collection of related issues. The stakeholders work together in a consensus process to find a solution that is mutually acceptable [33].

We have compared different most well-known consensus algorithms based on the security parameters in Table.2.

Accepted Manuscript

Table2. Comparison of different consensus algorithms w.r.t security parameters [31] [34] .

Consensus Algorithms	**Parameters**				
	Adversary Tolerance model	**Prone to Attacks**	**Secure against Attacks**	**Energy Consumption**	**Consensus Finality**
ELASTICO	Faulty processes may have up to 1/4 of the machine power	Double attack on spend	-	-	Absolute/immediate irreversibility
Implicit Consensus	Defective process number ≤ process number/3	DDoS attack	-	-	Absolute
Leader-Free Byzantine consensus	Defective process number < process number/3	-	Sybil attack	-	Probabilistic
PoT (Proof of Trust)	n≥ 3b+1 where; n is the number of nodes and b is the number of Byzantine nodes	DDoS attack	Collusion & Sybil attack	-	Probabilistic
DBFT (Delegated Byzantine Fault Tolerance)	-	-	-	-	Probabilistic
PoPF (Proof of Participation & Fees)	No node may possess over 50% of computational capacity.	-	51% attack	Lower energy intake than PoW.	Absolute
Ripple	False processes! = (processes-1)/5	Sybil & DDoS attack	-	-	Probabilistic
PoW (Proof of Work)	No node may possess over 50% of computational capacity.	Sybil, DDoS, Bribe & Selfish mining attack	-	Electricity Consumption up to 538 KWh	Probabilistic
PoV (Proof of Vote)	Incorrect processes! 50% of processes	-	-	-	Probabilistic

Accepted Manuscript

3.2. Growth of Cloud Computing

The percentage of global cloud-dedicated IT spending continues to accelerate in 2021. Gartner, the research and consultancy company headquartered in Stamford, Conn, focuses on initiatives that bring end-users global public cloud spending to $304.9 billion (18 percent next year), up from $257.5 billion this year [35].

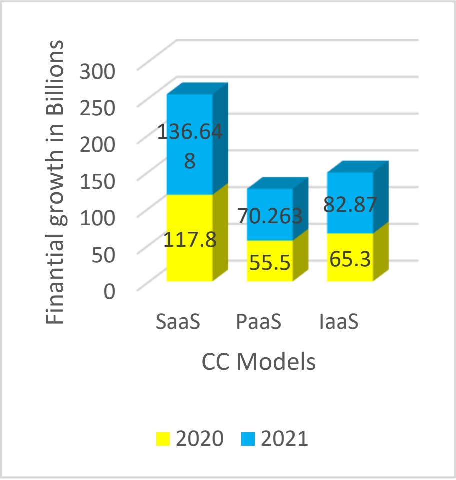

Figure 8: Growth of CC Worldwide

3.3. Impact of COVID-19 on Cloud Computing Market

The global cloud protection market is projected to increase from USD 34.5 trillion in 2020 to USD 68.5 trillion in 2025 in the post-COVID-19 scenario, to a CAGR of 14.7 percent over the projected period. The numbers of security breaches have supported the growth in the Business ecosystem Security Cloud and cyber-attacks and requirements to respect legislation and data protection [36].

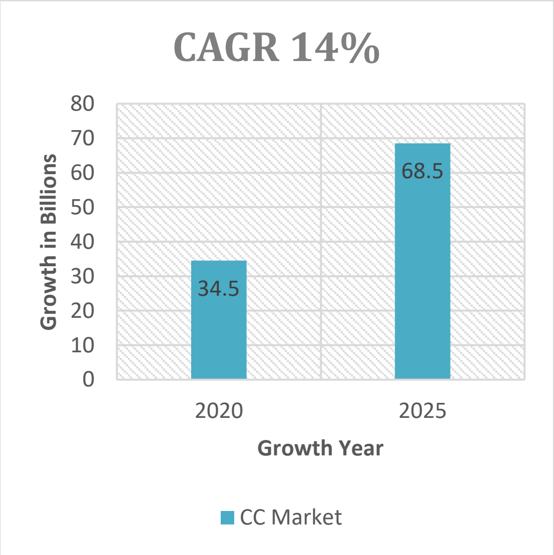

Figure 9: CC Market Worldwide due to COVID-19

4. FUTURE WORKS

4.1. Use Cases of Blockchain in Cybersecurity

Though not unbreakable, blockchain has grown into one of the dumbest types of digital network transactions. The technology has been credited as designed and planned for its information integrity assurance. Many industries will benefit from it if well-used. Blockchain can be applied in many applications with the ability to be functional for many purposes. One of the strongest applications will be the incorporation of cybersecurity solutions with many other technologies. Below are several cases of the potential use of blockchain to improve cybersecurity

