JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Data Security of Dynamic and Robust Role Based Access Control from Multiple Authorities in Cloud Environment

Vikas Nagrale [*], Ashutosh Kumar [**], Mayur Yalij[***] , Prof S.V. Shinde**

*(Computer engineering, PDEA College of Engineering , Pune (India)
Vickynagrale1210@gmail.com

**(Computer engineering, PDEA College of Engineering , Pune (India)
Ashutosh081097@gmail.com

***(Computer engineering, PDEA College of Engineering , Pune (India)
yalijmayur@gmail.com

****(Computer engineering, PDEA College of Engineering , Pune (India)
sashsir@gmail.com

Abstract:

Data integrity maintenance is that the major objective in cloud storage. It includes audition using TTP for unauthorized access. This work implements protecting the information and regeneration of information if someone mishandles it. This job are going to be assigned to a Proxy server. the info of the users are going to be stored publicly and personal area of the cloud. so only public cloud data are going to be accessed by user and personal cloud will remain more secured. Once any unauthorized modification is formed, the first data within the private cloud are going to be retrieved by the Proxy server and can be returned to the user. Cloud storage generally provides different redundancy configuration to users so as to take care of the specified balance between performance and fault tolerance. Data availability is critical in distributed storage systems, mostly when node failures are prevalent in real world. This research work explores about secure data storage and sharing using proposed AES 128 encryption algorithm and Role Base Access Control (RBAC) for secure data access scheme for user. This work also dispensed backup server approach it works like proxy storage server for spontaneous data recovery for all distributed data servers. The experiment analysis has proposed publicly similarly as private cloud environment.

Keywords: RBAC, El Gamal encryption scheme, Secure user access policy, Proxy Key Generation Role Base Access Control (RBAC), Advanced encryption standard (AES), TPA (Third Party Auditor), TMACS: Threshold Multi-Authority Access Control System

INTRODUCTION:

In existing system, a user are often a knowledge Owner and an information Consumer simultaneously. Authorities are assumed to own powerful computation abilities, and that they are supervised by government offices because some attributes partially contain users' personally identifiable information. The full attribute set is split A threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, within which multiple authorities jointly manage an identical attribute set. In TMACS, taking advantage of (t; n) threshold secret sharing, the passkey may be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. Security and performance analysis results show that TMACS isn't only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive within the system. Further, by efficiently combining the normal multi-authority scheme with TMACS, construct a hybrid one, which satisfies the scenario of attributes coming from different authorities likewise as achieving security and system-level robustness. In security analysis of attribute revocation in multi-authority data access control for cloud storage systems provides the mechanism in managing attribute revocation could achieve both forward security and backward security. Analysis and investigation reports show that the work adopts a bidirectional re-encryption method in cipher text updating, so that security vulnerability appears. Also proposed attack method demonstrates that a rejected user can still decrypt new cipher texts that are claimed to wish the remake secret keys to decrypt in an exceedingly very semi anonymous privilege control scheme Anomy Control to house not only the knowledge privacy, but also the user identity privacy in existing access control schemes. Anomy Control scatter the central authority to limit the identity leakage and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data are often managed in a very fine-grained manner. The Anomy Control-F, which was fully prevents the identity leakage and achieve the whole anonymity.

Author's security research shows that both Anomy Control and Anomy Control-F are secure under the decisional bilinear Diffie–Hellman assumption, and author's performance evaluation exhibits the workability of scheme. Cipher-text Policy Attribute-based Encryption (CP-ABE) is taken into consideration one altogether the foremost suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it's difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems due to the attribute revocation problem. To do that designed an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where multiple authorities exist at the same time and every authority was able to issue attributes independently. Specifically, it proposed a revocable multi-authority CP-ABE scheme, and applies it because the underlying techniques to style the knowledge access control scheme. Sharing data during a multi-owner manner while protecting data and identity privacy from an untrusted cloud is additionally a very challenging task, thanks to the constant change of the membership. For that proposes a secure multi-owner data sharing scheme, named Mona, for dynamic groups within the cloud. By exploiting group signature and dynamic broadcast encryption techniques, any cloud user can secretly share data with other users.

