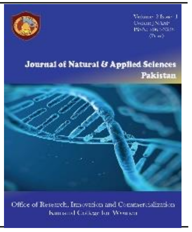
Contents lists available http://www.kinnaird.edu.pk/

Journal of Natural and Applied Sciences Pakistan

Journal homepage: http://jnasp.kinnaird.edu.pk/



REINVENTING CLOUD STORAGE USING THE BLOCKCHAIN

Sidra Anwar[1], Jannat Shehzadi[1], Momna Mir[1], Zummer Zulfiqar[1*]
[1]Department of Computer Science, GC Women University Sialkot, Pakistan

Article Info

*Corresponding Author
Email: zummerzulfiqar12@gmail.com

Keywords
Cloud Computing, Cloud Storage, Blockchain, Privacy Policy, Encryption, Symmetric key, Non-Symmetric key, Data Security

Abstract

Cloud storage is an environment in which data is stored and people access their data from any location through internet. It facilitates the users, instead of purchasing the hardware which is quite costly, to store their data on cloud storage. Here we found some hazards in cloud storage infrastructure in which security and privacy are the major concerns of cloud's nature because these issues will reduce the growth of cloud. So cloud users must understand and vigilant about the risk of data breaches in this environment. Besides this, the existing solutions for the security are highly considered for analysis. Although, security and privacy of data is of utmost important to all of its users regardless of the nature of the data being stored. In public cloud, people don't trust on the involvement of third party because there is a peril of data leakage and data integrity. The purpose of this paper is to achieve data security of cloud storage and to formulate corresponding cloud storage security policy. To solve the obstacles associated to data privacy and security, some techniques of block-chain apply on cloud which maintains the integrity of data and make their storage more reliable and secure for cloud users. So that, they store their data on cloud's storage without any reluctance.

1. Introduction

The cloud computing has been broadly implemented to manage data storage and on requirement figure out. It's a structure that permits adaptable entry to a shared pool of configurable registration resources on request (e.g. grids, databases, stockpile, maintenance and software) that could be quickly distributed and discharged with slight control or intervention by maintenance provider. Cloud computing acts as pronounced tasks for the business world nowadays which offers pooled processing resources. Information becomes an essential component of cloud computing in recent times.

Term information in the long run seeks its privacy and security issue. The necessity of data storage has been greater than before with the rise of new innovations. Cloud storage is developed due to the immense rise in the datasets.

The advantage of cloud computing includes reduced cost, re-provisioning of resources etc (Jayapandian *et al*, 2017). Cloud storage has become one of the illustrations of data storage with the evolution of cloud computing in recent times. Cloud storage system manages information stockpiling and administration functions via group application, grid innovation, and distributed record framework that gathers various data storage devices to work together via application programs. Cloud storage is usually known for its centralized system (Takabi *et al*, 2010). Records can be stored remotely via cloud storage and can benefit from high-quality on-demand applications and services from a shared pool of configurable computing resources without the local data storage and maintenance burden.

There have been more and more malicious attacks on cloud storage systems in recent years, and cloud storage of data leakage has also occurred frequently. The security of cloud storage involves the safety and privacy of the user's data. In order to safeguard privacy and integrity, users can not monitor information security (Zhe *et al*, 2017). With their data accessibility rates, centralized cloud storage hosts are vulnerable to third parties as per their anti-privacy laws and are prone to losing, changing, or manipulating the information their users hold.

In fact, centralized cloud storage providers are a single point of hack failure that has and will continue to cause major data leakage in the private data of users. Also, there are no means to trace the exact alteration, deletion or spying arise at any point in time. In the centralized framework, the cloud controller manages the storage structure and is managed with cloud controller's central server. All hosts are reserved for storing pictures, data and records with only one storage system (Liang *et al*, 2017). Also in the centralized system, users must trust a central entity, which can effectively exercise control over them. The information can be modified without the permission of the holder in the cloud. Therefore, it is important not only to protect cloud data, but also to ensure the integrity and accuracy of data (Pasupulati *et al*, 2016). The data is questionable in case of safety and security, and information is an important factor in this age, both for single users and for huge organizations.

The virtual infrastructure called Cloud Computing was implemented to overcome the data center's major shortcomings. It is a methodology that stores the data in the cloud, a virtual storage space. Encryption and Decryption are the major techniques of cloud for providing security and privacy to confidential data (Prianga *et al*, 2018). Besides, the existing cloud model is highly successful but there are some privacy issues when cloud information is being processed, which is why cloud users are reluctant to store their confidential and sensitive data in the cloud. Cloud computing also poses new and challenging security threats to outsourced data by users (Wang *et al*, 2013). So, upcoming generation of platforms plans to overcome those challenges by attempting some cryptography on cloud infrastructure through block chain techniques.

