SECURED CLOUD STORAGE USING BLOCKCHAIN TECHNOLOGY

Shubham Singh[1], Snehal Gite[2], Neha Bahare[3], Prof. A. V. Raut[4]

[1] *Student, Computer Engineering, LGNSCOE, Maharashtra, India*
[2] *Student, Computer Engineering, LGNSCOE, Maharashtra, India*
[3] *Student, Computer Engineering, LGNSCOE, Maharashtra, India*
[3] *Professor, Computer Engineering, LGNSCOE, Maharashtra, India*

ABSTRACT

There are many security issues related to cloud data storage and sharing now-a-days. Security of cloud storage can be achieved more efficiently by using this system. To protect the confidentiality of sensitive data while supporting deduplication, the convergent encryption technique has been proposed to encrypt the data before outsourcing. To better protect data security, the first attempt to formally address the problem of authorized data deduplication. In this system the data is divided into blocks using block chain technology and each block has unique hash value and the hash value of current block will be stored in previous block. If any unauthorized person tries to access the data the hash value will get changed and the link will be broken for further blocks. The data deduplication can be avoided and data integrity can be maintained. AES algorithm is used for encryption purpose and 'k-n secret sharing' and 'SHA' algorithm is used for hashing purpose and data distribution purpose. Security analysis demonstrates that our scheme is secure in terms of the definitions specified in the proposed security model. Using this system, the security can be achieved during data sharing and storage over cloud computing.

Keyword: *Cloud computing, Blockchain, HASH value, AES, SHA, Data integrity, Security, Encryptio, Decryption, Key/Token.*

1. INTRODUCTION:

Data is most important asset now a days. It is Strategy to drive a business decision in many different fields like health, education, finance, insurance and public administration. As the computer-aided human activities are relying more on data, thus trusting the data has become crucial. At the same time, the important role of data has become main target for cyber-attacks, which aim at undermining fundamental properties of CIA (Confidentiality, Integrity, Availability) that data should be exhibit in order to be trusted.

The Cyber-attacks on CIA properties may cause different impairments on data trust according to the undermined property. Specifically, sabotaging availability prevent data retrieval for a temporary period of time, but operations are performed or resumed as soon as data are accessible again. Compromising confidentiality discloses instead private data and cannot be reverted, but original data are still available for use, at least to the extent allowed by the inflicted damage (i.e., an organization which is victim of data leakage may have to face economic problems). Instead, tampering with integrity of data is highly damaging attack that always paves dangerous or critical issues to data trust. Indeed, tampering with data can go undetected and can maliciously drive the operations, by deleting specific entries (i.e., removing inconvenient traces) or by modifying particular sections of data (i.e., changing behavior of data consumers).

Block chain was introduced in 2008 as the basis of Bitcoin protocol. Bitcoin is a combination of cryptography and distributed systems enables value to be transferred as data gets transferred over internet. Over the past 2-3 years, Blockchain has emerged as visible for multi-party business processes addressing and value exchange without sharing complex data schemes and third-party intermediaries. At its core, Blockchain is a secure, distributed, shared

ledger- a new shared data structure where bank can store or record their transactions and work together to validate updates. Smart contracts act as a shared tool to govern the changes to the underlying ledger in accordance to pre-agreed rules or terms.
This records which are shared, enables organizations to collaborate more efficiently- and because every member in the network holds the record of every transaction, it is nearly impossible to manipulate the data or change the data undetected. While cryptocurrencies like Bitcoin were responsible for making the blockchain technology popular, blockchain protocols with business-oriented uses are now proliferating, revealing the value of this innovative technology to disrupt business models and transform operations. This offer three key benefits:

Fig -1 Benefits of Blockchain

1.1 Blockchain technology for cloud storage:

Cycling back to the idea of client-server computing, workloads will still be centrally managed and controlled with a blockchain approach. Essentially, even if processing the data is physically distributed, the workloads remain logically centralized. This is different than a hybrid cloud approach where companies maintain data both on the public and private cloud. Blockchain creates a decentralized and distributed storage marketplace. Blockchain technology for cloud storage can be a rather complex data structure to understand. This graphic from Blockgeeks helps explain it a bit.

2. LITERATURE SURVEY:

1.Anonymous and Traceable Group Data Sharing in Cloud Computing:- Group data sharing in cloud environments has become a hot topic in recent decades. With the popularity of cloud computing, how to achieve secure and efficient data sharing in cloud environments is an urgent problem to be solved. This paper focuses on enabling data sharing and storage for the same group in the cloud with high security and efficiency in an anonymous manner. By leveraging the key agreement and the group signature, a novel traceable group data sharing scheme is proposed to support anonymous multiple users in public clouds. On the one hand, group members can communicate anonymously with respect to the group signature, and the real identities of members can be traced if necessary. On the other hand, a common conference key is derived based on the key agreement to enable group members to share and store their data securely. Note that a symmetric balanced incomplete block design is utilized for key generation, which substantially reduces the burden on members to derive a common conference key.