PURPOSE:

In the proposed research work aim to style and implement a system which is able to provide the info security from collusion attack in trusted also un-trusted cloud environments. The system will focus long communication scenario between data owner, user, TPA and authorities using different security techniques, it'll provide highest security than all existing approaches. (Using Amazon EC2 VM Console

SCOPE:

The research work specializes in cloud data storage security, which has always been a most aspect of quality of service. For ensuring the correctness of cloud client's data within the cloud, during this paper propose a highly effective and versatile distributed scheme with two features, apposing to its predecessors. By using the homomorphic token with distributed verification of erasure coded data. During this paper proposed the combination of storage correctness insurance and data error localization most of works, the new scheme further supports secure and efficient dynamic operation on data block including operations. We depend on erasure-correcting code within the file distribution preparation to support redundancy parity vectors for verification of erasure coded data using the homomorphic token, this scheme achieves the combination of information error localization and storage correctness insurance. This paper proposed highly effective and versatile distributed scheme with explicit dynamic data provide to making sure the correctness of user's data within the cloud. Our scheme enables the information owner to delegate of knowledge file re-encryption and user secret key update to cloud servers without disclosing data contents. during this paper we achieve this goal by exploiting and uniquely combing techniques that's token pre-computation, data correctness verification further as data localization and data recovery. within the first reason cryptography services for the intention of information security protection couldn't be directly adopted because of the users" loss control of knowledge under cloud computing. So, verification of correct data storage within the must be conducted without explicit knowledge of the whole data. This construction dramatically decreasing the communication and storage overhead as compared to the based file of replication in distribution techniques. Therefore, correctness of knowledge and availability of the information being stored on the distributed cloud servers is also guaranteed. The key issues are to highly detect any unauthorized data alternation and corruption, possibly thanks to server compromise byzantine failure.

LITERATURE SURVEY:

1.Wei Li, Kaiping Xue TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage .

System proposed a access control systems for public cloud storage, brings a single-point bottleneck on both security and performance against the only authority for any specific attribute. First design multi-authority access control architecture to cope with the matter. By introducing the combining of (t, n) threshold secret sharing and multi-authority CP-ABE scheme, then proposes and realizes a strong and verifiable multi-authority access system publically cloud storage, during which multiple authorities jointly manage a regular attribute set. Further by efficiently combining the normal multi-authority scheme with this scheme, construct a hybrid one, which might satisfy the scenario of attributes coming from different authorities further as achieving security and system-level robustness. Cloud storage is a vital service of cloud computing.

2. Zhou, V. Varadharajan, and M. Hitchens: Achieving secure role-based access control on encrypted data in cloud storage

Proposed a role-based encryption (RBE) scheme that integrates the cryptographic techniques with RBAC. The RBE scheme allows RBAC policies to be enforced for the encrypted data stored publicly clouds. supported the proposed scheme, system also present a secure RBE-based hybrid cloud storage architecture that permits a company to store data securely in an exceedingly public cloud, while maintaining the sensitive information associated with the organization's structure in a very private cloud. System describes a practical implementation of the proposed RBE-based architecture and discusses the performance results. They also demonstrate that users only have to keep one key for decryption, and system operations are efficient no matter the complexity of the role hierarchy and user membership within the system.

3. Jung, et al : A semi-anonymous attribute-based privilege control scheme

AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to deal with the user privacy problem in an exceedingly cloud storage server. The proposed scheme was ready to protect user's privacy against each single authority.A Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. The scheme was tolerant against authority compromise, and compromising of up to (N −2) authorities didn't bring the entire system down. Author has provided detailed about security and feasibility of the scheme. Also implements the 000 toolkit of a multi-authority based encryption scheme AnonyControl and AnonyControl.

4. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, proposed Sirius: Securing remote untrusted storage

System presents SiRiUS, a secure classification system designed to be layered over insecure network and P2P file systems like NFS, CIFS, Ocean Store, and Yahoo! Briefcase. SiRiUS assumes the network storage is not trustworthy and provides its own read-write cryptographic access control for the file level sharing purpose. Key management and revocation is straightforward with minimal out-of-band communication. filing system freshness guarantees are supported by SiRiUS using hash tree constructions.

METHODOLOGY

Multi-Authority In which all data records are encrypted by multiple authorities. By deploying an improved multi-authority attribute-based encryption scheme, all authorities can distribute their search capability to clients under different different authorities without additional negotiations.

Multi-Client In this work search capabilities are encrypted under an access policy before being sent to the clients, only the allowed clients with corresponding attributes can obtain a valid search token.

Fine-Grained Access Control Attribute-based encryption (ABE) protocol Provides fine-grained access control for encrypted data based on client's attributes. Such protocol allows the client whose attributes satisfy the access policy to decrypt the encrypted messages that are encrypted under certain policies.

Data integrity maintenance is the major objective in cloud storage. It includes audition using TPA for unauthorized access. To implements this work for protecting the data and regeneration of data if someone mishandles it. This job will be assigned to a Data Chunks.

The data of the users will be stored in public and private area of the cloud. So that only public cloud data will be accessed by user and private cloud will remain more secured.