4.2. Private Messaging Security

More and more people enter social media with the internet shrinking the planet into a virtual village. There is also a growing number of social media sites. More social applications are launched every morning, as conversational business becomes more popular. During these encounters, large quantities of metadata are obtained. Most users on the social media site protect services and their data with poor passwords. Many messaging companies warm up to blockchain to secure username data as a superior alternative for their existing end-to-end encryption. A basic security protocol can be built using Blockchain. Blockchain can be used to create a centralized API system to allow cross-messenger communication capabilities.

Recent attacks on social media such as Twitter and Facebook have been numerous. These attacks lead to privacy violations with millions of accounts broken and user details in the wrong hands. Blockchain technology will deter potential cyber-attacks if well applied in these messaging networks.

4.3. IoT Security

Hackers use edge devices, such as thermostats and routers, increasingly to gain access to networks in general. With the current fascination with artificial intelligence (AI) hackers have been made easier to access overall systems such as home automation through edge devices such as "smart" switches. Many of these IoT devices have sketchy security features in most situations [51].

In this event, blockchain can be used by decentralizing their administration to protect these overall systems or devices. The method would allow the system the opportunity to make safety decisions on its own. By decentralizing such systems, blockchain ensures that such attacks are more difficult to execute (if even possible).

4.4. DNS & DDoS Security

Distributed Denial of Service (DDoS) is an attack if a user is refused access to a destination resource or service, such as a network resource, server, or website. These attacks shut down resource networks or slow them down.

On the other hand, a very centralized Domain Name System (DNS) makes it a great target for hackers who penetrate the connection between the IP address and the website name. This attack makes a website unavailable, inexpensive, and even redirected to other scam websites.

Fortunately, blockchain can be used for the decentralization of the DNS entries to reduce such attacks. Blockchain would have replaced the insecure single points abused by hackers with decentralized solutions.

4.5. Storage of Decentralising Medium

The hacks and theft of business data are becoming a significant cause of concern for organizations. Most businesses do use the centralized storage method. A hacker needs only one weak point to access the entire data contained in these systems. Such an assault leaves sensitive and confidential information in the hands of a perpetrator, such as company finances.

Blockchain can secure confidential data by ensuring a decentralized data storage form. This mitigation approach would make the penetration of data storage systems harder and even difficult for hackers. Many

Accepted Manuscript

storage companies are evaluating ways that blockchain can secure data from hackers. Apollo Currency Team is a clear example of an enterprise that is already using the blockchain framework (The Apollo Data Cloud).

4.6. Data Transmission Protection

In the future, Blockchain can be used to avoid unauthorized access to data during transit. Data transmission can be ensured using the full encryption function of the technology to prevent malicious actors from getting access to it, whether it's an entity or an organization. This approach would lead to a general increase in the trust and integrity of blockchain data. Malicious intent hackers tap data in transit to either change or erase its presence. This leaves a big difference in unreliable channels of communication, such as emails.

4.7. Reduce the protection of human beings due to cyber-attacks

We have recently seen the deployment of unmanned military vehicles and public transport due to ground-breaking technical advances. Data transfers from sensors to remote control databases are facilitated via these automated vehicles and weapons via the Internet. However, hackers were trying to disrupt and gain access to networks, such as the Car Area Network (CAN). When taped, these networks have full control access to the hackers' critical automotive functions. Such incidents will have a direct effect on human protection. However, several adversities would be prevented through data verification performed on blockchain for any data which passes through and into those systems.

4.8. Blockchain: The Future of Cloud Computing

Cloud computing based on Blockchain not only decentralizes data storage. This technology is used more than ever as part of data logistics platforms. Many approved users can access the data at the same time, communicating, interpreting, and modifying it according to their wishes. This type of cloud computing solution enables workers to analyze and manage knowledge virtually and safely [37].

The use of blockchain also allows the virtualization of contractual transactions and other exchanges, resulting in a significant increase in consumption across many industries.

Blockchain is going to take over cloud computing in the future as Blockchain will certainly ensure information security. The data stored in blockchain are completely centralized since it is stored in several nodes worldwide, rather than at just one location. This addresses the problem of data security in the event of a mistake in storing information.