Each node participates in the network for the provision of services in decentralized architecture, thus providing better efficiency due to the distributed characteristics of the block chain (Pasupulati *et al*, 2016), availability is also guaranteed. With cloud data provenance service based on block chain, all data operations are recorded in a transparent and permanent manner. Therefore, the trust between users and cloud service providers can be easily created. Securing data in the cloud, cryptography has played a major role (Prianga *et al*, 2018). By using block chain techniques, data integrity would be ensuring.

The storage system is retained at the cluster zone in the decentralized form. This type includes a group of clusters with different storage structures for other clusters (Wang *et al*, 2013). Distributed or decentralized cloud mechanisms are extremely flexible. The reinventing cloud storage logically draws these following conclusions regarding data storage, providing the highest possible data security;

- To achieve reliability of the storage system should be decentralized and should share information in an encrypted form between independent storage nodes.
- Secure storage system essentially includes monitoring of nodes for failover, verifying data integrity and availability.
- To provide transparency to the data storage processes.
- To attain immutability of the data.

In summary, cloud computing is certainly an excellent innovation for data storage. In spite of the fact that there are numerous points of interest, e.g., fewer maintenance problems, instant software updates, trustworthiness and cost-effectiveness, the significant disservice that has been experienced in cloud is the security of the data stored. To overwhelm the major challenges such as data integrity and security, block chain techniques would be used for securing the data. The cloud storage using the block chain technique would resolve the privacy issue in cloud storage and it will increase the reliability of organization to securely store their sensitive data on cloud. By using block chain techniques, the data on cloud storage will secure the client-side data from the third party.

2. Background

In the recent years, every business enterprise, facing the developing limitless business data, requires variously the more Storage space to help the business activities that should be possible consistently in this way; the cost of the data storing and managing is also more and more high (Ying *et al*, 2009). Cloud storage structure could be a collaboration storage administration framework with many gadgets, numerous operation areas, and various assistance structures. The advancement of cloud storage framework act as an advantage from the broadband system, capacity virtualization, stockpiling system, application stockpiling incorporated with servers and capacity gadgets, clump innovation, grid cipher, dispersed document framework, content transmission structure, information compression, knowledge encryption (Zeng *et al*, 2009). Cloud storage could be a portrait of grid on-line stockpiling where information is kept in virtualized pools of the depot that area unit typically presented by third parties. Storage facilities are hand over by providers of capacity. Big data centers are preserving by capacity providers. Cloud-centralized, along with an integrated factor, frequently hold better processing improvement although rise the possibility of a catastrophic breakdown in the circumstance of a zero-day bug (Fu, 2010). For illustration, storage of clouds like Amazon, Google Documents, and Rackspace, by contribution infinite storage through very low prices however with immense accessibility, determine the possibility of storage maintenance in a unique computing portrait. Because of its inventiveness compared to the standard maintenance figure, cloud computing hike advanced security queries (Peterson, 2010).

In this section, consider the background of blockchain and the parties involved in it. The chain of blocks stems from its technical structure. All blocks are connected by a cryptographic hash to the preceding segment; a piece of a data structure that grants a series of contracts to be stored. Agreements are set up and swapped by blockchain system peers and the blockchain status is customized (Wust *et al*, 2018). The introduction of bitcoin as the first procreation of blockchain, do community ledgers along monetary transactions (Liu *et al*, 2017).

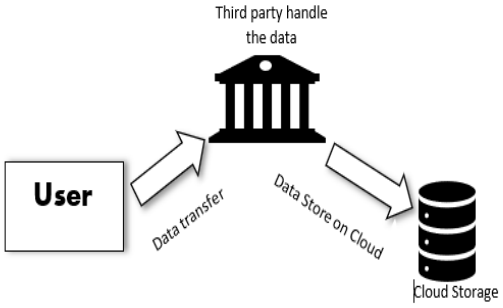


Figure 1: Cloud Storage Architecture

Bitcoin is an electronic distributed payment scheme with a public contract ledger named as Blockchain (Nakamoto, 2008). In the second era, blockchains attempt a broad, programmable set-up with an open record that registers the computational outcomes. Smart contracts have been introduced as a self-governing curriculum that runs over the system of the blockchain (Omohundro, 2014). Smart contracts could communicate causes, situations, and like a whole system of trade (Weber et al, 2016).

