Public Key Encryption for Cloud Storage Attack using Blockchain

Akshay Babrekar, Rohini G. Pise

Abstract: *Cloud storage enables user to store data and make it available when it is requested by user. Data generated electronically is very important and it must be encrypted to make sure that the data is tramper-proof. There are two important points to be considered, keyword guessing attack and making cloud storage secure from hackers. In Keyword guessing attack the Keywords search by user are encrypted using secure mechanism and securing the cloud storage means use such techniques which assured to give Confidentiality, Integrity and Accessibility using Blockchain Technology. It is decentralized cloud storage which assist different security mechanisms to protect data. Decentralized cloud storage is itself secure than centralized cloud storage. Because the concept of decentralized is not to store data on single storage device but to store on multiple servers. While storing the data on different location it divided into small parts, and at the time of retrieving data it is available as a complete single block of original data. Whereas in centralized cloud storage data is stored on single storage device. As technology progress the risk from fraudulent users also increases. For this reason, we need some encryption, decryption and authentication mechanism to verify user and if it is authenticated allow access to use its data. There are some techniques also available where user made request on cloud server to receive data which makes cloud server to learn keywords except resulting data. In this paper we make an attempt to review encryption and decryption for cloud storage using blockchain technology to improve security of data.*

Keywords — Cloud storage, Keyword guessing attack, securing the cloud, Blockchain, Encryption

I. INTRODUCTION

Using cloud storage user can access his data via internet. These services include send and receive data from systems, where user send their data to multiple users and it is received by target receiver by searching the keywords. This also reduce the load of system which holds data and allows user to store data on the cloud server. While, using these service's security of data remains a question. Confidentiality of data is one of the most important issue. Hence, data must be encrypted before sending. In public key encryption keywords and data kept encrypted under receiver's public key. Resulting cyphertext data store on server, then receiver creates trapdoor to test weather cyphertext of keyword is same as trapdoor for retrieving data.

The main advantage of cloud server is that it is reliable. If one node fails, still user is able to retrieve the data. To gain access control on data, method use to the encryption remains a trust. In case for decentralized cloud storage slowing factor is an issue, due to independent and dynamic nature of network reduces control of owner on network on their resources. For centralized systems, Cloud Service Provider (CSP) is considered to be most trusted platform for the operation performed by authenticated users. User side encryption is first strategy to protect data but this kind of security mechanism remains unsafe in case where encrypted key is reveal or data nodes are not performing the operation which is given by owner. These operations like deleting data, reconstructing the resource entity. So, the security of encryption key is not adequate in decentralized cloud storage, additional layers security is to be needed. On the other side, reliability of DCS is increases due to independent participation of data storage resources. If attentive precaution method is used then makes it possible for data owner to completely relay on the DCS to store their data. For this purpose, there are various methods are available which can be used with blockchain technology to enhance the security level. Apart from encrypting the data, Confidentiality, Integrity and Accessibility of data is also important which can be achieved by blockchain. When user request to access data and after permission is given to user, all the transactions is captured with the help of blockchain and the data security is maintained because it makes the transactions unalterable. It is mostly promising technology which minimize the chances of attacks and threads to data. In blockchain data is divided into block and each block have its different hash as well as nonce value which is reference to the next and previous block in chain. Hash is having 256-bits and Nonce is having 32-bits so it's approximately four billion probable combination of hash and nonce. Alteration to any one earlier block requires re-mining not only that block but also all blocks which are in chain. Hence, it is tough to exploit blockchain technology. After complete mining chain of block is accepted by rest of the nodes.

Manuscript received on May 25, 2020.
Revised Manuscript received on June 29, 2020.
Manuscript published on July 30, 2020.
***** Correspondence Author

Akshay Babrekar*, Department of Information Technology, Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune, India. Email: a.babrekar.ab@gmail.com

Rohini G. Pise, Department of Information Technology, Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune, India. Email: rohinipise@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

II. LITREATURE SURVYE

Yuan Zhang, Chunxiang Xu, Jianbing Ni, Hongwei Li, and Xuemin (Sherman) Shen; in their paper title “Blockchain-assisted Public-key Encryption with Keyword Search against Keyword Guessing Attacks for Cloud Storage” state that encryption technique use for search keyword is plays vital role in such applications where user request for some results to storage server and server respond without learning about data than search result.

The difficulty of this technique is introduced by Song etal, where it searches word by word of all files, which makes this method inefficient. Currently, many searchable techniques are there with different features basically these are symmetric cryptography system and applicable where user sends data to cloud storage and then user search by keywords.

