IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10230

# SECURE CLOUD DATA SHARING USING DIGITAL SIGNATURE BASED TRIO ACCESS CONTROL WITH KEY SHARES

**P. Maalini[1], R. Vadivel[2]***

Department of Information Technology, Bharathiar University, Tamil Nadu India[1]

Department of Information Technology, Bharathiar University, India[2]

**Abstract:** Cloud computing multitenancy and virtualization features present remarkable security and access control difficulties because of sharing of actual resources. Since a (public) cloud might not have any power over download demand specifically, an assistance client may send limitless quantities of download solicitation to cloud worker, a malicious service user may launch denial-of-service (DoS)/distributed denial-of-service (DDoS) attacks to burn-through the resources of distributed storage administration worker. So the cloud administration couldn't have the option to react genuine clients' administration demands. Apart from economic loss, unlimited download itself could open a window for network attackers to observe the encrypted download data that may lead to some potential information leakage (e.g., file size). In this project, we propose a new mechanism, Digital Signature based Trio Access Control with Key Shares, to tackle the above aforementioned two problems and also Key stealing attacks and network URL attacks. Computerized Signature age utilizing ECC is utilized to produce advanced mark to the clients, that will evades organization and URL based assaults. Key Shares are included this record to maintain a strategic distance from cloud insiders key taking assaults.

**Keywords**: Cloud-based data sharing, access control, cloud storage service, DDos, ECC

## 1.INTRODUCTION

Distributed computing is perceived as an option in contrast to customary data innovation [1] due to its inborn asset sharing and low-support attributes. By moving the nearby information the board frameworks into cloud workers, clients can appreciate excellent administrations and save critical ventures on their neighborhood foundations. Quite possibly the most basic administrations offered by cloud suppliers is information stockpiling. Allow us to consider a useful information application. An organization permits its staffs in a similar gathering or division to store what's more, share records in the cloud. By using the cloud, the staffs can be totally delivered from the inconvenient neighborhood information stockpiling and support. However, it also poses a significant risk to the confidentiality of those stored files. An individual or an association doesn't need buying the capacity gadgets. Rather they can store their information to the cloud and document information to evade data misfortune in the event of framework disappointment like equipment or programming disappointments.

Advantages of utilizing cloud storage include greater accessibility, higher reliability, fast deployment and more grounded security are few just to name. Regardless of these mentioned benefits, cloud storage leads to new challenges on data access control, which is the basic issue to guarantee information security.

## 2.RELATED WORKS

In Cloud registering accessible encryption is a testing task. Be that as it may, the greater part of the current works follow the model of one size fits all and disregard personalized search over rethought scrambled information. This structure utilizing semantic cosmology WordNet by breaking down clients looking through history and by receiving a system for creating a score which communicates information purchaser interest, constructs client interest model for each information buyer. This system upholds both customized multi-catchphrase positioning inquiry and question augmentation.

Utilizing WordNet, the entrance recurrence of both mentioned catchphrases and catchphrases identified with them are recorded. Diverse access recurrence of catchphrases as various need mirrors the unique significance of watchwords concerning clients interest. After question utilizing search control instrument scrambled hunt will be shipped off the cloud worker.

In the wake of accepting a hunt question from a lawful client, the cloud worker will lead some assigned pursuit over the file and positioned important encoded records will be returned by cloud worker. Here cloud worker is the single power who does looking, ordering and positioning of pertinent records and sends back to the user[1].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10230

Notwithstanding, the catchphrase based inquiry can't satisfy the client aim of search as they don't follow semantic portrayal of data of clients recovery. This work proposes a semantic hunt plot which relies upon idea chain of importance just as the semantic relationship between them. Here in this plan archives get listed first and the hidden entrance will be assembled dependent on the idea pecking order and it is further improved for getting sorted out every one of the reports file vectors by using tree-based list structure. Lately, the general strategy for looking through scrambled information includes five steps: archive highlight extraction, making a file which is accessible, making secret entrance for search, utilizing hidden entryway looking through the record and return the query items. For each record two record vectors are created, one for coordinating with the solicitation containing the ideas for search and one more is utilized to choose the property estimation which fulfills the solicitation for the search. When the cloud worker gets the hidden entrance, accessible list will be looked for required report and fulfills the inquiry demand by returning the encoded documents[2].

