JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN TECHNOLOGY FOR SECURE CLOUD COMPUTING SERVICES

[1]Jaffer Sharief, [2] Mallesi V
[1]M.Tech Scholar, [2]Associate Professor & Head
[1,2]Department of Computer Science & Engineering
[1,2] Bheema Institute of Technology & Science, Adoni, Kurnool Dist. A.P, India

***Abstract:*.**
A well-known technology that has been around for a long time is cloud computing. However, several of the difficulties associated with cloud computing, such as interoperability, data management, and data security, are still being faced. The world is turning to blockchain technology, which is still relatively new, because of its authenticity and security, which are its two primary distinguishing characteristics. There are several benefits of combining blockchain and cloud computing, including usability, trust, security, scalability, data management, and many others. We will describe about how combining a scalable cloud environment with a blockchain network may improve server services, data security, and user data management. Also, we will identify the most recent solution from a security perspective, public information is kept in the cloud computing system in a manner that preserves its confidentiality, integrity, and authenticity. Further we will investigate about cloud@blockchain platform. Finally, we will design a blockchain based approaches for loan transaction and analysis will disclose that the blockchain technology will improve the security in cloud computing services.

***IndexTerms* – blockchain, cloud computing services, cloud@blockchain, decentralized, secure, smart contact,**

I. INTRODUCTION

Large-scale, distributed computer technologies gave rise to the clearly defined field of cloud computing. The processing load that users must bear will be lessened via cloud computing. Numerous benefits exist, including lower hardware and maintenance costs, global availability, flexibility with a fully automated process, and simple scaling. The cloud has been used by several large corporations, including IBM, Google, Amazon, and Microsoft. Many new apps, like Google App Engine, Google Cloud Platform, Amazon Cloud, Elastic computing platform, etc., are prototypes. It offers us the convenience of a pay-per-use system and a flexible IT architecture that are available over the internet on mobile devices. Despite the fact that the cloud offers a wide range of helpful services, businesses are reluctant to adopt it because of privacy concerns. Significant constraints preventing the cloud from being used include security concerns and its difficulties. The future of the sectors working to enhance privacy and security is blockchain technology. Blockchain is a decentralized ledger that stores chain-like, tamper-evident data devoid of a central repository. Nodes are the components or users of the blockchain technology [1-3]..

Blockchain offers a decentralized network where all network nodes actively participate in the data validation and verification process. Cryptography will be used to encrypt the data that will be stored on the blockchain. Each block has a timestamp, an encrypted hash, and a hash of the block before it in the chain via which it will link. As a result, the blockchain's data is tamper-evident. Blockchain technology offers the data security, and since participating users will be confirmed in the network, there is no longer a privacy risk with the data. We can address the data's privacy and security issues by integrating with blockchain technology to support the rise of cloud computing. It enhances data security, service availability, and cloud data management[4].

Cloud offers a wide range of services, which are primarily categorized into three delivery types. The first service is Software as a Service (SaaS), which functions as an online application hosted for consumers. A single platform of cloud-based software that offers a variety of services to a large number of users is delivered by the cloud service provider together with the full apps or projects [5]. The cloud infrastructure is not within the control of cloud customers. A notable example of SaaS is Google Mail, SalesForce.com, and Amazon Web Services. Platform as a Service is the second service (PaaS). We may install our application and libraries of programming languages on the platform thanks to the cloud service provider. SaaS hosts the entire application on the cloud, whereas PaaS just offers the platform; this is how SaaS and PaaS vary from one another [6]. The finest PaaS example is the Google search engine. The third offering is Infrastructure as a Service (IaaS), which enables users to directly use network-based resources for processing, storage, and other functions [7-9]. The purpose of the study is to define the function of blockchain technology in the context of cloud computing as well as to pinpoint any potential risks and difficulties associated with its use in this context. The objectives are to determine the breadth of blockchain technology and its use in the context of cloud computing, as well as the security implications of blockchain technology's use in this context. In order to examine the most recent solution from a security perspective, public information must be kept in the cloud computing system in a manner that preserves its confidentiality, integrity, and authenticity.