The classical standard of cloud computing is using the innovation of virtual computing. Personal user data can be distributed in the different virtual data centers instead of staying through national boundaries in the similar environmental locality (Arockiam *et al,* 2013).

The main privacy problems are i) Faith ii) Ambiguity iii) Compliance (Pearson, 2012).

In the cloud the information stored is alike as data stored elsewhere and the three parts of data security need to be considered: privacy, reliability, and user-friendliness (Chen *et al*, 2012). There are many sorts of problems that a distributed storage client may look during the utilization of the administration, both at the venture level and as a consumer (Mathew, 2012).Cloud storage resources are not inherently secured. Wide consideration is needed for the security thread associated with cloud storage maintenance. Cloud clients, however, usually have no authority over the servers used for cloud storage. This ensures that there is a fundamental risk of information on the cloud that is being exposed to strangers or by the cloud contractor itself (information privacy); data being exploited through the cloud provider (information trustworthiness); and data being disapproved by outsider on the cloud (information accessibility). The cloud storage should assure privacy, reliability and availability of information both in act and at repose (Kumar *et al*, 2011).

Data integrity is an elementary form of security for cloud storage (Kaufman, 2009). As information is at the core of cloud storage administration, it is significant that the cloud specialist organizations offer help of information trustworthiness to its clients (Brodkin, 2008). Regarding information trustworthiness authentication, as a result of information transmission, customers can not access data to test their reliability and then move the information. The proven information integrity result from NEC Labs can guide the authentication of community fact integrity (Zeng, 2008). Cong Wang suggested a numerical method to authenticate the data reliability and put it away in the cloud (Wang *et al*, 2009). Data encryption is the common solution to data privacy. To ensure efficient authentication, both encryption algorithm and key strength need to be considered. For these circumstances, symmetric encryption calculations are more applicable than asymmetric computation. Key management is another key issue with data encryption. Who have been answerable for key administration? Preferably, it is the information proprietors. In any case, at current, in light of the fact that the clients don't have sufficient experience to supervise the keys, cloud providers normally allot the key managing. (Chen *et al*, 2012).

Blockchain innovation also has certain mechanical threats and impediments that have been examine. Swan declares seven technological threats and restrictions to the transformation of Blockchain innovation later on (Swan, 2015): Latency: It currently takes about 10 minutes to complete one transaction to establish adequate protection for a Bitcoin transaction block. Double (twofold) spending is the consequence of effective going through cash more than once (Vigil *et al*, 2018). Decentralized factors are gradual but attempt compartmentalization of hazard. These compensations need to be treated ahead maintain a cloud computing structure (Schwartz, 2015).

The benefit of the Blockchain is that the open record (public ledger) cannot be altered either removed when the information being acknowledged through hubs. That's why Blockchain is highly recognized for its highlights of information integrity (Swan, 2015). The solid purpose of Blockchain strategy, information honesty, is the motivation behind why its consumption stretches out as well to particular organizations and operation as well. To finish up, the blockchain is unchanging and expanded in a completely decentralized manner with open auditability. Smart contract blockchain could achieve solid self-sufficient program execution (Yli-Huumo *et al,* 2016).

3. Related Work

Today our industrial information moves toward the cloud computing for storing their data on cloud storage which depends on pay-by-usage but this have some disadvantages along with some advantages. Privacy and security of data, these two are the most genuine security issues identified with client information.

Shacham *et al*. 2008 proposed an Infrastructure as a Servive (IaaS) reliable cloud computing policy (TCCP). Using TCG / TPM, TCCP certifies a software node's network integrity in IaaS already providing facilities to cloud consumers; this is use in the architecture of CloudZone to improve the performance of cloud-running weblet containers.

Bowers et al, 2008 defined a model of Proofs of Retrievability (POR) to make sure the security of the data subcontracted. Bowers et al, 2008 proposed POR model that allows for an infinite number of questions with less overhead for public verifiability. A theoretical model for POR development was proposed by Ateniese *et al*, 2007. It enhances standards (Bowers et al, 2008). Ateniese *et al*, 2008 later recommended a HAIL protocol in their successive work, HAIL receives data reliability and accessibility in the cloud. Nevertheless, this protocol will not resolve all data security risks.

Curtmola *et al*, 2008 called a Provable Data Possession (PDP) to confirm farm out data integrity; Filho *et al*, 2006 presented a Scalable Data Possession (SDP) in their subsequent work, this method entirely overwhelms the obstacles in the PDP scheme (Schwarz *et al*, 2006), but it also works only for one database.