The files uploaded on the blockchain are not managed or accessible by any entity. Furthermore, any party that holds the information has a key for accessing the encrypted data.

And even though anyone can access your file, it is a partial file that the person who can access it is unhelpful. It is extremely likely that blockchain technology will take over [38].

4.9. Attractive Blockchain business growth opportunities

Blockchain's worldwide market size is estimated at an astounding 67.3 percent annual growth rate of Compound (CAGR) by 2020, from 3.0 billion US dollars by 2020 to 39.7 billion US dollars by 2025. The growing need to optimize business operations and supply chain management applications with Blockchain technology is driving the entire Blockchain industry [29].

- It is projected that the global blockchain market will hit USD 3.0 billion by 2020 and that it will reach USD 39.7 trillion by 2025.
- The rising demand is due to the growing number of venture financing and Blockchain technology investment and the increased popularity of Blockchain technologies in retail and supply chain management.
  Emerging market global expansion and large-scale blockchain technology deployment provide important market opportunities.

Accepted Manuscript

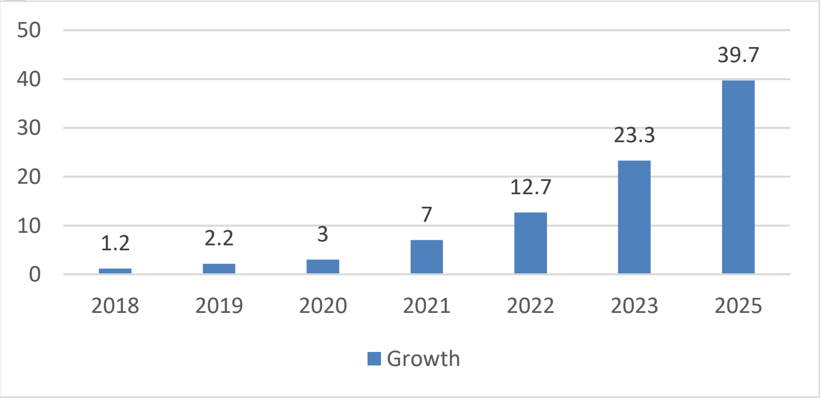

Figure 10: Attractive Blockchain business growth opportunities obtained from [30]

5. CONCLUSION

The key points addressed in this report are security problems and privacy. In this report, the convenient solutions available are also discussed. In addition, we explored the comparative study of various consensus algorithms for blockchain and suggested the best ones. We may therefore conclude that the security vulnerabilities must be minimized, and the blockchain methods must be strengthened to boost the Cloud Storage service. We have also discussed the growth rate of Cloud Computing model wise and CAGR (Compound Annual Growth Rate) of Cloud Computing and COVID-19 impact on annual growth of cloud computing till 2025, and we have concluded that growth of Cloud Computing will increase up to 14% till 2025. As blockchain is decentralized technology and has many benefits, it is possible that blockchain may take over cloud computing in the future.

REFERENCES

[1] A. Markandey, P. Dhamdhere, and Y. Gajmal, "Data access security in cloud computing: A review," *2018 Int. Conf. Comput. Power Commun. Technol. GUCON 2018*, pp. 633–636, 2019, doi: 10.1109/GUCON.2018.8675033.

[2] M. R. Bhaskar, K. Patidar, and R. Kushwah, "Cloud computing security: a review," *Accent. Trans. Inf. Secur.*, vol. 3, no. 12, pp. 36–39, 2018, doi: 10.19101/tis.2018.311002.

[3] X. Zhou, P. Lin, Z. Li, Y. Wang, W. Tan, and M. Huang, "Security of big data based on the technology of cloud computing," *Proc. - 2019 4th Int. Conf. Mech. Control Comput. Eng. ICMCCE 2019*, pp. 703–706, 2019, doi: 10.1109/ICMCCE48743.2019.00163.

[4] A. Mughal and A. Joseph, "Blockchain for Cloud Storage Security: A Review," *Proc. Int. Conf. Intell. Comput. Control Syst. ICICCS 2020*, no. Iciccs, pp. 1163–1169, 2020, doi: 10.1109/ICICCS48265.2020.9120930.

[5] S. Showkat and S. Qureshi, "Securing the internet of things using blockchain," *Proc. Conflu. 2020 - 10th Int. Conf. Cloud Comput. Data Sci. Eng.*, pp. 540–545, 2020, doi: 10.1109/Confluence47617.2020.9058258.