II. BLOCKCHAIN TECHNOLOGY

The blockchain is a relatively new technology, and studies are now being conducted to determine how safe it may make the usage of electronic money by allowing peer-to-peer communication alone. Taking a look at these technical advancements in cloud computing. The public ledger for transactions is a blockchain, which guards against hacking when dealing with virtual currency. It is made to prevent subjective manipulation by the operator of distributed peers and is a sort of distributed database with a data record list that is constantly expanding. The blockchain software is installed on computers, and transaction records are encrypted in accordance with a set of rules. Blockchain technology is used by Bitcoin, an electronic form of money. Since the Internet and encryption technologies have advanced comparing the use of blockchain versus keeping all data in a single database, the former can offer more security. In terms of data storage and administration, the implementation of these technologies in Bit coin demining was revolutionary since it allowed for the prevention of database attack damage. Furthermore, when used in a field where data disclosure is necessary, the blockchain's openness feature may enable transparency in data. Due to these advantages, it may be used in a variety of contexts, such as the financial industry and Internet of Things (IoT) environments, and its applications are anticipated to expand.

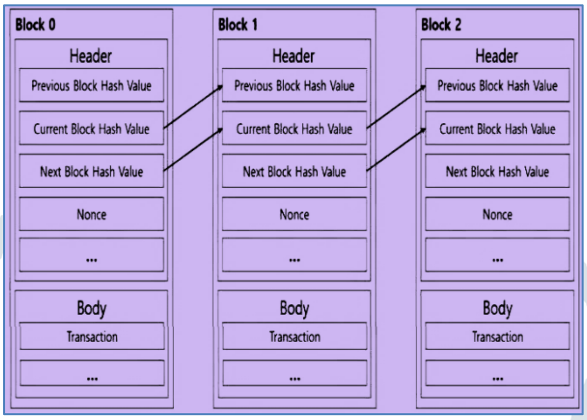


Fig.1. Blockchain Connection Structure [10]

When a new transaction occurs, all participants may update their ledgers to ensure integrity using a blockchain, which keeps a record of all transactions in one place. The single point of failure resulting from the reliance on a trusted third party has been eliminated thanks to the development of the Internet and encryption technology, which has allowed all participants to independently check the validity of a transaction. By integrating transactions from across the network into a block, the individual lending digital currency completes a transaction record on the blockchain through the work authentication process. After that, it is verified and connected to the preceding block to provide the hash value. To convey the most recent transaction detail block, this block is routinely updated and reflected on the electronic cash transaction information. This procedure permits the employment of a trustworthy mechanism while offering security for the exchange of electronic currencies. A lot of IT settings have adopted cloud computing because of its effectiveness and availability. Furthermore, critical security components including confidentiality, integrity, and authentication as well as access control have been examined in relation to cloud security and privacy problems.

III. BLOCKCHAIN SOLUTIONS TO SECURE CLOUD COMPUTING

An evaluation of security cases involving bitcoins utilizing blockchain was done after introducing the security reasons for doing so. Users' sensitive information may be leaked, resulting in financial and psychological harm, if user data is released in a cloud computing environment. The security of data transmission and storage, including confidentiality and integrity, is primarily researched in the context of cloud computing. Just keep in mind that further research is needed on anonymity and privacy protection. Blockchain is an example of a technology that ensures confidentiality. Blockchain may be improved to a useful service with higher security if linked with the cloud computing environment. If the blockchain approach is applied for storing user data in the cloud computing environment, user anonymity may be guaranteed [11]. When utilizing blockchain technology, an electronic wallet is installed. The user information may remain if the electronic wallet is not properly removed. The user information may be inferred from the remaining user information. We provide a technique that securely installs and removes the electronic wallet to address this issue. Cloud architecture can be design with the use for block chain to improve security in cloud computing [12].