Ateniese et al, 2008 used symmetric key cryptography to offer a partially interactive edition of the proven data possession (PDP) program. Itani et al, 2009 suggested the first dynamic proven data possession formulation that extended the PDP model to obtain updated data stored. The incentive problems in outsourcing computation are known to prevent cheating.

The PasS model (Privacy as a Service) (Itani *et al*, 2009) allows users to safely store and process private data. This is accomplished by introducing computer shielding and data isolation mechanisms that can be tailored to the client. But one thing to note here is that the homomorphic encryption technique (Talib *et al*, 2011) is still theoretical and lacks any practical implementation to allow specific algebraic operations on data encryption. A few cryptographic methodologies (Singh et al, 2011) were proposed to conceal information from the capacity supplier and in this way protect the security of information. The specialists broke down and exhibited that solitary cryptographic advances are insufficient in distributed computing to guarantee information security (Cavoukian, 2008). A major concern in such the services of cloud storage plans that there is no valid evidence to ensure that user data is not retained by the service provider even if the user prefers to remain unsubscribed (Shin *et al*, 2010). Later the client is unable to reach the service provider's storage facilities, to provide consumers with clearer and fair opportunities. It is suggested that some models distribute data fragments among multiple service providers in this way that no single service provider can retrieve anyone (Wang *et al*, 2010). If unauthorized access causes a service outage, we propose using a redundant distribution scheme (Chen *et al*, 2012) in the proposed model, where successful delivery requires at least the initial data pieces rather than the entire distribution range. At an acceptable budget, the proposed model (Gaetani *et al*, 2017) offered user data protection. Ateniese *et al*, 2007 give one of the main models that empower a customer to confirm on a solitary server the honesty of their reappropriated information without recovering it. Sookhak *et al*, 2014 examined and ordered in its study various RDA systems have been suggested to improve both safety and skills. (POW) based block chain, can guarantee confidentiality of information in a trustless condition. BigchainDB (McConaghy *et al*, 2016) is a comparative work, BitCoinNG is to improve exhibitions, giving up some security.but there are two fundamental constraints (Danezis *et al*, 2016) to their work: (I) centralization point and (ii) respectability ensures arrived at just with a greater part of fair mintettes. A characteristic way to remain customer data secret against untrusted CSP (Liu *et al*, 2012). Users of cloud systems normally assume that data is safe enough, (Gaetani *et al*, 2017) if it is encrypted, it does not safeguard that information from fraud caused by procedure errors and software bugs. Macintosh calculations (Zikratov, *et al*, 2017) take two sources of info, for an immense archive, downloading and registering the MAC of the record is an amazing procedure and takes a gigantic measure of time. Consequently, a lighter procedure is required, to figure the hashing esteem.

4. Comparison criteria

The centralized cloud storage hosts are vulnerable in their monitoring processes. Besides, the existing cloud model is highly successful, but also need some major privacy concerns.

Table 1: Comparison between cloud storage and Blockchain

Sr	Parameters	Cloud Storage	Blockchain
1	Structure	Centralized	Decentralized
2	Bandwidth	Big bandwidth required	High bandwidth required
3	Data Integrity	Data integrity is risky	Data integrity fully maintained
4	Privacy	Less privacy	Ensure the privacy of each node in block
5	Security	Weak security	High Security

Table 2: Comparative study b/w hash algorithm and cryptography

Sr.	Features	Hash	Symmetric	Asymmetric
1	No. of keys	0	1	2
2	Suggested key Length	256bits	128bits	2048bits
3	Common keys	SHA	RSA	RSA
4	Managing of key	-	Big issue	Secure and easy
5	Velocity	Fast	Fast	Relatively slow
6	Complication	Medium	Medium	High
7	Influence of key agreement	-	Failure of both sender and receiver	Only loss for the owner of Asymmetric key
8	Merits	User secure and safe from attacks	Less source consuming	Can provide digital signatures that can be denied
9	De-Merits	-	Cannot provide digital signatures that cannot be denied	More resource consuming

Table 3: Existing Work Analysis

Sr	Title	Author	Proposed Work	Threats	Block-chain based solution
1	Compact Proofs of Retrievability	(Shacham *et al*, 2008)	Proposed an Infrastructure as a Service (IaaS) reliable cloud computing policy (TCCP).	Over dependency	Block-chain provides independency.
2	Proofs of Retrievability	(Bowers,*et al*, 2008)	A model of Proofs of Retrievability (POR) makes sure	The information to be encrypted is enormous. There is	Block-chain deletes the block