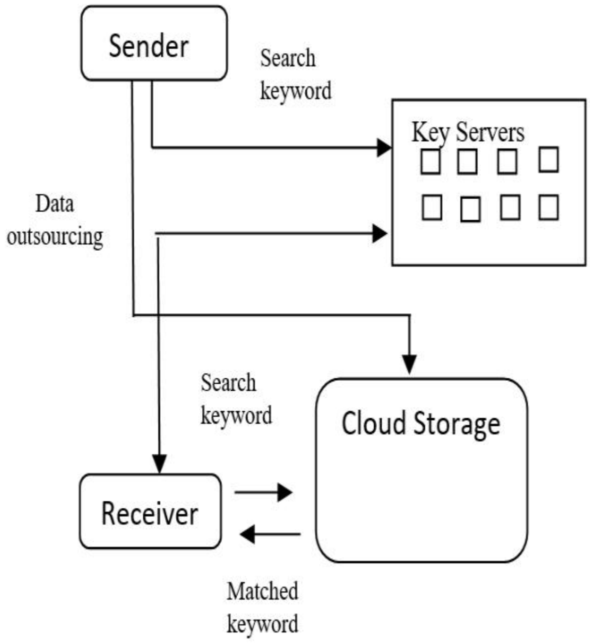

Fig 1 (a). Cloud based storage system [1]

As shown in Fig 1 (a) sender search for file on cloud server and the search file is sent to intended receiver and keyword are stored in key server in encrypted form. Then ciphertext are stored to cloud server. After receiver receives the search encrypted data on cloud server it is decrypted locally, these files are able to use for offline storage. When user search for particular file on cloud server, key server encrypts the generated keywords from user input to resist keyword guessing attack. Encrypted keywords as well as encrypted data then stored to cloud storage. In this system payment getaway is optional and not taken into consideration. Payment gateway is only intended to collect service charges from the user who what to store data on cloud storage of owner.[1]

Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, Pierangela Samarati; in their paper title “Securing Resources in Decentralized Cloud Storage states that data owner can store data in decentralize cloud storage” to share with multiple users at the same time they are able to delete data from cloud server. The contribution is threefold. First it assured by All-Or-Nothing-Transform (AONT) strategy. In this, plain text is converted in cipher text while data is store on cloud server making sure that the original data can be obtained from it.

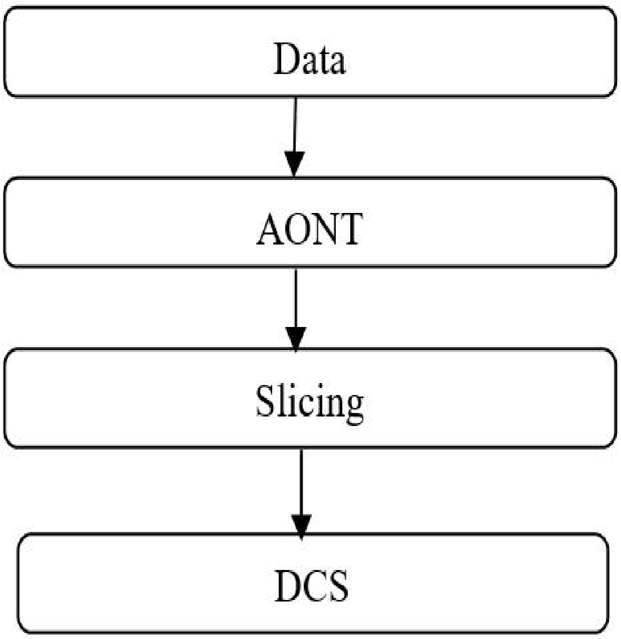

Fig 2 (a). DCS using AONT [2]

If some part of encrypted data is unavailable this technique does not enable to generate original data. Some scenarios to be considered: a) if user knows the encryption key and encrypted portion of data is not available, it will not be able to retrieve original data. b) if user do not have key, he won’t be able to execute keyword guessing task called brute force attack. c) even user have valid key it will not be useful if it is applied only some portion of encrypted data. Second is, making small chunks of data and distribute them across decentralized cloud storage (DCS) by making sure that availability and security of data. Third is, user is able to control in how many parts this data can be divided to ensure security and availability of data. In Fig 2 (a) As per characteristic of decentralized cloud storage (DCS) making data available after dividing of source data into several chunks and assigning it to the nodes is ensured by protecting and making data available to user. Availability is maintained by replication of data on cloud server because malicious servers do not let user to reach up to the data on server. DCS also remains a good option in case of reliability of service due to number of nodes are available to store the data, with the caution methods makes them promising service of storing and retrieving data.[2] Shangping Wang, Xu Wang, And Yaling Zhang; in their paper title “A secure cloud storage framework with access control based on blockchain” gives the brief idea about blockchain technology. In 2008 a fellow called Nakamoto introduced the concept of blockchain technology. Presently number of applications are using this technology, specially where trustworthiness is required. Blockchain is best fit for wide-range application, hence it is used in decentralized cloud storage where it deals with huge number of data sets and transaction logs.