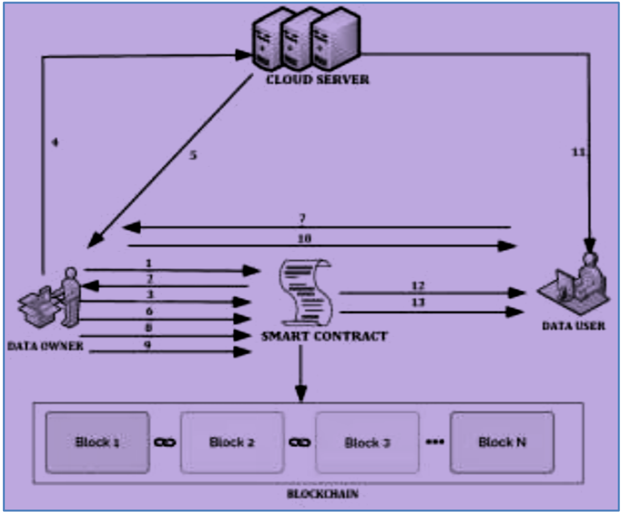


Fig.2: Secure Cloud Architecture Based on Blockchain [13]

The Figure 4.1 depicts the cloud architecture that uses block chains for security.

Blockchain: To prevent data from being altered or repudiated, all contracts and accompanying call logs are maintained on blockchains.

Smart Contract: This is utilized by users and owners to store and retrieve ciphertext data and to run encryption and decryption algorithms. The blockchain allows for the deployment of smart contracts (SC) and offers interfaces for data storage and retrieval.

Data Owner: A data owner's crucial activities include creating and deploying the SC and uploading the encrypted contents. Additionally, it assigns characteristics, specifies access control policies, and adds each user's valid access period.

Data User: A data user's tasks include gaining access to the encrypted files kept on the server. It decrypts the received ciphertext to acquire the content key needed for the decryption operation if its attributes satisfy the access structure included in the provided ciphertext.

Cloud Server: The encrypted files that the data owner submitted are stored on this cloud server. The various algorithms that are utilized are setup-algorithm (data owner), encryption algorithm, key generation algorithm (data owner) and decryption algorithm (data user).

IV. CLOUD@BLOCKCHAIN ARCHITECTURE

The cloud@blockchain is a secure cloud computing architecture which is based on blockchain. In this architecture each node will have a public transaction book and anybody can verify the legitimacy and integrity of every transaction because they are all recorded. A decentralized application on cloud@blockchain is made to protect against file piracy and preserve privacy.

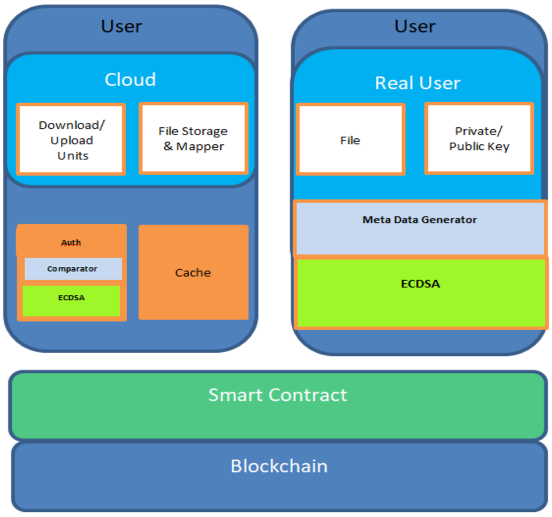


Fig. 3: Cloud@Blockchain Architecture [14]

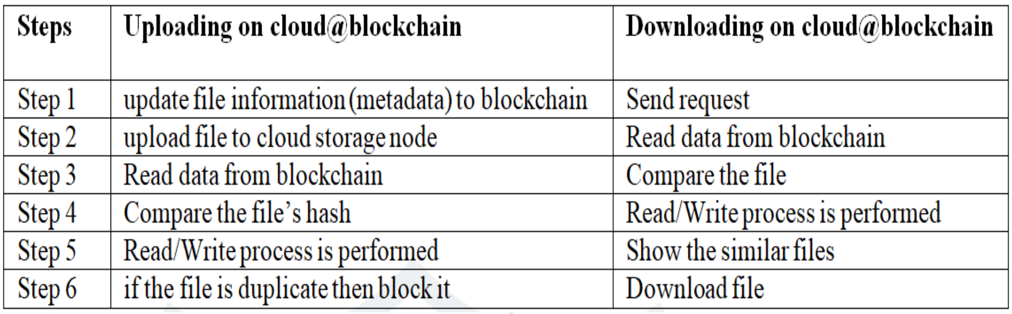
This architecture can be used in anonymous contest and digital certificate verification.