			the security of the data subcontracted.	a large overhead on the server side due to inserted sentinals and error correction keys	from its storage after a period.
3	Scalable and Efficient Provable Data Possession	(Ateniese *et al*, 2008)	Recommended a HAIL protocol in their successive work, expanding the POR systems on several servers.	Data security risk	Block-chain solves this by applying the hash technique on data.
4	MultipleReplica Provable Data Possession	(Curtmola *et al*, 2008)	Proposed Provable Data Possession (PDP) to confirm farm out data integrity; it identifies an enormous element of file leakage to confirm that the database maintained the original data without retrieving it	No guarantee of retrievability of file.	Guarantee of retrievability of file
5	Demonstrating Data Possession and Uncheatable Data Transfer	(Filho *et al*, 2006)	Presented a Scalable Data Possession (SDP) in their subsequent work, this method entirely overwhelms the obstacles in the PDP scheme	It works only for one database.	It works for multiple databases.
6	Preventing Software Piracy with Crypto-Microprocessors	(Best, 1980)	Proposed a Cryto-microprocessor which provides the encryption of data.	Privacy problem.	Block-chain provides maintain the data accurate.
7	Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures	(Itani *et al*, 2009)	Proposed PasS offers a privacy review system to warn users of the various data protection acts applicable to their data and to alert them of any potential risks that may occur in protecting their	Hacker will hack the data, because cloud storage has a single point of failure.	Block-chain encrypts the data using asymmetric technique and has not single point of failure.

			confidential information		
8	A secured cost-effective multi-cloud storage in cloud computing.	(Singh *et al*, 2011)	Organizations store data on cloud storage and have the facility to enforce better data security policies. In order to protect their data, cloud users will need to rely on the cloud service provider (SP) .Some cryptographic methodologies were proposed for the security.	Data integrity not maintained.	Block-chain use hash algorithm for maintaining the data integrity.
9	Towards secure cloud storage	(Shin *et al*, 2010)	A major concern in such the services of cloud storage plans that there is no valid evidence to ensure that user data is not retained by the service provider even if the user prefers to remain unsubscribed	Data leakage	Block-chain solves this issue by applying the cryptographic techniques and covert data to cipher text.
10	Data security and privacy protection issues in cloud computing	(Chen *et al*, 2012)	Propose using a redundant distribution scheme in the proposed model, where successful delivery requires at least the initial data pieces rather than the entire distribution range.	Privacy protection	Blockchain provide privacy by using the private and public keys.
11	Blockchain-based database to ensure data integrity in cloud computing environments	(Gaetani *et al*, 2017)	Users of cloud systems normally assume that data is safe enough, if it is encrypted before farm out it to the cloud.	It does not safeguard that information from fraud.	Block-chain solves this because it provides the immutability and transparency.
12	BigchainDB: A Scalable Blockchain	(McConaghy *et al*, 2016)	By exploiting the changelessness feature of the	Unauthorized access to database.	BitCoinNG is to improve exhibitions, giving

	Database (DRAFT)		Proposed (PoW) based block chain, our arrangement can also guarantee confidentiality of information in a trustless condition. BitcoinNG, a Bitcoin convention adapted to enhanced exhibitions, motivates the primary layer block chain we use to upgraded execution.		up some security. BigchainDB, can guarantee information uprightness even if a larger proportion of noxious diggers should occur
13	Secure and privacy preserving keyword searching for cloud storage services	(Liu *et al*, 2012)	Moving data to a cloud provides nice opportuneness for clients as they do not have to be compelled to think about concerning the huge funds investing in each hardware infrastructure preparation and management.	• User of cloud depend on service provider • Service providers will access the sensitive data on cloud storage.	Block-chain makes the cloud storage decentralized and makes the data on cloud storage in encrypted form.
14	Privacy preserving public auditing for secure cloud storage.	(Wang *et al*, 2010)	It is suggested that some models distribute data fragments among multiple service providers so that no single (SP) can retrieve anyone.	Change will occur in data if one service provider will change the data.	By using proof-of-work (POW), if anyone make changes it will easily identify.

Table 3 provides us the comparison of existing works based on data privacy of cloud storage to make it secure and maintain the integrity of data by using block chain techniques. Proof of retrievability (POR) and Proof of data possession (PDP) were proposed to make data accurate and ensure privacy and security of data. But after so much work done on it still there are so much work requires making cloud storage reliable because cloud storage is centralized and it has a single point of failure. To make the cloud storage reliable we apply the blockchain techniques on cloud storage like hash algorithm and cryptography to achieve immutability and transparency. Through this we can store our sensitive data on cloud storage without any threat of unauthorized access.