### 3.1 EXISTING SYSTEM

**Dual Access Control**

- ✓ Access control for proprietor – Avoid Insider Attacks.
- ✓ User Request handling by cloud worker - Avoid Economic Denial of Sustainability (EDoS) assaults.

**Disadvantages**

- ✓ Attackers have an option to attack through the URL based and the network based threads.
- ✓ Key stealing attacks is the severe issue, the cloud server authorities can steal the key without user permissions.

### 3.2 PROPOSED SYSTEM

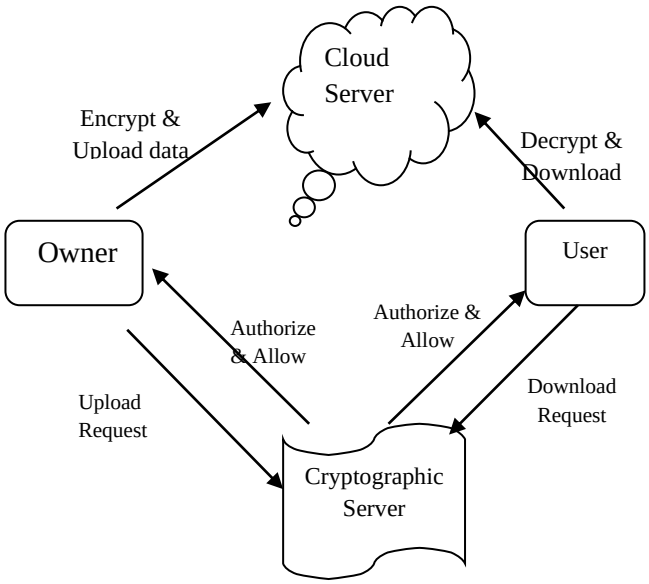
**Digital Signature based Trio Access Control with Key Shares**

1. Digital Signature Generation (using ECC – Elliptic Curve Cryptography algorithm) – Avoid network based attacks and URL attacks
2. Key Shares – Key is partitioned into two offers, one offer is given to cloud worker and another offer is given to information client, While unscrambling and downloading, these two offers will gets consolidate into one key, during this time the client need to give his key offer, after confirmation of key the record gets decoded and downloaded.
3. Access control for owner (with digital signature) – Avoid Insider Attacks
4. User Request handling by cloud worker (with computerized signature) - Avoid Economic Denial of Sustainability (EDoS) assaults

**Advantages**

- ✓ ECC is used in this cloud system which avoids network and URL based attacks.
- ✓ Key shares concept avoids key stealing attacks

### 4. SYSTEM MODEL



IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10230

## 5. IMPLEMENTATION

1. User Interface Administration
2. File Encryption and Uploading
3.Access Control on Upload Request
4.Key Share Generation
5.Access Control on Download Request
6.File Decryption and Download

**1. UI Administration**

The principle thought of this module is to plan the UI for clients in the task. The login page is to plan for information proprietor and information client. After the information proprietor logins into the framework, the page showed which permits the information proprietor to accomplish the encoded document transfer to the framework. At the point when the client logins to the framework, the framework permits the client to enter the unscrambling key and characteristics for recovery of determined document.

**2. File Encryption and Uploading**

Prior to getting to the record from framework, the client should enlist into the framework. Each record which is to be transferred is scrambled with encryption key. Whenever document is encoded, subsequent stage is to transfer it to the capacity framework alongside information unscrambling key.

**3. Access Control on Upload Request**

This module gives the entrance command over transfer demand as in just approved information proprietors can transfer and share the information. For a transfer demand UReq for a unique record, the entrance control on transfer demand system comprises of the accompanying advances:

The proprietor gives a call demand and sends the solicitation to the cloud worker.

Upon getting the call demand from the dataowner, the cloud worker authority accepts UReq as info.

**4. Key Share Generation**

*K* is a random secret generated by the CS for each of the data files. In any case, the length of the key can be adjusted by the prerequisites of the basic SKA. K is gotten in a two-venture measure. In the initial step, an irregular number R of length 256 pieces is produced to such an extent that R = {0, 1}256. In the subsequent stage, R is gone through a hash work that could be any hash work with a 256-bit yield. For our situation, we utilized secure hash calculation 256 (SHA-256). The subsequent advance totally randomizes the underlying client determined arbitrary number R.