In this work, we develop two mechanisms operating on the cloud@blockchain to improve existing cloud computing services.

- ***Anonymous file sharing:*** A significant amount of user data are collected by the cloud storage service. On cloud@blockchain, users can share files while protecting their privacy due to the anonymous file-sharing mechanism.
- ***Inspection for illegally uploaded files:*** A distinct fingerprint is produced and stored on the blockchain. Whenever a file is uploaded, it is simple to identify whether the file uploader is the owner.

All apps in this research are referred to as "users" since they are all built on the blockchain platform and this system has a flat architecture. The mediation layer for communication is a smart contract. Owner-uploaded metadata can be processed and stored by smart contracts. The user may easily verify the identity of the data owner using any cryptographic technique, such as the Elliptic Curve Digital Signature Algorithm (ECDSA). After receiving a request from the owner to upload anything, users (on the cloud side) can offer online storage services (user side). The authentication unit, upload unit, file storage unit, and mapper allow the cloud storage facility to confirm the owner's consent. While being accessible to the public, the blockchain protects owners' anonymity. Although nothing is completely safe, it is nearly hard to manipulate with blockchain.

Table 1Presents about uploading and downloading steps

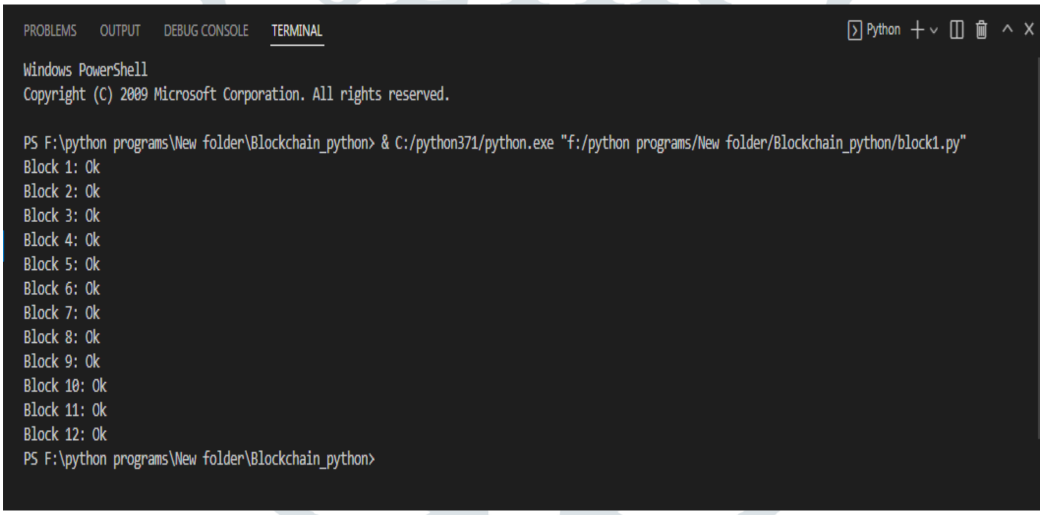


Steps	Uploading on cloud@blockchain	Downloading on cloud@blockchain
Step 1	update file information (metadata) to blockchain	Send request
Step 2	upload file to cloud storage node	Read data from blockchain
Step 3	Read data from blockchain	Compare the file
Step 4	Compare the file's hash	Read/Write process is performed
Step 5	Read/Write process is performed	Show the similar files
Step 6	if the file is duplicate then block it	Download file

V. Execution Results

The block chain for secure cloud computing services have been implemented and execution results are presented in the form of snaps shots below

