DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6341

Volume 9, No. 6, November-December 2018

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

BLOCKCHAIN-BASED SECURITY ARCHITECTURE FOR DISTRIBUTED CLOUD STORAGE

Nishant.G.Hulwan
Computer Department
MGM's College of Engineering and Technology
Navi Mumbai, India.

Prof. Sachin Chavan
Computer Department
MGM's College of Engineering and Technology
Navi Mumbai, India

Abstract: Cloud Computing is the use of hardware and software to deliver a service over a network (typically the Internet). It offers various data storage, infrastructure, and application. Moreover, we can say that the cloud is something which is present at a location. Cloud computing refers to manipulating and access hardware and software resources. Cloud computing based on service models. In this thesis paper, Our primary objective is to propose an auditing project for users who use cloud data sharing services which are attributed by multi-user modification, public auditing, high error awareness, probability efficient user nonexistent as well as a pragmatic computational and communication auditing performance. Our layout for this paper would be to resist user duplicate attack; while we are doing this, we won't consider any current methods that support multi-user modifications.

Keywords: Cloud Computing, Block Chain, Third Party Auditor,

1. INTRODUCTION

From the past, it's straightforward for a cloud user to share & communicate data all over, because of the enormous development of cloud storage services. Users' confidence & security of their shared data on the cloud, many techniques have proposed for maintaining, low cost, agility, multi-sharing, and reliability. Batch auditing of heterogeneous task is also efficiently supported in our plan, ample of experiments on Amazon Elastic Compute Cloud and divergent client devices (immediate and mobile devices) show that our design approves the client to scrutinize the integrity of a shared file with a continuous computational cost of 340ms on Desktop PC (4.6s on mobile devices) and a leap communication cost of 77kb for 99% error observation probability with data misconduct rate of 1%.

Maybe the confidential data get changed by service providers. It is required to eliminate the unwanted data for maintaining the privacy of cloud files. To determine this drawback, we propose a new framework which is Reliable and Scalable Secure Method to Store and Share Secrete Data for groups in Cloud as proposed by **Xuefeng Liu [1]**.

The support of dynamic data, public decency examine, low communication/ computational evaluate cost, low cache overhead. However, most of these procedures consider that only the indigenous data owner can modify the shared data, which examines these techniques to client read-only applications this was the main focus of **Jiawei Yuan [2].**

Moreover usage of blockchain in this architecture, an adversary cannot get anything about the raw users' file data from the blockchain, as only URLs and hash values stored in it. From previous failed attempts there have been new attempts which are considered far more realistic and allowing many cloud users to rebuild their data with confidentiality.

However, these attempts that have been made are not yet achievable there needs to be more effort. The main drawback is due to cramped area and high price system that requires high detection system.

```
/*
MySQL Data Transfer
Source Host: localhost
Source Database: blockchain
Target Host: localhost
Target Database: blockchain
Date: 01-Sep-18 9:58:21 PM
*/

SET FOREIGN_KEY_CHECKS=0;
-- ----------------------------
-- Table structure for blockchain
-- ----------------------------
DROP TABLE IF EXISTS `blockchain`;
CREATE TABLE `blockchain` (
  `blockChain_id` bigint(11) NOT NULL AUTO_INCREMENT,
  `file_id` bigint(255) DEFAULT NULL,
  `file_path` varchar(255) DEFAULT NULL,
  `hashValue` varchar(255) DEFAULT NULL,
  `user_name` varchar(255) DEFAULT NULL,
  `file_name` varchar(255) DEFAULT NULL,
  `date` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`blockChain_id`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
```

II. EXISTING SYSTEM

In the existing methods that validate multi user modifications we need to do a batch auditing of multiple files that will be stored and measured.

Only the data holder holds secret keys and can reorganize the statistics, and all other users who share data with the data manager only have to read the permission rules. If these solutions are insignificantly extended to support multiple writers who write data with data sincerity promise, the owner who owns the data has to stay online, collecting regeneration of data from other users who have used the data and regenerating authentication tags for them as proposed by **Pranjali waghe [3].**

```
-- ----------------------------
-- Table structure for create_group
-- ----------------------------
DROP TABLE IF EXISTS `create_group`;
CREATE TABLE `create_group` (
  `create_group_id` bigint(20) NOT NULL AUTO_INCREMENT,
  `group_name` varchar(255) DEFAULT NULL,
  `owner_id` bigint(20) DEFAULT NULL,
  PRIMARY KEY (`create_group_id`)
) ENGINE=InnoDB AUTO_INCREMENT=7 DEFAULT CHARSET=latin1;

-- ----------------------------
-- Table structure for create_members
-- ----------------------------
DROP TABLE IF EXISTS `create_members`;
CREATE TABLE `create_members` (
  `member_info_id` bigint(20) NOT NULL AUTO_INCREMENT,
  `group_member_name` varchar(255) DEFAULT NULL,
  `create_group_id` bigint(20) DEFAULT NULL,
  `registration_id` bigint(20) DEFAULT NULL,
  PRIMARY KEY (`member_info_id`)
) ENGINE=InnoDB AUTO_INCREMENT=17 DEFAULT CHARSET=latin1;

-- ----------------------------
-- Table structure for file_upload
-- ----------------------------
DROP TABLE IF EXISTS `file_upload`;
CREATE TABLE `file_upload` (
  `file_id` bigint(50) NOT NULL AUTO_INCREMENT,
  `user_name` varchar(255) DEFAULT NULL,
  `upload_date` varchar(255) DEFAULT NULL,
```