CS Key Share Ki: For every one of the clients in the gathering, the CS produces Ki, to such an extent that Ki = {0, 1}256. Ki fills in as the CS segment of the key and is utilized to register K at whatever point an encryption/unscrambling demand is gotten by the CS. In addition, it is guaranteed by examination that the unmistakable Ki is created for each record client.

Client Key Share Ki: K is registered for every one of the clients in the gathering as follows:

K1i= K ? Ki., Ki fills in as the client segment of the key and is utilized to register K when required.

**5. Access Control on Download Request**

This module gives the entrance command over download demand as in just approved clients can download and the common information. For a download demand Data Request for a common scrambled document, the entrance control on download demand system comprises of the accompanying advances:

The client gives a call demand and sends the solicitation to the cloud worker. Upon getting the call demand from the client, the cloud worker authority accepts DReq as info.

**6. File Decryption and Download**

Client demands the document by giving subtleties and accordingly framework answers with encoded record. It will avoid the unauthorized users or hackers. The recipient gets the scrambled document, and he has right job and mark, if it's right, the first record gets decoded for the collector. This permits them to get to data without approval and hence represents a danger to data protection.

## 6. OUTCOME AND POSSIBLE RESULT

In a multi-authority decentralized information access controlling framework credits are from various fields and overseen by various specialists. Clients can likewise share the information utilizing access strategy characterized with credits from various specialists.

The framework has been created in java. Every substance is tried by sending them on singular machines. The cloud, Proprietor, AA, CA and Observer sent on center I-3 processor with 4 gb RAM. Customer framework utilizes i3 processor with 2 gb smash. JRE-1.7 is introduced on every framework. Thesystem utilized jdk 1.7, IDE:Netbeans 7.4 and Adrive cloud for advancement. Mysql 5.3 data set is utilized for data set stockpiling. The system client's construction alongside assignment given below.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10230