To enhance the security of blockchain a decentralized cloud storage with Ethereum blockchain technology is used. In this concept, issue of single point failure is solved at some extenti by using decentralized cloud storage where data is store in multiple nodes rather than single node. Centralized cloud storage has the issue where if one node goes down all the dependent users on that node get affected and not been able to retrieve their data, moreover it has reliability issues, high cost and performance degradation to overcome on these issues it is recommended to use decentralized cloud storage. A method called Smart Contract to store and retrieve the encrypted files. Ethereum was first invented by Vitalik Buterin in 2013 with the capability to work with decentralized cloud storage. Evolution of Ethereum is made by crowdfunding in 2014 which was available to the users in 2015. Now, Ethereum got lots of attention and reached up to that level where it is called as discoverer of blockchain and known as next generation of blockchain. In smart contract system like Ethereum logs of retrieving and storing data is recorded through blockchain technology. This network consistently remains aware of if any new entry is going to be happens and results in the form of transaction. Initiate the Ethereum is similar to adding new entry to control scheme of transaction. With the help of blockchain technology makes all the transactions non-destructive and non-repudiation. Therefore, the information of transaction is protected.

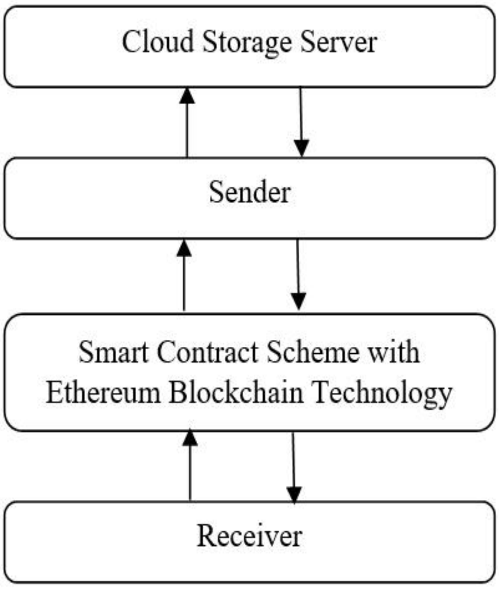

Fig 3 (a). Concept of system with Ethereum Blockchain Technology [3]

In Fig 3 (a) Smart contract scheme is developed. Data owner stores data. In this scheme, all the related information about data being upload with encryption to the cloud server. Then the data user request to access the data, response to this action is given by data owner who allocates some amount of time to access data. Once time given by data owner, user needs to access that data in given time, if data user wishes to access that data it requires to charge as per data owners demands. Now data user is allowed to access data as he has some amount of time to download the data which is store on cloud.[3] Yinghui Zhang, Robert H. Deng, Jiangang Shu, Kan Yang, Dong Zheng; in their paper title “TKSE: Trustworthy Keyword Search Over Encrypted Data with Two-Side Verifiability via Blockchain” presents a method which enhance the security of the system where two side verification is done, first user side verification is perform, second server side verification is performed. However, server-side verification takes in consideration that data owner can upload any invalid or malicious data to the cloud server. Therefore, server-side verification plays very important role to verify that the user is pre-register to use the service of putting his data on cloud storage. If user is not a valid user then he will not be able to use cloud services. After realization of keyword search on remote encrypted data, Song et al, contribute searchable encryption method in symmetric scheme where every keyword is encrypted independent using two-layer encryption method. Boneh et contribute public key based searchable encryption technique. Li et al contribute fuzzy keyword searching for encrypted data in cloud computing. Curtmola et al introduce two index-based methods and Li et al also contribute privacy aware data queries in cloud computing. Malicious cloud servers outsourced invalid encrypted data and some issues are faced in replication of data like integrity. To resolve this problem server-side verification is used.[4] G. Abinaya, Preksha Kothari, Alex Pavithran KP, Manasi Biswas, Farheen Khan; in their paper title “Block Chain Based Decentralized Cloud Storage” discussed two main issues that are rarely seen in traditional cloud services. The first one is, access provided to the user by using username and password which is not enough secure and second one is data stored in cloud storage is secure or not, if it is secured, then what kind of encryption algorithm is use to encrypt that data and what extent it able to protect that data. There are different algorithms use to encrypt and decrypt data in which one thing is common, they use same key for encryption and decryption.