This kind of meaningless extension introduces an enormous workload among users. This kind of situation occurs many times, and it doesn't matter if it's done internationally or locally, with existing cloud storage user policy.

As our design itself accurately supports batch analyzing, we can analyze all development files at the same time to save cost. Thus, our stratagem can be easily applied to current modules to support integrity among users and assurance without modifying their original blueprint.

```
  `file_path` varchar(255) DEFAULT NULL,
  `file_size` bigint(255) DEFAULT NULL,
  `file_name` varchar(255) DEFAULT NULL,
  `user_id` bigint(55) DEFAULT NULL,
  `fileExtension` varchar(255) DEFAULT NULL,
  `fileCount` bigint(55) DEFAULT NULL,
  `category` varchar(255) DEFAULT NULL,
  `PATH` varchar(255) DEFAULT NULL,
  `encryptName` varchar(255) DEFAULT NULL,
  `publickey` varchar(255) DEFAULT NULL,
  `status` varchar(255) DEFAULT NULL,
  `hashValue` varchar(255) DEFAULT NULL,
  `email` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`file_id`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=utf8;

-- ----------------------------
-- Table structure for group_file_upload
-- ----------------------------
DROP TABLE IF EXISTS `group_file_upload`;
CREATE TABLE `group_file_upload` (
  `group_by` bigint(20) NOT NULL AUTO_INCREMENT,
  `owner_id` bigint(20) DEFAULT NULL,
  `file_id` bigint(20) DEFAULT NULL,
  `group_name` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`group_by`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
```

III. PROPOSED SYSTEM

In this method we are going to make a survey of all the servers just to ensure that there are no illegal activities going on. Such a service, a series of schemes need to be submitted. However, for most of us, these existing schemes are for the data owner itself no one can access it without data owner. In the cloud, we have both reading and writing privileges and introduced a public integrity auditing scheme using ring signature-based homo-morphic authenticators — nevertheless, the scalability of reference.

Last but not the least, our proposed project plan allows us to go through the different collection of integrity auditing operations for multiple tasks (files) through our batch integrity auditing technique, which promotes our project regarding inspecting systematic and data manipulation detecting the possibility.

```
  `email` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  `confirm_password` varchar(255) DEFAULT NULL,
  `name` varchar(255) DEFAULT NULL,
  `mobile_no` bigint(20) DEFAULT NULL,
  `address` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`register_id`)
) ENGINE=InnoDB AUTO_INCREMENT=14 DEFAULT CHARSET=utf8;

-- ----------------------------
-- Table structure for requested_files
-- ----------------------------
DROP TABLE IF EXISTS `requested_files`;
CREATE TABLE `requested_files` (
  `id` bigint(20) NOT NULL AUTO_INCREMENT,
  `requester_id` bigint(20) DEFAULT NULL,
  `file_id` bigint(20) DEFAULT NULL,
  `file_name` varchar(255) DEFAULT NULL,
  `owner_id` bigint(20) DEFAULT NULL,
  `status` varchar(255) DEFAULT NULL,
  `req_id` bigint(20) DEFAULT NULL,
  `operation` varchar(255) DEFAULT NULL,
  `requester_email_id` varchar(255) DEFAULT NULL,
  `requester_name` varchar(255) DEFAULT NULL,
  `email_generate_key` varchar(255) DEFAULT NULL,
  `owner_name` varchar(255) DEFAULT NULL,
  `requester_date` varchar(255) DEFAULT NULL,
  `uploaded_date` varchar(255) DEFAULT NULL,
  `file_extension` varchar(255) DEFAULT NULL,
  `encryptName` varchar(255) DEFAULT NULL,
  `file_path` varchar(255) DEFAULT NULL,
  `viewed_status` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
```

The Third party administrator refers to any party that checks the integrity of data stored on the cloud. We know that how much honesty is important integrity is nothing but to ensure that data is safe, reliable and efficient. Entrusted input is devoid of Integrity: In this architecture, an adversary cannot get anything about the raw users' file data from the block-chain, as only URLs and hash values stored in it.