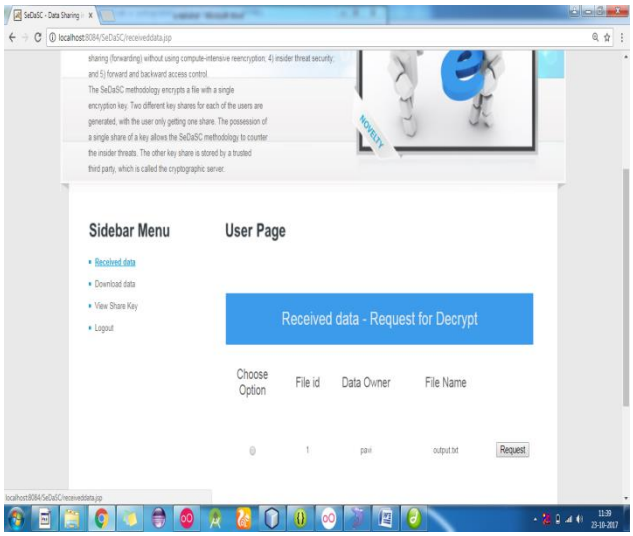



Fig 1. User Request Decrypt page

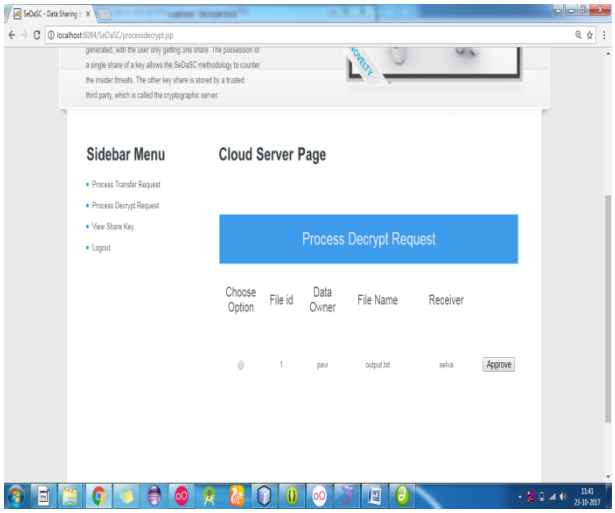



Fig 2. Cloud server approval

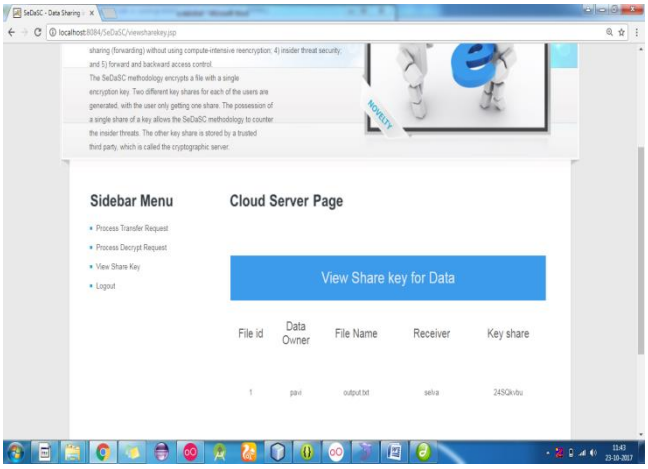



Fig 3.Server share key page

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10230

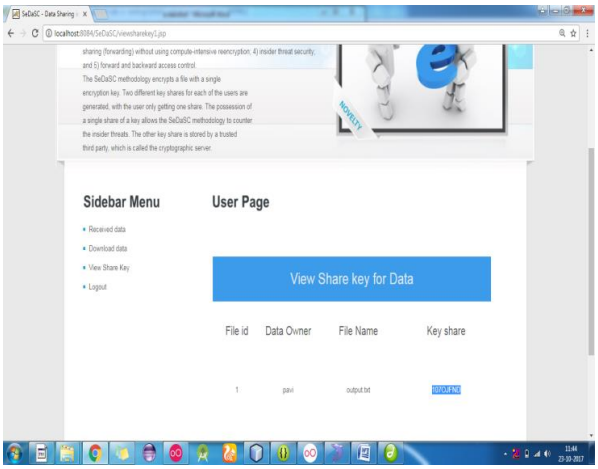



Fig 4. User Download File

## 7. CONCLUSION

We tended to a fascinating and dependable issue in cloud-based information sharing, and introduced two double access control frameworks. The proposed frameworks are impervious to DDoS/EDoS assaults. We express that the method used to accomplish the component of control on download demand is "transplantable" to other CP-ABE developments. This revocable multi-authority information access conspire with evident rethought unscrambling and it is secure and irrefutable. In this upgraded framework, we utilize the way that the restricted intel stacked into the area can't be removed.Building a double access control framework for cloud information sharing from straightforward area is an intriguing issue. In our future work, we will think about the relating answer for the issue. Making this plan viable with existing ABE plans, uphold productive client renouncement.

## REFERENCE

[1] Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin. Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2):111–128, 2013.
[2] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.
[3] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.
[4] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
[5] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.
[6] Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.
[7] Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017.
[8] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.
[9] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.
[10] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE transactions on information forensics and security, 10(3):665–678, 2015.

## AUTHORS PROFILE

**P. Maalini** received Bachelors Degree in Computer Application in the year 2019 from VLB Janakiammal College of Arts and Science, Coimbatore, Tamil Nadu, affiliated to Bharathiar University. She is currently pursuing a Masters Degree in Information Technology from 2019 to 2021, at Bharathiar University, Coimbatore, Tamil Nadu. Her area of interest is Robotics and Artificial Intelligent.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10230

**R. Vadivel** is an Assistant Professor in the Department of Information Technology, Bharathiar University, Tamil Nadu, India. He received his Ph.D degree in Computer Science from Manonmaniam Sundaranar University in the year 2013. He obtained his Diploma in Electronics and Communication Engineering from State Board of Technical Education in the year 1999, B.E., Degree in Computer Science and Engineering from Periyar University in the year 2002, M.E., degree in Computer Science and Engineering from Annamalai University in the year 2007. He had published over 40 journals papers and over 30 conferences papers both at National and International level. His areas of interest include Computer Networks, Network Security, Information Security, etc.