© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Peer to Peer File Sharing by Blockchain Using IOT

M. Amirtha Krishnan, C. Gowri Shankar, S. Arvind Raj, A. Ragavan

Information Technology, Anna University, SKP Engineering College, Tiruvannamalai, Tamil Nadu, India

ABSTRACT

Hadoop envisioned as the next-generation architecture of IT enterprise. It moves the application software and databases to the centralized large data centers. Sender using IBE does not required public key, but directly encrypts message with receiver's identity. Accordingly, receiver obtaining the private key associated with the corresponding identity from Private Key Generator (PKG) is able to decrypt such cipher text. The problem of ensuring the integrity of data storage in Hadoop. The task of allowing a Third-Party Auditor (TPA) to verify the integrity of dynamic data stored in the cloud. Aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. By using IOT layers we can able to track our files or data where it is currently located.

Keywords : Hadoop- PKG-Cloud Security- Block-Chain-Peer to Peer-IOT.

I. INTRODUCTION

Peer-to-peer programs can be an efficient way to share large files with others, such as personal video recordings or large sets of photos. Peer-to-peer is also used to ease direct communication between computers or device users. For example, Skype built its communications systems on Peer-to-peer technology. Hadoop envisioned as the next-generation architecture of IT enterprise. It moves the application software and databases to the centralized large data centers. Sender using IBE need not to look up public key and certificate, but directly encrypts message with receiver's identity. Accordingly receiver obtaining the private key associated with the corresponding identity from Private Key Generator (PKG) is able to decrypt such cipher text. A block is the "current" part of a blockchain which records some or all of the recent transactions, and once completed, goes into the blockchain as permanent database. By using the IOT layers we can able to track our files which we have sent or receiving the data.

II. METHODS AND MATERIAL

A. Existing System

To ensure the problem of data integrity, many schemes are proposed.

" PDP" Provable Data Possession model that ensure the possession of files on untrusted storages. PDP supports basic block operation with limited functionality.

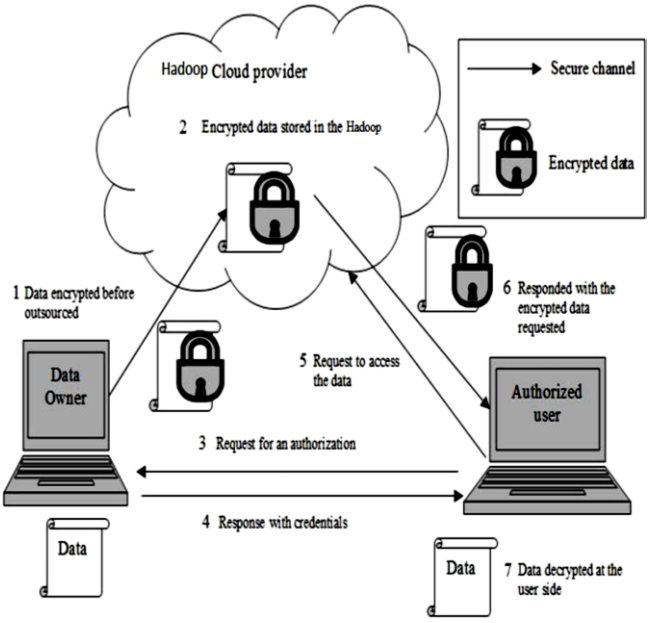
"POR" Proof of Retrievability model that involves in spot checking ,error correcting codes sentinels are embedded. POR does not supports public auditability "RSA" Algorithm only used. It only supports static data storage.

B. Proposed System

The TPA is to verify the integrity of dynamic data stored in the cloud. TPA can eliminates the involvements of client through auditing. TPA is trusted to assess the CSP's (Cloud Security and Privacy) storage security upon request from the user. To achieve efficient storage security, Merkle Hash Tree Construction for block tag authentication. By using Blockchian Technology We can view live transfers from many Clients and track the file using IOT layers.
Advantages:

- To provide Identity Based security.
- The storage servers autonomously perform encoding and re-encryption process and the key servers independently perform partial decryption process.
- Auto Key update can be performed in server aided settings.

C. System Architecture



The procedures are :

Step 1 : We have the data owner, server(Hadoop Cloud Provider)and user. First the data of the owner should be encrypted before outsourced securely.

Step 2 : In the Hadoop cloud provider, the encrypted data stored in the Hadoop from the data owner through secured channel.

Step 3 : Then the user sends request for authorization to the data owner.