(A) Methods and Materials

The edition of the same file without downloading is done by allocating time intervals and third-party authority which assigns a particular time for a specific user does it. This authority watches the all type of action from the user to allocate the time of the user respectively. The specialty of this time allocation is only the valid user can access a file at that time, so no other user cannot able to access the data. Hence the time interval mainly used for avoiding the same files access collision. It reduces cloud space by taking a low time to upload a file no need to download files.

Different Methods in Cloud Computing

(a) Public cloud : In public cloud resources are provided on Internet by pay per use model

(b) Private cloud : In private cloud an entire data is owned by an organization and operated internally

(c) Hybrid cloud: In hybrid cloud data is provided by both private and public cloud.

Different types of cloud Computing

(a) **Software as a Service:** It involves license applications of the customers. These licenses are provided as payment through model or on demand model.

(b) **Infrastructure as a Service:** This method involves everything from operating systems to service and IP based connectivity.

```
-- ----------------------------
-- Table structure for uploaded_image
-- ----------------------------
DROP TABLE IF EXISTS `uploaded_image`;
CREATE TABLE `uploaded_image` (
  `image_id` bigint(20) NOT NULL,
  `email` varchar(255) DEFAULT NULL,
  `date` varchar(255) DEFAULT NULL,
  `image_address` varchar(255) DEFAULT NULL,
  `register_id` bigint(20) DEFAULT NULL,
  PRIMARY KEY (`image_id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- ----------------------------
-- Table structure for user_upload
-- ----------------------------
DROP TABLE IF EXISTS `user_upload`;
CREATE TABLE `user_upload` (
  `userupload_id` bigint(20) NOT NULL AUTO_INCREMENT,
  `user_id` bigint(20) DEFAULT NULL,
  `file_id` bigint(20) DEFAULT NULL,
  `shared_with` varchar(255) DEFAULT NULL,
```

IV. IMPLEMENTATION METHODOLOGY

Key Generation In our scheme the critical generation algorithm generates the public key (PK), a master key (MK), secret key (SK) of the user. There is a K number of users in group sharing data. Master, a user, is an owner of data. So all the user can access and modify the shared data are in the cloud. PA performs data integrity auditing for adjusted data of the user. Key Generation as the part of set up algorithm generates public keys (PK), master keys (MK) of the system and secret key (SK) of users. In our design each user has their secret key for data modification; Key generation is a proficiency which is used to store the data in a different methodology. Mainly the public key algorithm called RSA which plays a vital role in crucial generation technologies such as a single shared key. Which uses symmetric key algorithm through data is stored very securely. Since the public key algorithm employs two keys namely public and a private key, and the public key is made as visible to end user & they can use that public key to encrypt the data and finish user can decrypt the data using the private key. In some conditions they keys have been generated using Random Number Generator technique, and it is very efficient that hackers cannot easily guess the keys and provide robust security proposed by **S.Monika1 [4]**.

V. USER REVOCATION

An advanced version of user revocation has proposed. In cloud computing users can easily modify the data or copy the data from respective users. So data integrity is very important to maintain Confidentiality. To maintain Confidentiality data is shared among the groups and blocks. It also uses the method of proxy re-signature to avoid downloading the signed block by the user. Finally, the integrity of the challenged file can be verified by the running verification algorithm as stated by **Siva Sakthi [5]**.

VI. INTEGRITY AUDITING

Integrity auditing is a scheme where users can share their data on cloud. This is based on a method called ring signature. In this scheme a user revocation is not considered and the auditing size grows from cloud size to data size. Moreover, if a cloud tag is responsible for an update it is compromised during the user revocation process as proposed by **Swapnil Deshmukh [6]**.

(A) How to use Cloud Storage?

Cloud storage is a technique in which it lets you store the data on the Internet or other network to a storage system which is offsite and managed by the third party. Cloud Storage system which includes storage such as back up emails, pictures, videos, and other personal files. When user access the list in the cloud storage access to allow the data to view and modify the content directly from the cloud storage as proposed by **C.Pavani1 [7].**

(B) Public Verification

When user revocation occurs our scheme only required the master user to send one group element to the cloud and also add owner group element to a public key — public integrity auditing technique is proposed regarding efficient and data corruption detection probability. Many schemes have been introduced for public verification and cloud storage users allow using their data to cloud servers to save data storage. Mostly public verification is introduced to improve third party authority and to maintain data integrity.

VII. TIME ALLOCATION

To access the file from the cloud storage the user sends a secret key of a particular file third party authority (TPA). TPA allocated the appropriate file modification time for the user when the time expired the access time for the user, so the time allotted for another user to access the same file within the particular term given to them.