[6] W. Wang, "*Data Security of SaaS Platform based on Blockchain and Decentralized Technology*," *Proc. 5th Int. Conf. Inven. Comput. Technol. ICICT 2020*, pp. 848–851, 2020, doi: 10.1109/ICICT48043.2020.9112421.

[7] D. Dalton and L. Kehoe, "*Written by the Deloitte EMEA Grid Blockchain Lab with insights from Deloitte global cyber SMEs from members firms including For more information please contact*." Accessed: Dec. 24, 2020. [Online]. Available: http://uk.businessinsider.com/world-economic-forum-potential-of-blockchain-in-financial-services-2016.

[8] M. Shah, M. Shaikh, V. Mishra, and G. Tuscano, "Decentralized Cloud Storage Using Blockchain," *Proc. 4th Int. Conf. Trends Electron. Informatics, ICOEI 2020*, no. Icoei, pp. 384–389, 2020, doi: 10.1109/ICOEI48184.2020.9143004.

[9] Y. Sharma, H. Gupta, and S. K. Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing," *Proc. - 2019 Amity Int. Conf. Artif. Intell. AICAI 2019*, pp. 898–902, 2019, doi: 10.1109/AICAI.2019.8701398.

[10] S. G. Sharma, L. Ahuja, and D. P. Goyal, "Building Secure Infrastructure for Cloud Computing Using Blockchain," *Proc. 2nd Int. Conf. Intell. Comput. Control Syst. ICICCS 2018*, no. Iciccs, pp. 1985–1988, 2019, doi: 10.1109/ICCONS.2018.8663145.

[11] A. Ben Lazreg, A. Ben Arbia, and H. Youssef, "Cloudlet-Cloud Network Communication Based on Blockchain Technology," *Int. Conf. Inf. Netw.*, vol. 2020-Janua, pp. 164–169, 2020, doi: 10.1109/ICOIN48656.2020.9016592.

[12] S. Prianga, R. Sagana, and E. Sharon, "Evolutionary Survey on Data Security in Cloud Computing Using Blockchain," *2018 IEEE Int. Conf. Syst. Comput. Autom. Networking, ICSCA 2018*, pp. 1–6, 2018, doi: 10.1109/ICSCAN.2018.8541258.

[13] Murthy, Ch VNU Bharathi, and M. Lawanya Shri, "A Survey on Integrating Cloud Computing with Blockchain," *Int. Conf. Emerg. Trends Inf. Technol. Eng. ic-ETITE 2020*, pp. 1–6, 2020, doi: 10.1109/ic-ETITE47903.2020.470.

[14] S. P. Gochhayat, E. Bandara, S. Shetty, and P. Foytik, "Yugala: Blockchain based encrypted cloud storage for IoT data," *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 483–489, 2019, doi: 10.1109/Blockchain.2019.00073.

[15] S. Tahir and M. Rajarajan, "*Privacy-Preserving Searchable Encryption Framework for Permissioned Blockchain Networks*," Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree, pp. 1628–1633, 2018, doi: 10.1109/Cybermatics_2018.2018.00272.

[16] D. Yadav, A. Shinde, A. Nair, Y. Patil, and S. Kanchan, "E*nhancing Data Security in Cloud Using Blockchain*," Proc. Int. Conf. Intell. Comput. Control Syst. ICICCS 2020, no. Iciccs, pp. 753–757, 2020, doi: 10.1109/ICICCS48265.2020.9121109.

[17] S. M. J. Islam, Z. H. Chaudhury, and S. Islam, "A Simple and Secured Cryptography System of Cloud Computing," *2019 IEEE Can. Conf. Electr. Comput. Eng. CCECE 2019*, pp. 1–3, 2019, doi: 10.1109/CCECE.2019.8861845.

Accepted Manuscript

[18] J. K. Mudhar, S. Kalra, and J. Malhotra, “*An Efficient Blockchain Based Authentication Scheme to Secure Fog Enabled IoT Devices,” Indo - Taiwan 2nd Int. Conf. Comput. Anal. Networks, Indo-Taiwan ICAN 2020 - Proc.*, pp. 75–80, 2020, doi: 10.1109/Indo-TaiwanICAN48429.2020.9181356.

[19] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, “*AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud*,” *IEEE Access*, vol. 8, pp. 70604–70615, 2020, doi: 10.1109/ACCESS.2020.2985762.