5. Discussion

Cloud computing provides the resources as well as services as per the need of organization or people. It is mostly used for the storage services to reduce the overhead of the hardware storage and make resources remotely available on the internet (Venkatesh, *et al,* 2018). In this study, we have been discussed the privacy and security concerns of cloud storage. With cloud storage, data is stored on multiple third-party servers, rather than on the dedicated servers used in traditional networked data storage (Wu *et al,* 2010). As the need of data storage increases, the security concerns have been on the rise. The issues in cloud storage services are like; there is no suitable security mechanism in the process of data transmission and storage in the cloud storage system (Pasupulati *et al,* 2016).

Cloud Architect show that users have no control on their own data. So, the absence of effective security policies in cloud storage poses a challenge in cloud computing (Saeed, 2018). Encryption and Decryption are the major techniques of cloud for providing security and privacy to confidential data but these techniques do not provide sufficient security (Liang *et al,* 2017). In this paper, we propose a decentralized nature of cloud by using blockchain techniques. These techniques will address the trust issues related to third-party involvement (Wu *et al,* 2010).

There are various problems discussed in cloud computing. We try to overthrow them using Blockchain technology. Block chain techniques are needed which can mainly ensure users' privacy and control on their personal data. In addition, the implementation of a protocol that turns a block chain into an automated access-control manager that does not require trust in a third party. The reinvented cloud storage platform is aimed to present in order to perform data storage processes on a service provider's end in more secure way by encryption and distribution over a transparent and trustworthy network. This means that the data cannot be accessed, altered or deleted by any party other than the data owner.

The key advantages of decentralized nature of cloud storage are:

- Storing data in various data centers and prevent the loss of data by making copies of the data.
- It also saves money by copying shards of data to a number of devices on the network in an attempt to control redundancy.
- Also eliminate the risk of disruptions.
- Store a large number of information than their particular equipment takes into consideration without making wasteful stockpiling equipment speculations.
- The stored information is spread among decentralized clients, and each node encrypts the data to ensure data security, and data integrity can be maintained using a temper proof.

6. Conclusion & Future Work

Cloud computing storage has become a hot term in the last few years, but a clear description of what it is, what it can do, and why companies might use it is often difficult to find. Security is the major aspect in all terms. The main problem of today's cloud storage is the existence of a mediator, a provider of cloud services. Trusted third party usually has access to the data because it stores encryption keys. Data is stored on centralized servers, which are attractive points for malicious attacks. When security level in cloud becomes high then confidentiality, integrity and privacy will be more convenient for the users and service providers. Despite of many advantages there are lots of issues in cloud computing environment regarding the security of the data transmission and data storage over internet. In this study, the propose work of blockchain-based distributed cloud storage architecture to provide more secure and reliable cloud storage services for enterprises or individual users. By using these techniques, the cloud storage will become more efficient than the existing ones in terms of privacy and security and data integrity. Comparative simulation results illustrate that our architecture has an outstanding security performance. In future, further work on block chain will be done in order to enhance the privacy and security of cloud storage.

References

Arockiam, L., & Monikandan, S. (2013). Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. *International Journal of Advanced Research in Computer and Communication Engineering,* 2(8), 3064-3070.

Ateniese, G., Pietro, R. D., Mancini, L. V., & Tsudik, G. (2008). Scalable and Efficient Provable Data Possession. In *SecureComm '08: Proceedings of the 4th international conference on Security and privacy in communication networks.* doi: 10.1145/1460877.1460889

Ateniese, G., R. Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007). Provable Data Possession at Untrusted Stores. In *Proceedings of the 14th ACM Conference on Computer and Communications Security.* doi: 10.1145/1315245.1315318

Best, R.M. (1980). *Preventing software piracy with crypto-microprocessors.* Retrieved from https://www.semanticscholar.org/paper/Preventing-software-piracy-with Best/b787c1104bb4e1620ab4153ab1fa15c01d5ba2a6

Bowers, K., D. Juels, A. & Oprea, A. (2008). *HAIL: A High-Availability and Integrity Layer for Cloud Storage, Cryptology ePrint Archive, Report 2008/489.* Retrieved from http://eprint.iacr.org/

Bowers, K., D. Juels, A. & Oprea, A. (2008). *Proofs of Retrievability: Theory and Implementation, Cryptology ePrint*

Archive, Report 2008/175. Retrieved from http://eprint.iacr.org/

Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. *Network World.*

Cavoukian, A. (2008). Privacy in Clouds. *Identity in the Information Society* (*IDIS),* 1, 89–108. doi: 10.1007/s12394-008-0005-z

Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues In Cloud Computing. In *International Conference on Computer Science and Electronics Engineering ICCSEE.* doi: 10.1109/ICCSEE.2012.193

Curtmola, R., Khan, O., Burns, R., & Ateniese, G. (2008). MR-PDP: Multiple-Replica Provable Data Possession. In *the 28th International Conference on Distributed Computing Systems* (ICDCS). doi: 10.1109/ICDCS.2008.68

Danezis, G., & Meiklejohn, S. (2016). Centrally Banked Cryptocurrencies. In *23rd Annual Network and Distributed System Security Symposium, NDSS.*

Filho, D.L., & Barreto, P.S. (2006). Demonstrating data possession and uncheatable data transfer. *IACR Cryptol. ePrint Arch., 2006*, 150.