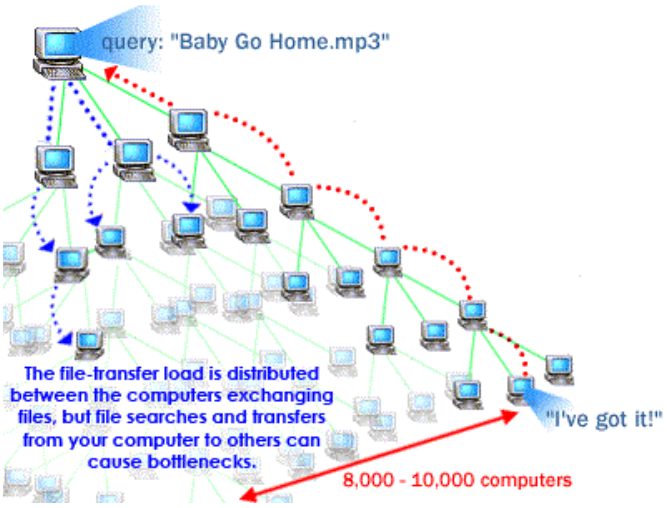
Step 4 : The data owner reviews the request from the user and then sends the response with credentials.

Step 5 : Now the user request to access the data to the Hadoop cloud provider.

Step 6 : Through the secured channel the Hadoop cloud provider responded with the encrypted data to the user.

Step 7 : Finally the Authorized user decrypts the accessed data and then use for its own.

Peer to Peer File Sharing



D. Modules

The list of modules are

- Third Party Auditor module
- Merkle Hash Tree and RC5 Design for Integrity Module
- Hadoop Service Provider module

Module Description

1. Third Party Auditor module

- Expertise and capabilities, trusted to access the Hadoop storage services.
- Inter-mediator who verify the client's request.
- Original data files can be recovered.

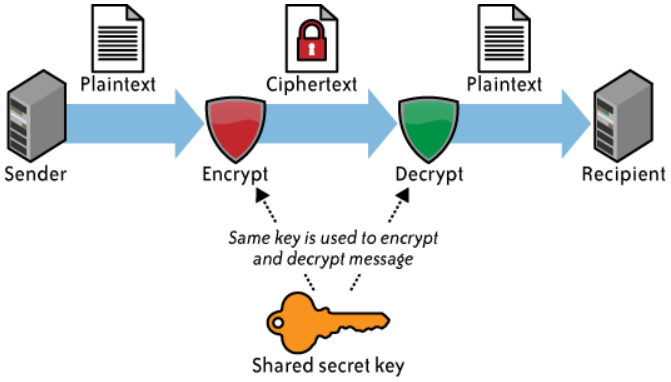
2. Merkle Hash Tree and RC5 Design for Integrity Module

Merkle Hash Tree

Efficiently and securely prove that the set of elements are undamaged and unaltered.
Authenticate both the values and position of data blocks.

RC5 Design for Integrity Module

RC5 encryption and decryption both enlarge the random key into 2(r+1) words that will be used serially (and only once each) during the encryption and decryption processes.



3. Hadoop Service Provider module

Significant storage space and computation resource to maintain the client's data.

The clients may interact with the Hadoop server via CSP to access or retrieve their pre-stored data.

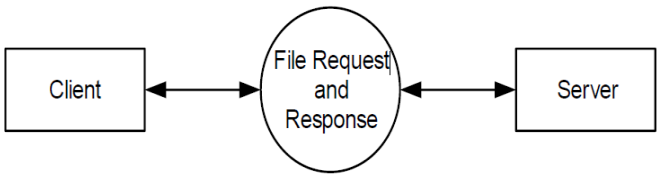
The user give their data to CSP; CSP has control on the data

III. RESULTS AND DISCUSSION

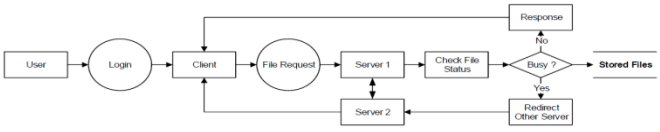
A. Unified Modeling Language(UML)