2.On-Blockchain-Based Anonymized Dataset Distribution Platform In this paper, we design a distributed platform for anonymized dataset trading without any centralized trusted third party. The platform consists of peers and consensus based blockchain mechanism, and each peer acts as a data broker, data receiver, or verifier for blockchain in a data transfer transaction. A data broker collects data from data owners under their consent for data trading. The Privacy Policy Manager (PPM)manages the consent information and confirms them on behalf of data owners, when data distribution is requested from data broker. We implement a prototype system of the platform using an open-source blockchain mechanism, Hyperledger Fabric, and provide evaluation results of the prototype system.

3. Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds Cloud-Trust is used to assess the security level of four multi-tenant IaaS cloud architectures equipped with alternative cloud security controls and to show the probability of CCS penetration (high value data compromise) is high if a minimal set of security controls are implemented. CCS penetration probability drops substantially if a cloud defense in depth security architecture is adopted that protects virtual machine (VM) images at rest, strengthens CSP and cloud tenant

system administrator access controls, and which employs other network security controls to minimize cloud network surveillance and discovery of live VMs.

3.SYSTEM ARCHITECTURE:

In this system architecture there are three main components which are as follows:
1. User.
2. Public Cloud.
3. Private Cloud

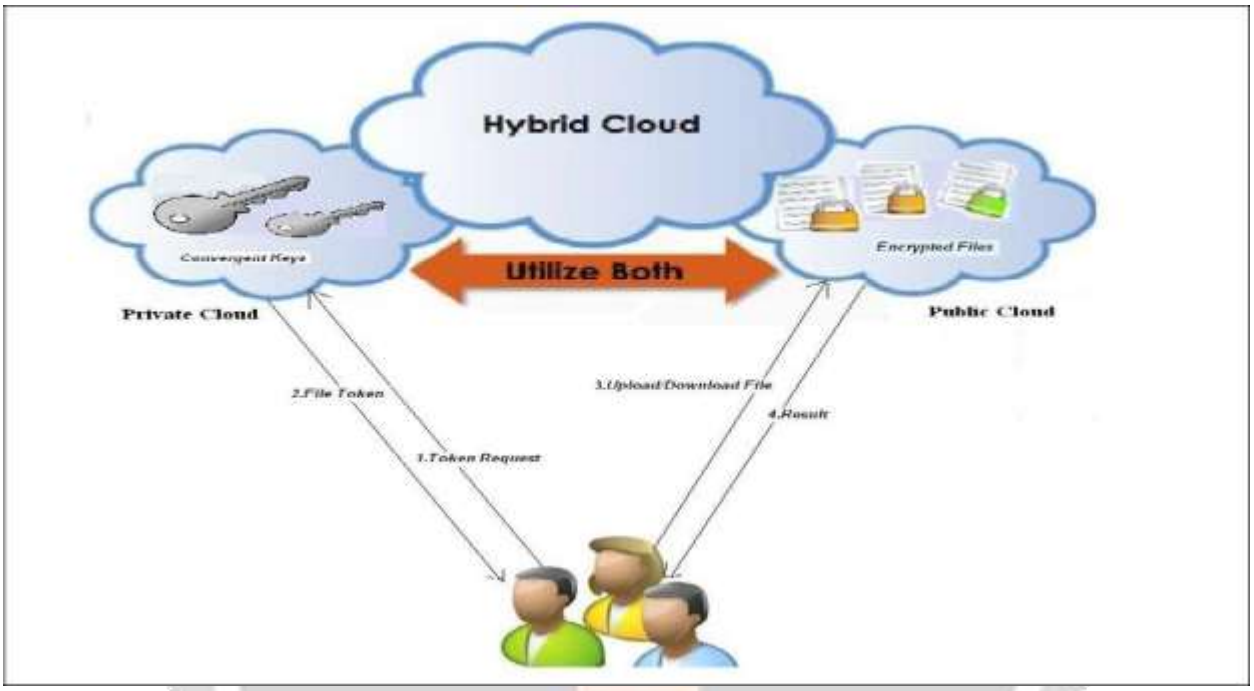

Fig -2 System architecture

First if the user wants to upload the files on the public cloud which is available to all, then user will first encrypt that file with the convergent key and then sends it to the public cloud at the same time user also generates the key for that file and sends that key to the private cloud for the purpose of security. In the public cloud we use one algorithm for encryption, which is used to divide the data into blocks of files which is entered in the public cloud. Hence it also minimizes the bandwidth. That means we requires the less storage space for storing the files on the public cloud. In the public cloud any person that means the unauthorized person can also access or store the data so we can conclude that in the public cloud the security is not provided. In general for providing more security user can use the private cloud instead of using the public cloud. User generates the key at the time of uploading file and store it to the private cloud. When user wants to downloads the file that user had uploaded, user sends the request to the public cloud. Public cloud provides the list of files that are uploads the many user of the public cloud because there is no security is provided in the public cloud. When user selects one of the file from the list of files then private cloud sends a message like enter the key!. User has to enter the key that he generated for that file. When user enter the key, the private cloud checks the key for that file and if the key is correct that means user is valid then private cloud give access to that user to download that file successfully. Then user downloads the file from the public cloud and decrypt that file by using the same convergent key which is used at the time of encryption of that file. In this way user can make a use of the architecture.

4. MATHEMATICAL MODEL:

- **Input: I = F, U, P**
  where,
  F = File to be uploaded.
  U = User name assigned to user. P = Password given by user.

- **Output: O = O1, O2, O**
  where,
  O1 = Duplication is found.