Fu, S. (2010). Failure-aware resource management for high-availability computing clusters with distributed virtual machines. *Journal of Parallel and Distributed Computing, 70*(4), 384- 393. doi: 10.1016/j.jpdc.2010.01.002

Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017). Blockchain-Based Database to Ensure Data Integrity in Cloud Computing Environments. ITASEC.

Itani, W., Kayssi, A., & Chehab, A. (2009). Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures. In *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.* doi: 10.1109/DASC.2009.139

Jayapandian, N., & Zubair Rahman, A. M. J. M. (2017). Secure and efficient online data storage and sharing over cloud environment using probabilistic with homomorphic encryption. *Cluster Computing*, 20(2), 1561–1573. doi:10.1007/s10586-017-0809-4

Kaufman, L.M. (2009).Data Security in the World of Cloud Computing. *IEEE Security and Privacy, 7*(40), 61-64. doi: 10.1109/MSP.2009.87

Kumar, R. S., & Saxena, A. (2011). Data integrity proofs in cloud storage. In *Third International Conference on Communication Systems and Networks (COMSNETS 2011*.doi: 10.1109/COMSNETS.2011.5716422

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud

Environment with Enhanced Privacy and Availability. In *17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID).* doi:10.1109/ccgrid.2017.8

Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. In *IEEE International Conference on Web Services (ICWS).* doi: 10.1109/ICWS.2017.54

Liu, Q., Wang, G., & Wu, J. (2012). Secure and privacy preserving keyword searching for cloud storage services. *Journal of Network and Computer Applications*, 35(3), 927-933.

Mathew, A.B. (2012). Survey Paper on Security & Privacy Issues in Cloud Storage Systems. *EECE 571B, Term Survey Paper.*

McConaghy, T., Marques, R., M¨uller, A., Jonghe, D.D., McConaghy, T., McMullen, G. Henderson, R., Bellemare, S., & Granzotto, A. (2016). *BigchainDB: A Scalable Blockchain Database.* Retrieved from https://mycourses.aalto.fi/pluginfile.php/378362/mod_resource/content/1/bigchaindb-whitepaper.pdf

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Retrieved from http://bitcoin. org/bitcoin. pdf.

Omohundro, S. (2014).Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters,* 1(2), 19-21.doi: 10.1145/2685328.2685334

Pasupulati, R. P., & Shropshire, J. (2016). Analysis of centralized and decentralized cloud architectures. *SoutheastCon 2016,* 1-7.

Pearson, S. (2012). Privacy, Security and Trust in Cloud Computing. In Pearson, S., & Yee, George. (Eds.), *Privacy and Security for Cloud Computing* (3-42). Berlin, Germany: Springer.

Peterson, G. (2010). Don't Trust. And Verify: A Security Architecture Stack for the Cloud. *IEEE Security and Privacy Magazine (IEEE SECUR PRIV)* 8(5), 83-86. doi:10.1109/MSP.2010.149

Prianga, S., Sagana, R., & Sharon, E. (2018). Evolutionary Survey on Data Security in Cloud Computing Using Blockchain. In *IEEE International Conference on System, Computation, Automation and Networking (ICSCA).* doi:10.1109/icscan.2018.8541258

Saeed, Z. R. (2018). Improved Cloud Storage Security of Using Three Layers Cryptography Algorithms. *International Journal of Computer Science and Information Security (IJCSIS),* 16(10), 34-39.

