Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.224 – 228

A Novel Design for Authentication of Data Stored via Decentralized Entry Control over Cloud

C.V Swamy Reddy [1], A. Deepthi [1], K.V Sai [1],

Ch. Radha Krishna Murthy[1], K.Subba Rao [2]

[1]UG Scholar, Department of Computer Science & Engineering, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India

[2]Associate Professor, Department of Computer Science & Engineering, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India

[1] swami.reddy2@gmail.com, [2] subbukatte@gmail.com

Abstract: Cloud provides uninterrupted services in the remote location and cloud computing is accessing application over a network also provides the advantage for storing the data. One of the most fundamental advantages is it will not require any software on your local system. However there is a major issue with security of those stored data. The reason behind it is that the cloud storage servers are managed by some cloud provider which are not fully trusted and the data may be confidential and sensitive which is stored in cloud so here a possible chance of data violation. We can resolve this problem by using encryption, that is encrypting the data and then upload into the cloud but unfortunately data sharing in cloud is not a secure process because servers are not trusty based, data owner storing their data in those cloud servers and providing respective decryption key to the authorized users by this the unauthorized users and those cloud server are not in a position to access these data because they don't have an idea on decryption key. The single owner way prevents the appropriation of key arrangement quality based encryption and different plans. To solve the above described problems we propose a solution with a novel architecture for authentication of data stored in clouds through decentralized access control. In particular, the newly allowed clients can specifically decode information. Client removal can be effortlessly carried out through a novel renouncement list.

Keywords: Access control, authentication of user, attribute-based signatures, attribute-based encryption, cloud storage.

I. INTRODUCTION

Cloud computing is the means of delivering computing as a service rather than a product, whereby shared resources, information and software are provided to users and other devices as a utility over a network. Cloud computing is a model for enabling easy, convenient and on-demand network access to various configurable computing resources (e.g., networks, servers and services) that can be rapidly released with minimal management effort or service provider interaction.

Even there are many definitions of Cloud Computing, the simplest one defines cloud computing as getting computer services or resources from the Internet rather than from local individual platforms.

Cloud Computing can be deployed as following:

• Software-as-a-Service (SaaS) - software application services obtained from the Internet.

• Platform-as-a-Service (PaaS) - the user uses the Internet platform as a computing platform, rather than having his own individual resource platform.

• Infrastructure-as-a-Service (IaaS) - It provides virtualized computing resources over the Internet.

It is the result of significant challenges which are arising from the efforts in adopting new technologies in teaching and learning environments. This is mainly a result of new generation of students with learning new things fastly, and it is becoming clear to most of the people, including students that the traditional ways are unable to address the needs of higher education where the need is on higher order learning experiences and outcomes demanding changing knowledge and communication based society.

II. RELATED WORK

II.I Existing System with Drawbacks

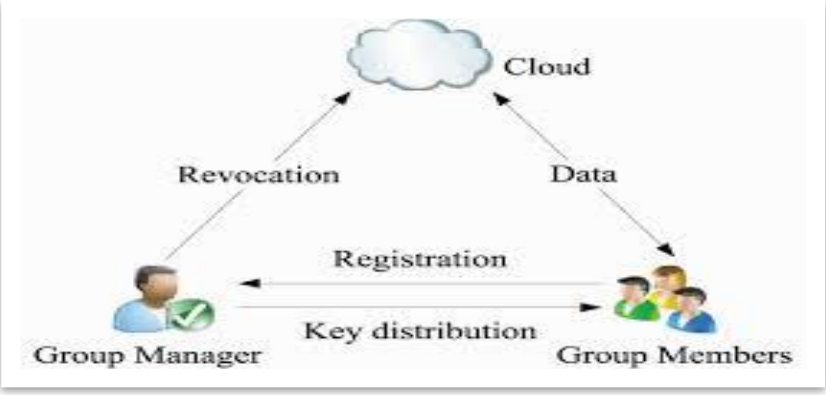
A few security methods for information sharing over untrusted servers have been already been proposed. In these methodologies, information is which is stored in untrusted cloud in encrypted format and only the relating decoding keys are provided only to approved clients. In this way the unapproved users and additionally stockpiling servers can't take in the information records since they don't have any idea of the unscrambling keys. Then again, the complexities of user support in these plans are straightly increasing with the quantity of information proprietors and the quantity of disavowed clients.