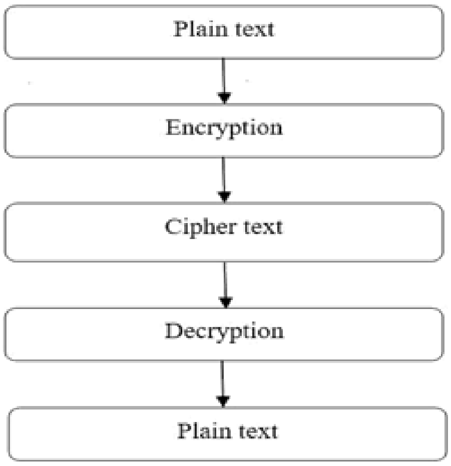

Fig 4 (a). Method used in traditional Algorithms [5]

To achieve higher security of such mechanism is developed which gives the guarantee of three parameters of data security which is confidentiality, integrity, accessibility. The proposed approach is split into following three steps.

A) Encryption of files: Authentication encryption method is used to encrypt data files if any alteration is done in data user can identify data is tampered. Encrypted data blocks are divided into segments of 4 KB with different encryption keys. Nonce for every block of data must be increasing in same order (e.g. if it starts from 2 then it will be like 2,4,6,8… so on) from where it starts. If it reaches to its maximum representable value it starts from 0. To avoid reordering attacks, the segment number is deterministically chosen for starting nonce. If multiple blocks are uploaded in this case, nonce will be starts from number of blocks and number of segments being uploaded.

B) Breaks into parts: File is break into parts after encryption process it is more secure procedure to ensure confidentiality, integrity and availability. User has complete control on private key and hence he is the only person who is able to access encrypted file. After this process file is being ready to store on cloud server. For the reliability purpose three copies of file is stored on network. Therefore, it is argued that the while storing data on cloud decentralized cloud storage is reliable option. Because the number of nodes is equally proportional to the availability of data.

C) **File Distribution:** Currently the rate of data stored on cloud is increasing day by day. Data theft not only caused by weak authentication, weak password, it may be possible the storage medium is not secure enough of protect data from attackers. Authentication problem can be solved by one-time-password using mobile or token. But the actual problem is, the place where data is kept is secured or not. If it is not secure then it becomes an attractive point of data stealing, data altering and due to such issues security of data is compromised. The current structure of cloud structure is performed through centralized cloud structure and it is not secure perspective of data integrity, confidentiality, availability. By these cloud structure many problems can be faced by user which can be solved using blockchain technology. In this paper [5] possible solution is given by using decentralized cloud storage using blockchain technology which is given in Fig 5 (a).

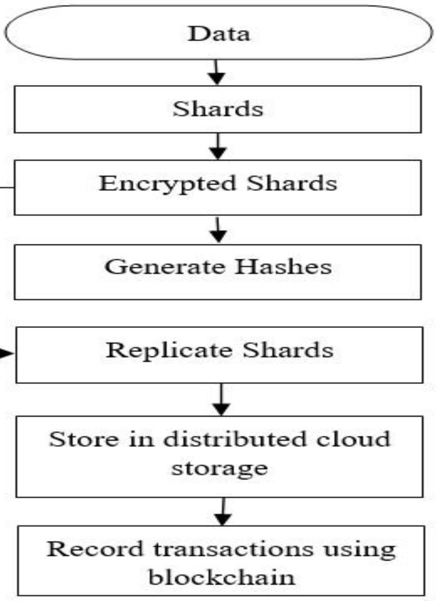
Data
Shards
Encrypted Shards
Generate Hashes
Replicate Shards
Store in distributed cloud storage
Record transactions using blockchain

Fig 5 (a). Decentralized cloud storage [5]