Schwartz, L. M. (2015). *Five Common Misconceptions about Cloud Platforms.* Retrieved from https://www.forbes.com/sites/oracle/202

0/05/14/gpu-chips-are-poised-to-rewrite-again-whats-possible-in-cloud computing/#77f4d8f87c23

Schwarz, T.S.J. & Miller, E.L. (2006). Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage. In *26th IEEE International Conference on Distributed Computing Systems (ICDCS'06),* Lisboa, Portugal, 12-12. doi: 10.1109/ICDCS.2006.80

Shacham H., Waters B. (2008). Compact Proofs of Retrievability. In: Pieprzyk J. (Eds.), *Advances in Cryptology - ASIACRYPT 2008. ASIACRYPT 2008.* Lecture Notes in Computer Science, 5350. Springer, Berlin, Heidelberg

Shin, S., & Kobara, K. (2010). *Towards Secure Cloud Storage (Demo for CloudCom 2010).* Retrieved from https://www.semanticscholar.org/paper/Towards-Secure-Cloud-Storage-(-Demo-for-CloudCom-)-Shin-Kobara/b3aacd7ad88ee73f0454ef73d796215e7eca0288

Singh, Y., Kandah, F., & Zhang, W. (2011). A secured cost-effective multi-cloud storage in cloud computing. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).* doi: 10.1109/INFCOMW.2011.5928887

Sookhak, M., Talebian, H., Ahmed, E., Gani, A., & Khurram, M., K. (2014). A review on remote data auditing in single cloud server: Taxonomy and open issues. *Journal of Network and Computer Applications,* 43, 121–141.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Retrieved from http://shop.oreilly.com/product/0636920037040.do

Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010).Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy Magazine*, 8(6), 24–31. doi:10.1109/msp.2010.186

Talib, A. M., Atan, R., Abdullah, R., & Azrifah, M. (2011). Cloudzone: Towards An Integrity Layer Of Cloud Data Storage Based On Multi Agent System Architecture. In *IEEE Conference on Open Systems.* doi: 10.1109/ICOS.2011.6079311

Venkatesh, A., & Eastaff, M. S. (2018). A Study of Data Storage Security Issues in Cloud Computing. *International Journal of Scientific Research in Computer Science, Engineering and information Technology*, 3(1), 1741-1745. Retrieved from https://www.academia.edu/37802999/A_Study_of_Data_Storage_Security_Issues_in_Cloud_Computing

Vigil, A., Pathak, P., Upadhyay, S., Singh, D., & Garg, V. (2018). Blockchain over Transaction System. In *3rd International Conference on Communication and*

Electronics Systems (ICCES).doi: 10.1109/CESYS.2018.8723962

Wang, C., Chow, S. S. M., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-Preserving Public Auditing for Secure Cloud Storage. *IEEE Transactions on Computers*, 62(2), 362–375. doi:10.1109/tc.2011.245

Wang, C., Wang, Q., Ren, K., & Lou, W. (2009). Ensuring Data Storage Security in Cloud Computing. In *Proceedings of the 17th International Workshop on Quality of Service*. Retrieved from https://eprint.iacr.org/2009/081.pdf

Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. In *Proceedings of the 29th conference on Information Communications (INFOCOM)*. doi: 10.1109/INFCOM.2010.5462173

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A, & Mendling, J. (2016).Untrusted business process monitoring and execution using blockchain. In *Business Process Management: 14th International Conference*. doi: 10.1007/978-3-319-45348-4_19

Wu, J., Ping, L., Ge, X., Wang, Y., & Fu, J. (2010). Cloud Storage as the Infrastructure of Cloud Computing. In *International Conference on Intelligent Computing and Cognitive Informatics*. doi:10.1109/icicci.2010.119

Wust, K., & Gervais, A. (2018). Do you need a Blockchain? In *Crypto Valley Conference on Blockchain Technology (CVCBT)*.doi: 10.1109/CVCBT.2018.00011

Ying, Z., & Yong, S. (2009). Cloud storage management technology. In *Second International Conference on Information and Computing Science*. doi: 10.1109/ICIC.2009.85

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research On Blockchain Technology?—A Systematic Review. *PloS one*, *11*(10). doi:10.1371/journal.pone.0163477

Zeng, K. (2008). Publicly verifiable remote data integrity, In: Chen L, Ryan MD, Wang G, (Eds.), *Information and Communications Security. ICICS 2008.* Lecture Notes in Computer Science, 5308. Springer, Berlin, Heidelberg

Zeng, W., Zhao, Y., Ou, K., & Song, W. (2009). Research on cloud storage architecture and key technologies. In *ICIS '09: The 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*. doi:10.1145/1655925.1656114

Zhe, D., Qinghong, W., Naizheng, S., & Yuhan, Z. (2017). Study on Data Security Policy Based on Cloud Storage. In *IEEE 3rd*

International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS). doi:10.1109/bigdatasecurity.2017.12

Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., & Yalansky, L. (2017). Ensuring data integrity using blockchain technology. In *20th Conference of Open Innovations Association (FRUCT).* doi: 10.23919/FRUCT.2017.8071359