II.II Proposed System with Features

We propose a novel architecture for authentication of data stored via decentralized entry control in clouds which. It infers that any user in the group can safely share information to others by the untrusted cloud. In particular, the newly allowed clients can straight forwardly change information records shared before their interest without reaching with information proprietors. Client removal can be effectively carried out through a novel revocation list without redesigning the mystery keys of the remaining users. It provides secure and protection saving access control to users. In addition, the original personalities of information proprietors can be uncovered by the gathering director when question happen.

The main aim of this paper is sharing information in a multi-proprietor way while safeguarding information and character protection from the untrusted cloud is still a major issue. Here, we propose a protected multi-proprietor information data sharing plan, named novel structural planning information put away by means of decentralized access control. Meanwhile, the capacity overhead and encryption calculation expense of our plan are autonomous with the quantity of disavowed clients.

III. SYSTEM ARCHITECTURE



IV. MODULE WISE FUNCTIONAL REQUIREMENTS

The following are the modules of our project. They are:

1. **Admin:** In admin module at first admin have to login and then admin can add Group, View Group, view user message, view users& Deletes Group.

2. **Manager:** In this manager can has to login first then manager add users in Group. He can also perform operations like uploading file, view file & download file. Manager can delete file and revoke user.

3. **User:** In this user has to register first and then he can login and he can upload, view & download files.

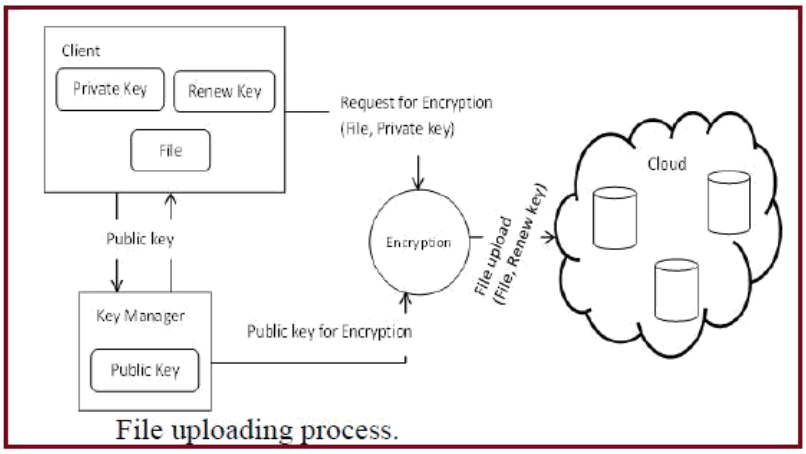
4. **Decentralized Entry Control (Data Sharing Scheme):** In this first it identifies users in group. In this we perform encryption and decryption using AES algorithm for security.

V. ENCRYPTION / DECRYPTION

We used AES algorithm for encryption/Decryption in our project. This algorithm is the proven mechanism for secure transactions. Here we are using the AES algorithm with key the size of 128 bits for security. The AES has three altered 128-bit square figures with cryptographic key sizes of 128, 192 and 256 bits which provides more security. Key size is boundless in nature, while the square size most extreme is of size 256 bits. The AES outline depends on a substitution-change system (SPN) and it does not utilize the Data Encryption Standard (DES). In 1997, the NIST started a five-year calculation leading to the improvement in procedure to supplant the DES and Triple DES. The NIST calculation determination procedure encouraged the open joint effort and incorporated a nearby survey of 15 competitors. After an extraordinary assessment of various competitors, the Rijndael outline, made by two Belgian cryptographers, was the last decision.