In traditional cloud storage there is no data registry system like blockchain technology which tracks the confidentiality of data and also, they do not have any technique to identify whether the data we are uploading to the storage is already placed or not. This kind of storage system does not create additional copy of data in case of inactive server which stores master data. Where as in case of decentralized cloud storage it is characterized by multiple nodes that use to store data in decentralized manner are independent resources which are fragmented in shards allocated to different nodes. This technique is achieved by blockchain technology. For decentralized cloud storage Sia, Storj, IPFS services used, if user wants to give this storage to other users it is possible and if he wants then he will charge to the other user who wish to store his data on storage. However, security concern sluggish performance of system perception of loss of control may be faced due to multiple and independent nodes present in decentralized structure.[5] Trends Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang; in their paper title “An Overview of Blockchain Technology: Architecture, Consensus, and Future” actual implementation of blockchain is given. Blockchain is concept where transactions are kept in sequence to track what kind of operations made by user.

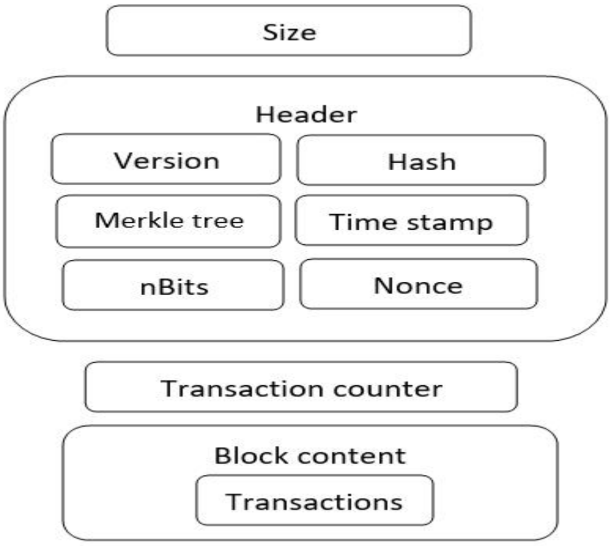

Fig 6 (a). Architecture of blockchain continuous sequence [6]

- Size: Contains size of block
- Header: It is actual data which is break in chunk of pieces. This block contains some information about block such as version, hash, Merkle tree, time stamp, nBits, nonce.
- nBits: The header of previous block is appended to next block which is called hash. This hash block is target to nBits.
- Nonce: This starts with 0 and gets increases in same way.
- Hash: It is header block.
- Time stamp: Contains value of every record which is being update with respect to time.

- Transaction counter: It contains each detail about transactions. This block is designed by using asymmetric cryptography mechanism to verify authentication.

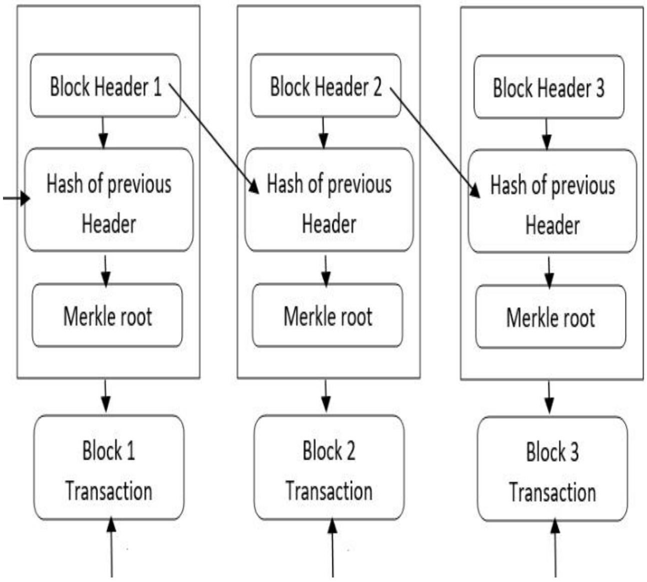

Fig 6 (b). Block Structure of Blockchain [6]

As shown if Fig 6 (b) it consists of block header which remains at the top of the data block and contains the information to which is the next target block and then appended to next block of data. Now, where this header block is pointed to the next block it is called hash block. All the hash and header of block is stored in Merkel root block. Combination of header, hash and Merkle root is then combined in single block and whatever the transactions is made by blocks is kept in single block which is called block of transaction. With the combination of all these blocks forms structure of blockchain where alteration of blocks is very difficult. Hence, in chain of blocks if even single block is altered or try to replace then it is not possible to recover the original data.