State Transition Diagram

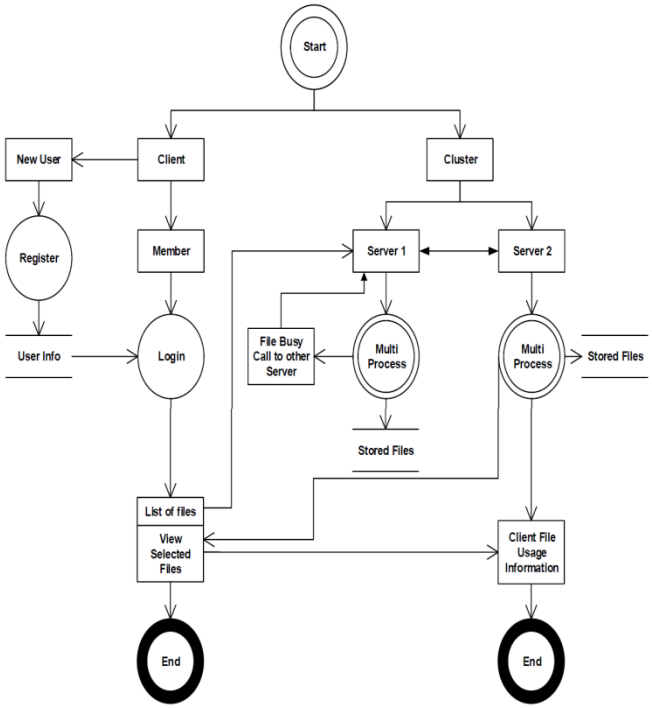
Level 0



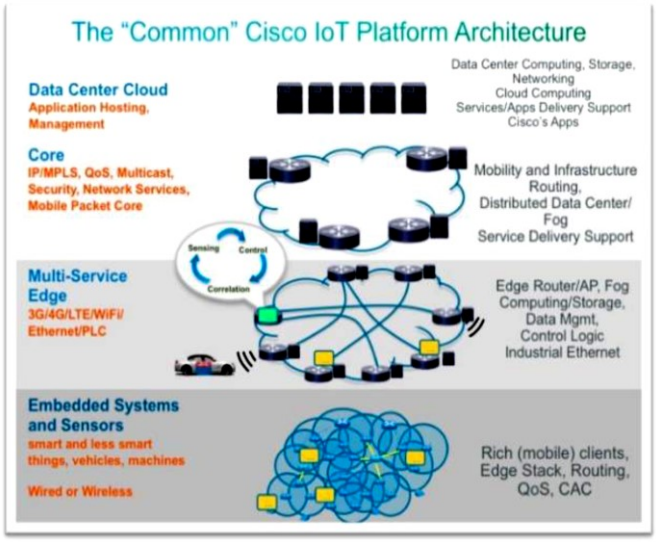
Level 1



Level 2



B. IOT Architecture Layers for Tracking Our Data



Layers of IOT

- Embedded Systems Layer
- Multi-Service Edge Layer
- Core Network Layer
- Data Center Cloud Layer

Embedded Systems Layer

The first layer of the IoT/M2M architecture is comprised of embedded systems, sensors and actuators. As such, these are small devices, with varying operating systems, CPU types, memory, etc.

Multi-Service Edge Layer

The variability in the capabilities of endpoint devices, and their potentially enormous numbers highlight the importance of the multi-service edge in the IoT/M2M architecture.

Core Network Layer

The architecture of the core network layer is similar to the architecture deployed in conventional networks. This layer provides path to carry and exchange data and network information between multiple sub-networks.

Data Center Cloud Layer

The architecture of the data center/cloud layer that are deployed in conventional networks. The function of this layer is to host applications that are critical in providing services and to manage the end-to-end IoT architecture.

IV. CONCLUSION

From this we conclude that Files can be sent anywhere at any time by which systems are connected in peer to peer where data secured using TPA cloud service and data are stored in Hadoop server. To ensure the problem of data integrity, many schemes are proposed such as PDP (Provable Data Possession model) POR (Proof of Retrievability) RSA that can be overcome by TPA in cloud Security, The data are sent to the Authorized user and the sender and receiver can able to track our file or data using IOT layers.

V. REFERENCES

[1]. Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, Senior Member, IEEE, "Identity-Based Encryption with Outsourced Revocation in Hadoop", IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 2, FEBRUARY 2015.

[2]. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation,"in Advances in Cryptology (CRYPTO'98). New York, NY, USA:Springer, 1998, pp. 137–152.

[3]. V. Goyal, "Certificate revocation using fine grained certificate spacepartitioning," in Financial Cryptography and Data Security, S. Dietrichand R. Dhamija, Eds. Berlin, Germany: Springer, 2007, vol. 4886,pp. 247–259.

[4]. F. Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: Efficientcertificate validation and revocation," in Public Key Cryptography(PKC'04), F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany:Springer, 2004, vol. 2947, pp. 375–388.

[5]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryptionwith efficient revocation," in Proc. 15thACMConf. Comput. Commun.Security (CCS'08), 2008, pp. 417–426.

[6]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," inAdvances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin,Germany: Springer, 2005, vol. 3494, pp. 557–557. 7] Malathi, Murugesan, "A Scheme for Checking Data Correctness in the Cloud", International Conference on Information and Network Technology (ICINT 2012). 2013.3. 8]N.Madhuri, T.V.Suneetha, A.Haritha, P.V.S.Lakshmi, "A Protocol for Ensuring Data Integrity in Cloud Environment", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[7]. XU Chun-xiang, HE Xiao-hu, Daniel Abraha, "Cryptanalysis of auditing protocol proposed by Wang et al. for data storage security in Cloud Computing", School of Computer Science and Engineering, University of Electronics Science and Technology of China, 2006. 10]

[8]. K. Govinda, E.Sathiyamoorthy, "Data Auditing in Cloud Environment using Message Authentication Code", International Conference on Emerging Trends on Advanced Engineering Research (ICETT), 2012. 11]

[9]. Miss. M. Sowparnika1, Prof. R. Dheenadayalu2, "Improving data integrity on cloud storage services", International Journal of Engineering Science Invention(ISSN), Volume 2, Issue 2 ,February.