VI. FILE UPLOAD

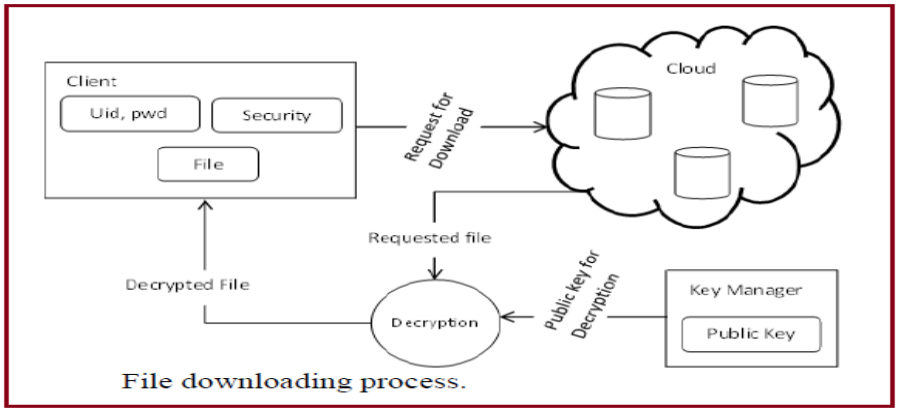
The customer made solicitation to the key supervisor for people in general key, which will be produced by approach connected with the document. Diverse approaches for records, open key additionally contrasts. Be that as it may, for same open key for same strategy will be created. At that point the customer produces a private key by consolidating the username, secret word and security certifications. At that point the document is scrambled with general society key and private key and sent to the cloud.



File uploading process.

VII. FILE DOWNLOAD

The customer can download the document after finish of the confirmation process. As the general population key kept up by the key director, the customer solicitation key. The confirmed customer can get general society key. At that point the customer can unscramble the document with general society key and the private key. The clients' qualifications were put away in the customer itself. Amid download the document the cloud will verify the client whether the client is legitimate to download the record. Yet, the cloud doesn't have any characteristics or the subtle elements of the client.



File downloading process.

VIII. FILE ACCESS CONTROL

Capacity to breaking point and control the entrance to host frameworks and applications through correspondence joins. To accomplish, access must be distinguished or confirmed. After accomplished the verification prepare the clients must take up with right strategies with the records. To recoup the document, the customer must demand the key administrator to create general society key. For that the customer must be verified. The characteristic based encryption standard is utilized for document access which is confirmed by means of a quality connected with the record. With record access control the document downloaded from the cloud will be in the configuration of read just or compose bolstered. Every client has connected with strategies for every record. So the right client will get to the right document. For making record get to the trait based encryption plan is used.

IX. CONCLUSION & FUTURE SCOPE

Although, there still exists scope for the improvement of our project in the future. Our project has been developed mainly by taking the example of the environment of the company. We will extend our project to the field's equivalent to schooling, enjoyment, various social networks and other wider areas. For example, we can hire our mission within the universities to keep the data base of the students which can be used by the groups of lecturers. Here lecturer turns into the crew member and the pinnacle of the division becomes the staff manager and principal turns into the admin. Additional enhancement within the security of the data uploaded by using the individuals will also be finished.

REFERENCES

1 S SushmitaRuj, Milos Stojmenovic and Amiya Nayak,"Decentralized Access Control with Anonymous Authentication of DataStored in Clouds", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS

2 Yang Tang, Patrick P.C. Lee, John C.S. Lui and Radia Perlman,"Secure Overlay Cloud Storage with Access Control and AssuredDeletion", IEEE Transcations on dependable and secure computing, VOL.9, NO. 6, NOVEMBER/DECEMBER 2012

3 Y. Tang, P.P.C. Lee, J.C.S. Lui, and R. Perlman, "FADE: SecureOverlay Cloud Storage with File Assured Deletion," Proc. Sixth Int'l ICSTConf.Security and Privacy in Comm. Networks (SecureComm).

4 R. Perlman, "File System Design with Assured Delete," Proc.Network and Distributed System Security Symp. ISOC (NDSS), 2007

5 Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed accesscontrol in clouds," in IEEE TrustCom,

6 A. Rahumed, H.C.H. Chen, Y. Tang, P.P.C. Lee, and J.C.S. Lui,"A Secure Cloud Backup System with Assured Deletion and VersionControl," Proc. Third Int'l Workshop Security in Cloud Computing, 2011

7 S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based DataSharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), Apr. 2010.

8 G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-basedencryption for fine-grained access control in cloud storage services," inACM CCS, , pp. 735–737, 2010.