On the other side, if size of block is large it requires large space and reduces the speed of operation on network. Therefore, to maintain a balance between security and size of blocks is big challenge. However, some solution is needs to be given to fix these issues. Additionally, it may be possible that privacy theft is also possible in blockchain even when the user accesses his data through his public and private key. There are so many sources where information is available but lots of study on a blockchain is remaining.[6]

III. COMPARISON BETWEEN LITERATURE PAPERS

Table 1: Comparison between papers

Sr. No	Parameters	Paper 1	Paper 2	Paper 3	Paper 4	Paper 5	Paper 6
1	Algorithm	SEPSE	AONT	CP-ABE	TKSE	SHA-256	Consensus
2	Smart Contract Mechanism	Not Used	Distributed Hash Table	Ethereum Technology	Multiparty protocols-based Bitcoin blockchain	Token Method	Consensus Algorithm
3	Cloud Storage	DCS	DCS	DCS	-	DCS	DCS
4	Keyword Guessing Attack	PEKS with Fuzzy to resist KGA	-	-	Elliptic Curve Digital Signature Algorithm	-	-
5	Challenges	To resist KGA	Loss of control	To achieve CP-ABE	To achieve payment without third party	DoS-attacks	Privacy leakage, Selfish Mining

IV. CONCLUSION

Currently, the security of an electronic data is most important. As user store his data on cloud storage there might be chances of altering or modifying data because cloud storage will always remain attractive place for intruders to steal data. Due to this reason encryption algorithm is necessary to protect that data which makes it in unreadable form and to extraction of information from that data block is will become unachievable for intruder.

By using blockchain technology it limits to data alteration and modification due to its hash-based function, if block of data does not have header value of next block it cannot be appended. Furthermore, to improve security of blockchain technology various methods can be shown in this paper can be used.

REFERANCES

1. Yuan Zhang, Chunxiang Xu, Jianbing Ni, Hongwei Li, Xuemin Shen - Blockchain-assisted Public-key Encryption with Keyword Search against Keyword Guessing Attacks for Cloud Storage, IEEE Transactions on Cloud Computing, vol. 2168-7161 (c) 2019.
2. Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, Pierangela Samarati - Securing Resources in Decentralized Cloud Storage, Ieee Transactions on Information Forensics and Security, Vol. Xx, No. Yy, Month 2019.
3. Shangping Wang, Xu Wang, And Yaling Zhang - A Secure Cloud Storage Framework with Access Control Based on Blockchain, IEEE Access, Volume 7, 2019.
4. Yinghui Zhang, Robert H. Deng, Jiangang Shu, Kan Yang, Dong Zheng - TKSE: Trustworthy Keyword Search Over Encrypted Data with Two-Side Verifiability via Blockchain, IEEE Access, Volume 6, 2018.
5. G. Abinaya, Preksha Kothari, Alex Pavithran KP, Manasi Biswas, Farheen Khan - Block Chain Based Decentralized Cloud Storage, International Journal of
6. Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-4, April 2019.
7. Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang - An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 978-1-5386-1996-4/17 $31.00 © 2017 IEEE DOI 10.1109/BigDataCongress.2017.85.
8. Simanta Shekhar Sarmah - Application of Block chain in Cloud Computing, IEEE Computer Society, 978-1-5386-1996-4/17 $31.00 © 2017 IEEE DOI 10.1109/BigDataCongress.2017.85.
9. Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone - Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments, e First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy, 2017.
10. Jin Ho Park, Jong Hyuk Park - Blockchain Security in Cloud Computing: Use Cases, Challenges and Solutions, Symmetry 2017, 9, 164; DOI:10.3390/sym9080164.
11. Vidhya Ramani, Tanesh Kumar, An Braeken, Madhusanka Liyanage, Mika Ylianttila - Secure and Efficient Data Accessibility in Blockchain based Healthcare Systems, Research gate, DOI: 10.1109/GLOCOM.2018.86472221.
12. Yuan Zhang, Yunlong Mao, Minze Xu, Fengyuan Xu and Sheng Zhong - Towards Thwarting Template Side-channel Attacks in Secure Cloud Deduplications, DOI 10.1109/TDSC.2019.2911502, IEEE Transactions on Dependable and Secure Computing.

AUTHORS PROFILE

Mr. Akshay D. Babrekar is pursuing his Masters in Information Technology from Pimpri Chinchwad College of Engineering permanently afflicted to Savitribai Phule Pune University. His area of research interest is DIC, EDC, IoT**.**

Mrs. Rohini G. Pise is currently working as an assistant professor in IT Department, Pimpri Chinchwad College of Engineering, Pune. Her area of research interest is Computer security, Information security, Internet of Things, Cryptography.