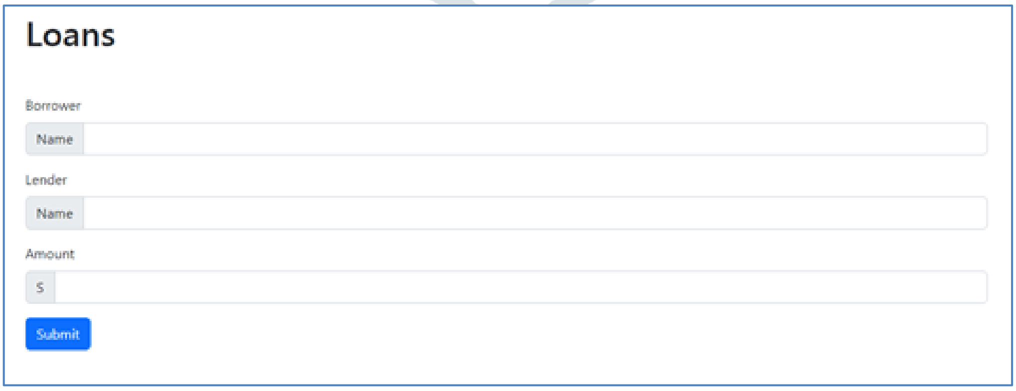
BLOCKS CHECKING



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS F:\python programs\New folder\Blockchain_python> & C:/python371/python.exe "f:/python programs/New folder/Blockchain_python/block1.py"
Block 1: Ok
Block 2: Ok
Block 3: Ok
Block 4: Ok
Block 5: Ok
Block 6: Ok
Block 7: Ok
Block 8: Ok
Block 9: Ok
Block 10: Ok
Block 11: Ok
Block 12: Ok
PS F:\python programs\New folder\Blockchain_python>
```

Fig.4 Block Checking Process



Loans

Borrower

Name

Lender

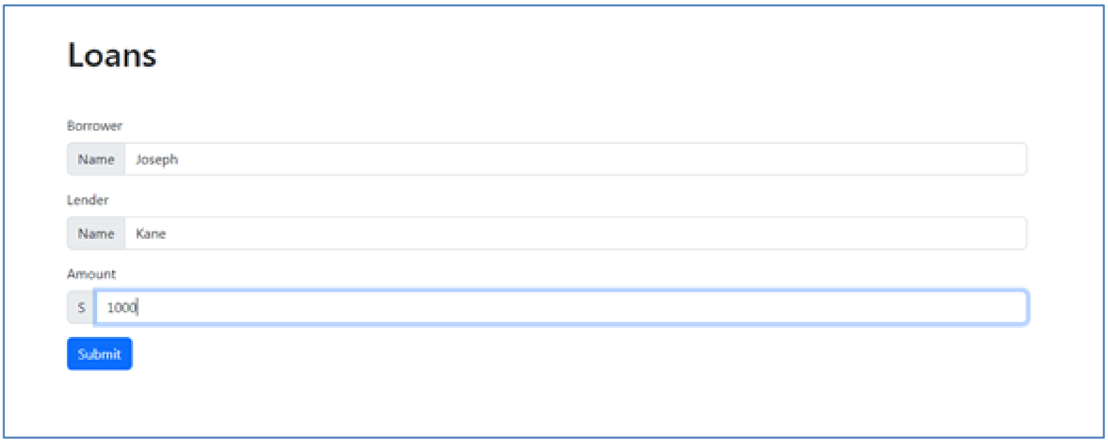
Name

Amount

$

Fig.5 Loan Webpage

TRANSACTION CHECKING



Loans

Borrower

Name Joseph

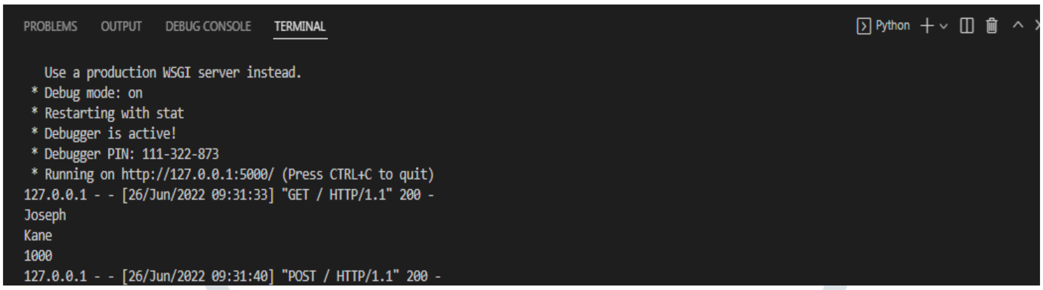
Lender

Name Kane

Amount

$ 1000

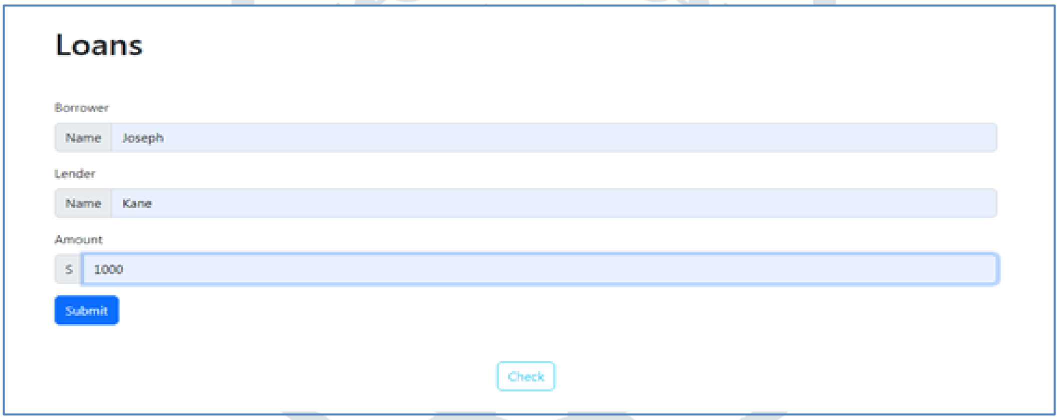
Fig.6 Web Page for Transaction Checking