[20] W. Y. Tsai, T. C. Chou, J. L. Chen, Y. W. Ma, and C. J. Huang, “*Blockchain as a Platform for Secure Cloud Computing Services*,” *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2020, pp. 155–158, 2020, doi: 10.23919/ICACT48636.2020.9061435.

[21] M. Popli and Gagandeep, “A survey on cloud security issues and challenges,” *Proc. 2019 6th Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2019*, pp. 230–235, 2019.

[22] Y. Miao, Q. Huang, M. Xiao, and H. Li, “*Decentralized and Privacy-Preserving Public Auditing for Cloud Storage Based on Blockchain*,” *IEEE Access*, vol. 8, pp. 139813–139826, 2020, doi: 10.1109/ACCESS.2020.3013153.

[23] K. Gai, J. Guo, L. Zhu, and S. Yu, “*Blockchain Meets Cloud Computing: A Survey*,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 2009–2030, 2020, doi: 10.1109/COMST.2020.2989392.

[24] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, “*Blockchain-based incentives for secure and collaborative data sharing in multiple clouds*,” *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1229–1241, 2020, doi: 10.1109/JSAC.2020.2986619.

[25] C. Melo, J. Dantas, R. MacIel, P. Pereira, E. Quesado, and P. MacIel, “*Blockchain provisioning over private cloud computing environments: Availability modeling and cost requirements*,” *Proceeding 2019 IEEE 8th Int. Conf. Cloud Networking, CloudNet 2019*, no. 2, pp. 1–3, 2019, doi: 10.1109/CloudNet47604.2019.9064125.

[26] E. A. Kanimozhi, M. Suguna, and S. Mercy Shalini, “Immediate Detection of Data Corruption by Integrating Blockchain in Cloud Computing,” *Proc. - Int. Conf. Vis. Towar. Emerg. Trends Commun. Networking, ViTECoN 2019*, pp. 1–4, 2019, doi: 10.1109/ViTECoN.2019.8899394.

[27] V. Reantongcome, V. Visoottiviseth, W. Sawangphol, A. Khurat, S. Kashihara, and D. Fall, “S*ecuring and Trustworthy Blockchain-based Multi-Tenant Cloud Computing*,” *ISCAIE 2020 - IEEE 10th Symp. Comput. Appl. Ind. Electron.*, pp. 256–261, 2020, doi: 10.1109/ISCAIE47305.2020.9108796.

[28] Danni White,“Top 10 Benefits of Blockchain Technology in Cloud Computing in 2020.”[Online]. Avaliable:https://www.techfunnel.com/information-technology/benefits-of-blockchain-in-cloud-computing/ [Accessed Dec. 25, 2020].

[29] Sandeep Sugla,“Blockchain Market Size, Growth, Trends and Forecast to 2025 | MarketsandMarkets.” [Online],Avaliable:https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html [Accessed Dec. 24, 2020].

[30] Hadley Ward,“Global market for blockchain technology20182025|Statista.”[Online],Avaliable:https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/ [Accessed Dec. 25, 2020].

[31] Packhub,“Consensus - Mastering Blockchain - SecondEdition.”,[Online],Avaliable:https://subscription.packtpub.com/book/data/9781788839044/1/ch01lvl1sec14/consensus [Accessed Dec. 25, 2020].

[32]Packhub,“Summary - Mastering Blockchain - SecondEdition.”,[Online],Avaliable:https://subscription.packtpub.com/book/data/9781788839044/1/ch01lvl1sec16/summary [Accessed Dec. 25, 2020].

[33] Wu, Zhibin, and Jiuping Xu, "A consistency and consensus based decision support model for group decision making with multiplicative preference relations.",*Consensus-Based Decision-Making Processes*, vol. 52, issue 3, pp.757-767, 2012.

[34] N. Chaudhry and M. M. Yousaf, “*Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities,*” *ICOSST 2018 - 2018 Int. Conf. Open Source Syst. Technol. Proc.*, no. December, pp. 54–63, 2019, doi: 10.1109/ICOSST.2018.8632190.

[35] Doona Goddison,“10 Future Cloud Computing Trends To Watch In 2021.”[Online] Avaliable: https://www.crn.com/news/cloud/10-future-cloud-computing-trends-to-watch-in-2021 [Accessed Dec. 25, 2020].