  O2 = Duplication is not found.
  O3 = Upload/Download a original file.

- **Functions: F = F1, F2, F3,F4,F5,F6,F7,F8,F9,F10**
  Where,
  F1 = User Registration.
  F2 = Login.
  F3 = Upload a file.
  F4 = Encrypt a file.
  F5 = Signature calculate.
  F6 = Store to private cloud.
  F7 =Check the key/token.
  F8 = Store in public cloud.
  F9 = Decrypt a file.
  F10= Download a original file.

5.CONCLUSIONS:

Thus, by implementing blockchain on cloud computing we can achieve security over the data stored on the cloud storage. Data cannot be tampered and cannot be accessed by unauthorized person, if tried to access by unauthorized person then the key/token value will not get matched and the hash value will be changed and the data will be safe and secured. We also presented several new security constructions supporting authorized duplicate key check in hybrid cloud architecture, in which the security-check tokens of files are generated by the private cloud server with private keys. In this way, the operation of storing and retrieving the data in cloud has become secured.

6. REFERENCES:

[1]. Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, and Dawn Song. Provable data possession at untrusted stores. In Proceedings of the 14th ACM conference on Computer and communications security, pages 598–609. ACM, 2007.
[2]. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In 2015 IEEE Symposium on Security and Privacy, pages 104–121. IEEE, 2015.
[3]. Ittay Eyal, Adem Efe Gencer, Emin Gu¨n Sirer, and Robbert Van Renesse. Bitcoin-NG: A scalable blockchain protocol. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), pages 45–59, 2016.
[4]. Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications, pages 281–310. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.
[5] Mehdi Sookhak, Abdullah Gani, Hamid Talebian, Adnan Akhunzada, Samee U. Khan, Rajkumar Buyya, and Albert Y. Zomaya. Remote Data Auditing in Cloud Computing Environments: A Survey, Taxonomy, and Open Issues. ACM Comput. Surv., 47(4):65:1–65:34, May 2015.

[6] Francesco Paolo Schiavo, Vladimiro Sassone, Luca Nicoletti, and Andrea Margheri. FaaS: Federation-as-a-Service, 2016. Technical Report. Available at https://arxiv.org/abs/1612. 03937.
[7] Bojan Suzic, Bernd Pru¨nster, Dominik Ziegler, Alexander Marsalek, and Andreas Reiter. Balancing Utility and Security: Securing Cloud Federations of Public Entities. In C&TC, volume 10033 of LNCS, pages 943–961. Springer, 2016.
[8] Mor Weiss, Boris Rozenberg, and Muhammad Barham. Practical Solutions For Format-Preserving Encryption. CoRR, abs/1506.04113, 2015.
[9] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014.
[10] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," NIST Spec. Publ., pp. 800–144, 2011.
[11] P. Mell and T. Grance, "The NIST Definition of Cloud Computing." NIST, 2011.
[12] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud Migration Research: A Systematic Review," IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 142–157, 2013.
[13] M. Hines, U. Deshpande, and K. Gopalan, "Post-copy live migration of virtual machines," ACM SIGOPS Oper. Syst. Rev., vol. Volume 43, no. Issue 3, Jul. 2009.
[14] M. I. Gofman, et. al., "SPARC: A Security and Privacy Aware Virtual Machine Checkpointing Mechanism," in Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, 2011, pp. 115–124.
[15] Mandiant, "M-Trends 2010: the Advanced Persistent Threat." Mandiant, 2010.
[16] D. X. Song, D. Wagner, and X. Tian, "Timing Analysis of Keystrokes and Timing Attacks on SSH," in USENIX Security Symposium, 2001, vol. 2001.
[17] J. Fortes, "Cloud Computing Security: What Changes with Software-Defined Networking?," presented at the ARO Workshop on Cloud Security, Mar 11, 2013.