```
   Use a production WSGI server instead.
 * Debug mode: on
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 111-322-873
 * Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
127.0.0.1 - - [26/Jun/2022 09:31:33] "GET / HTTP/1.1" 200 -
Joseph
Kane
1000
127.0.0.1 - - [26/Jun/2022 09:31:40] "POST / HTTP/1.1" 200 -
```

Fig.7 Shows the Transaction Details

CHECKING INTEGRITY



Loans

Borrower

Name Joseph

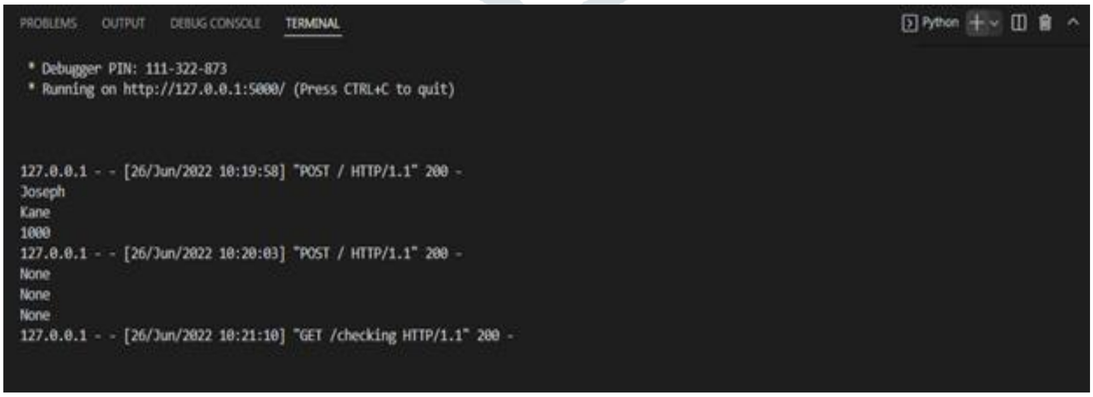
Lender

Name Kane

Amount

$ 1000

Fig.8 Web Page for Checking Integrity



```
 * Debugger PIN: 111-322-873
 * Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)