VIII. THIRD PARTY AUTHORITY

Cloud computing is literally transforming how businesses work in market. One major aspect is that data is being centralized or outsourced to the cloud. From a different perspective including both users and IT professionals storing the data in a careful manner brings more appealing benefits to the market. Cloud computing has also brought new challenging threat towards outsourced data. CSP are separate administrative entities, data outsourcing is actually relinquishing ultimate control of data as proposed by **A. Hannah [8].**

IX. BLOCKCHAIN AS A TRADING MECHANISM

In this architecture, an adversary cannot get anything about the raw users' file data from the block-chain, as only URLs and hash values are stored in it.

(a) Algorithms:

This algorithm uses four methods as stated as follows

(1) **Key Generation**: Each user Generates its own key a random input is given to the user and it produces output which is a private key and public key.
(2) **Resigning key**: Resigning key is a key which is generated by cloud. This key is specially generated for the users who lie within the group.
(3) **Proof Verification**: A proof sign by the administrator is checked by verifier.
(4) **Regeneration of sign**: At the time of creation of the key users uses original data that computes a block for each signature. After revocation of user cloud resigns the block modified by revoked user.

RELATED SURVEYS ON BLOCKCHAIN TECHNOLOGIES

Year	Author	Main focus/contributions
2016	Tschorsch and Scheuermann [7]	Fundamental structures and insights of the core of the Bitcoin protocol and its applications
2017	Sankar et al. [29]	Feasibility and efficiency of consensus protocols in blockchain.
2017	Kaushik et al. [30]	A brief survey on bitcoin.
2018	Khalilov and Levi [31]	An overview and detailed investigation of anonymity and privacy in Bitcoin-like digital cash systems.
2018	Fernández-Caramés and Fraga-Lamas [24]	A review on developing Blockchain-based IoT (BIoT) applications.
2018	Conti et al. [32]	A systematic survey that covers the security and the privacy aspects of Bitcoin.

Advantages of Cloud Computing

Comprehensive solution for securing the cloud computing infrastructure can be based on cryptographic mechanisms of secure computation proposed by **Ahmad-Reza Sadeghi [9]**. These schemas allow for distributed computation of arbitrary functions of private (secret) inputs while hiding any information about the contributions to the services. These mechanisms provide calculation on encrypted data. We rectify several settings where secure computation in the cloud is needed. We address all of these settings in the following way:
(1) We hide the user's data from other users of the same cloud service.

(2) Protecting user data from the cloud provider

(3) Securing computation between several servers

(4) Achieving estimate between untrusting parties.

X. CONCLUSION

In this thesis paper, we introduce a secure data-sharing protocol that we are implementing with the block-chain-based cloud-storage architecture is presented. In the past Research, A meta-key mechanism compatible with existing architecture is introduced to arrange encryption keys with the user's private key. Proxy re-encryption with some revision is applied to make data to be shared with high efficiency as well as enhancement of security. Details about this safety have been analyzing including collusion attack resistance property that doesn't exist in most practical proxy re-encryption schemes.

XI. REFERENCES.

[1] Xuefeng Liu, Yuqing Zhang, Boyang and Jingbo Yan," Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, 2012.
[2] Jiawei Yuan, Shucheng Yu," Public Integrity Auditing for Dynamic Data Sharing with Multiuser Modification," IEEE Transactions on Information Forensics and Security,2015.
[3] Pranjali waghe, Mayuri Khaire, Oshika Shinde, Prof. Torana Kamble, " Public Integrity Auditing Using Group User Revocation For Shared Dynamic Cloud Data," International Journal of Recent Trends in Engineering & Research,2017.
[4] S. Monika1, M. Jawahar2, S.K. Murugaraja, "Data Sharing in Cloud Storage by RSA based Encryption," International Journal of Computer Science Trends and Technology, 2015.
[5] Siva Sakthi Janani.G1, Vinodhini.S2, Miss.Divya.G3, "Group User Revocation For Shared Dynamic Data In Cloud," International Journal of Science Technology and management,2016.
[6] Swapnil Deshmukh, Sourabh Dhivare, Prof.Mr. Harshad Dagade," Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption," International Journal of Scientific & Engineering Research,2018.
[7] C. Pavani1, S.Vasundra, "Enabling Secure Data Sharing Scheme in the Cloud Storage Groups," International Research Journal of Engineering and Technology,2017.
[8] A.Hannah, B.Gobinathan," A new privacy-aware public auditing scheme for cloud data sharing with group users," International Journal of current engineering and scientific research (IJCESR), 2018.
[9] Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy," Token-Based Cloud Computing! Secure Outsourcing of Data and Arbitrary Computations with Lower Latency".2010.