[36] Cision,“Global Cloud Security Market Assessment Report 2020-2025: Drivers, Opportunities, Restraints and Challenges Resulting from COVID-19.”[Online],Avaliable:https://www.prnewswire.com/news-releases/global-cloud-security-market-assessment-report-2020-2025-drivers-opportunities-restraints-and-challenges-resulting-from-covid-19-301116347.html [Accessed Dec. 25, 2020].

[37] “The Future of the Blockchain & Cloud Computing | Quisitive | Quisitive.”[Online], Avaliable: https://quisitive.com/the-future-of-the-blockchain-and-cloud-computing/ [Accessed Dec. 25, 2020].

[38] Harsh Arora,“The Future of Cloud Computing: Blockchain Will Have Its Day - DATAVERSITY.[Online]Avaliable:”https://www.dataversity.net/the-future-of-cloud-computing-blockchain-will-have-its-day/# [Accessed Dec. 25,

Accepted Manuscript

2020].

[39] Ashraf, M. Usman, Eassa FA, Albeshri AA, Algarni A. "*Performance and power efficient massive parallel computational model for HPC heterogeneous exascale systems.*" IEEE Access 6, pp. 23095-23107, 2018.

[40] Ashraf, Muhammad Usman, Rida Qayyum, and Hina Ejaz. " *State-of-the-Art, Challenges: Privacy Provisioning in TTP Location Based Services Systems*." International Journal of Advanced Research in Computer Science (IJARCS) vol 10, issue 2, pp. 68-75, 2019.

[41] Fatima, Fariha, Saqib Ali, and Muhammad Usman Ashraf. "*Risk Reduction Activities Identification in Software Component Integration for Component Based Software Development (CBSD).*" International Journal of Modern Education and Computer Science vol 9, issue 4, pp. 19, 2017.

[42] Siddiqui, Nasir, et al. "*A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field.*" Plos one vol 15, issue 11, pp. e0241890 ,2020.

[43] Javed, Rushba, Sidra Anwar, Khadija Bibi, M. Usman Ashraf, and Samia Siddique. "*Prediction and monitoring agents using weblogs for improved disaster recovery in cloud.*" Int. J. Inf. Technol. Comput. Sci.(IJITCS) Vol,11, issue 4, pp. 09-17 2019.

[44] Ashraf, Muhammad Usman, Muhammad Usman, Sabah Arif, Abdul Basit, and Malik Sheraaz Khan, "*Provisioning quality of service for multimedia applications in cloud computing.*" Int. J. Inf. Technol. Comput. Sci.(IJITCS) , vol.10, issue 5, pp. 40-47 2018.

[45] Tariq, Saman. "*Measuring the Impact of Scope Changes on Project Plan Using EVM*." IEEE Access 8 2020.

[46] Alsubhi, Khalid, M. Usman Ashraf, and Iqra Ilyas. "*HBLP: A Privacy Protection Framework for TIP Attributes in NTTP-Based LBS Systems*." IEEE Access 8 ,2020.

[47] Alrahhal, Mohamad Shady, "*AES-route server model for location based services in road networks.*" International Journal Of Advanced Computer Science And Applications vol 8, issue 8, pp. 361-368, 2017.

[48] Riaz, Shamsa, M. Usman Ashraf, and Ahmer Siddiq. *"A Comparative Study of Big Data Tools and Deployment PIatforms*." 2020 International Conference on Engineering and Emerging Technologies (ICEET). IEEE, 2020.

[49] Alsubhi, Khalid, et al. "*MEACC: an energy-efficient framework for smart devices using cloud computing systems.*" Frontiers of Information Technology & Electronic Engineering vol. 21, issue 6 ,2020.

[50] Abid, Usra, and M. Usman Ashraf. "A Critical Survey On Privacy Prevelling In Collaborative Filtring Recomender System: Challenges, State-Of-The-Art Methods And Future Directions." 2020 International Conference on Engineering and Emerging Technologies (ICEET). IEEE, 2020.

[51] Manzoor, Anam, Waqar Ahmad, Muhammad Ehatisham-ul-Haq, Abdul Hannan, Muhammad Asif Khan, M. Usman Ashraf, Ahmed M. Alghamdi, and Ahmed S. Alfakeeh,"*Inferring Emotion Tags from Object Images Using Convolutional Neural Network*." Applied Sciences vol. 10, issue 15, pp. 5333, 2020.

[52] Alsubhi, K.. "*A Tool for Translating sequential source code to parallel code written in C++ and OpenACC*." 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2019.

Accepted Manuscript