127.0.0.1 - - [26/Jun/2022 10:19:58] "POST / HTTP/1.1" 200 -
Joseph
Kane
1000
127.0.0.1 - - [26/Jun/2022 10:20:03] "POST / HTTP/1.1" 200 -
None
None
None
127.0.0.1 - - [26/Jun/2022 10:21:10] "GET /checking HTTP/1.1" 200 -
```

Fig.9 Integrity details

CONCLUSION

We have investigated the security issues in cloud computing and understood the benefits of blockchain for secure cloud computing services. Also we presented the block chain solutions and cloud@blockchain architecture to improve security in the cloud computing. It is seen that the cloud@blockchain platform provides anonymous file sharing mechanism to provide privacy and data sharing and inspection mechanism to identity illegal uploads. Finally, we have designed a blockchain based approaches for loan transaction and analysis have shown that the blockchain technology had improved the security in cloud computing services.

REFERENCES

[1] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, ‘‘Blockchain challenges and opportunities: A survey,’’ Int. J. Web Grid Services, vol. 14, no. 4, pp. 352–375, 2018.
[2] D. Yaga, P. Mell, N. Roby, and K. Scarfone, ‘‘Blockchain technology overview,’’ 2019, arXiv:1906.11078. [Online]. Available: http://arxiv.org/abs/1906.11078
[3] D. B. Rawat, V. Chaudhary, and R. Doku, ‘‘Blockchain: Emerging applications and use cases,’’ 2019, arXiv:1904.12247. [Online]. Available: https://arxiv.org/abs/1904.12247
[4] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, ‘‘Analysis of blockchain technology: Pros, cons and SWOT,’’ Cluster Comput., vol. 22, no. 6, pp. 14743–14757, Nov. 2019.
[5] M. Risius and K. Spohrer, ‘‘A blockchain research framework,’’ Bus. Inf. Syst. Eng., vol. 59, no. 6, pp. 385–409, 2017
[6] M. K. R. Ingole and M. S. Yamde, ‘‘Blockchain technology in cloud computing: A systematic review,’’ Sipna College Eng. Technol., Maharashtra, India, Tech. Rep., 2018
[7] D. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. L. Njilla, ‘‘Data provenance in the cloud: A blockchain-based approach,’’ IEEE Consum. Electron. Mag., vol. 8, no. 4, pp. 38–44, Jul. 2019.
[8] C. V. N. U. B. Murthy and M. L. Shri, ‘‘A survey on integrating cloud computing with blockchain,’’ in Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (IC-ETITE), Feb. 2020, pp. 1–6.
[9] N. Sanghi, R. Bhatnagar, G. Kaur, and V. Jain, ‘‘BlockCloud: Blockchain with cloud computing,’’ in Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN), Oct. 2018, pp. 430–434
[10] Jin Ho Park, Jong Hyuk Park, Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions, in Symmetry Journal, Advanced in Artificial Intelligence and Cloud Computing, August 2018, Available: https://www.mdpi.com/2073-8994/9/8/164
[11] A. Harshavardhan, T. Vijayakumar, and S. R. Mugunthan, ‘‘Blockchain technology in cloud computing to overcome security vulnerabilities,’’ in Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud)(ISMAC) I-SMAC (IoT Social, Mobile, Anal., Cloud)(I-SMAC) 2nd Int. Conf., Aug. 2018, pp. 408–414
[12] A. Vatankhah Barenji, H. Guo, Z. Tian, Z. Li, W. M. Wang, and G. Q. Huang, ‘‘Blockchain-based cloud manufacturing: Decentralization,’’ 2019, arXiv:1901.10403. [Online]. Available: http://arxiv.org/ abs/1901.10403
[13] Mr. Amarnath J L , Dr. Pritam G Shah , Dr. Sarika Malhotra, Dr. Sharmila, “Design of Secured Cloud Architecture Using Blockchain Technology” Journal of Xi'an University of Architecture & Technology, ISSN No : 1006-7930, Page No: 983-987
Volume XII, Issue IV, 2020
[14] 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”, International Conference on Advanced Communications Technology(ICACT) ICACT2020 February 16 - 19, 2020, ISBN 979-11-88428-04-5, pp. 155-158.