SYSTEM ARCHITECTURE:

The proposed research work has been distributed into 5 different stages these are below:

1.Data Owner :

Data Owner uploads data and share data with others through the cloud storage.
Data owner can share data files as well as download data files at his side.
One more point in that Revocation; in revocation data owner can revoke any user with data file for permanently

2.TPA (Third Party Auditor)

The TPA is accountable for auditing the integrity of cloud data on behalf of group users.
Third Party Auditor can accept or reject the users request for file access.
The legal users are honest and cannot leak any private information to others.
User receives the requested file decrypted by TPA.

3.User:

In this user can access the file through the cloud storage then he must request to TPA for data accessibility.
When TPA grant access the request of users then then only user can access the information or download the information.
The legal group users are honest and cannot leak any private information to others.

4. Cloud Server:
Cloud server provides storage for user's data.
The cloud provides enormous storage space and computing resources for group users. Through the cloud storage, group users can enjoy the data and information sharing service.
It stores all the data in encrypted format and retrieves the data on TPA's request.
It is connecting in WAN network

5. Investigator:

To analyse attacks on the system.

TPA send push notification to investigator when he found hash value of file is changed and data is modified by attacker.

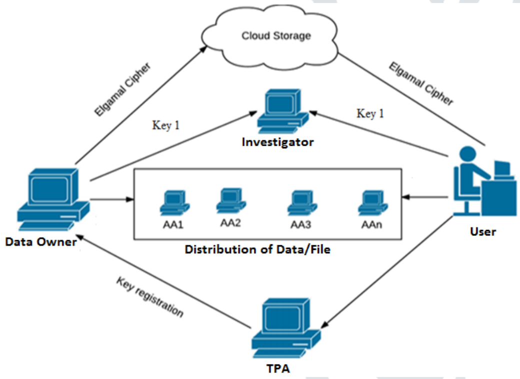
TPA encrypt the file and file content like name, data, creation data and generate the hash value in database.

After encryption, he stores encrypted file in cloud server and proxy server.

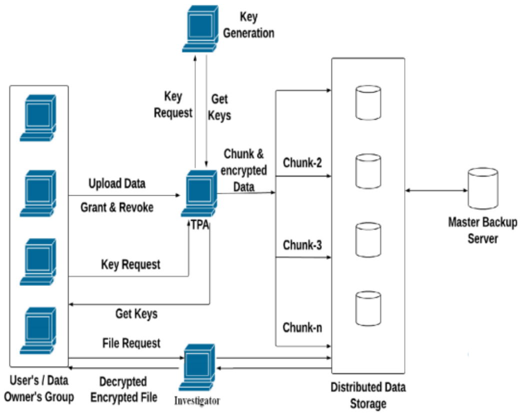
When user request for file, TPA send request to cloud server.

TPA generates hash value of file send by cloud.

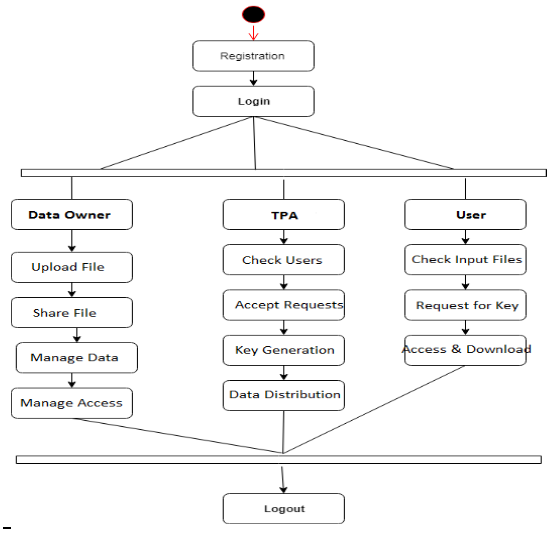
If hash value from TPA's database and hash value cloud's file is same then TPA directly send file to user. If hash value is different than TPA request for proxy server.



Analysis and design diagram



Architecture Diagram



Activity Diagram

ADVANTAGES :

Better data management system has been created to accelerate the process.

Ensure that all the valuable data or information is safeguarded.

Only authorised person can access the data.

Implement verification as well as authentication protocol between authorities and trusted third party.

Improve the time efficiency.

CONCLUSION:

In this work system propose a secure Role Base Access Control (RBAC) data sharing scheme for untrusted environment within the cloud. In our process, the users can securely get their private keys from middleware authorities, TPA provide and secure communication between multiple users. Also, our scheme is ready to produce

the secure revocation for untrusted user. The proxy key generation has also proposed during this work. When data owner revokes any specific user, the system automatically expired the prevailing keys and generates new keys for all other shared users. The system can do highest level security yet as privacy through such approaches. It's a revocable decentralized data access system can support efficient attribute revocation for multi-authority cloud storage systems. It eliminates decryption overhead of users in line with attributes. This secure attribute

based encryption technique for robust data security that's being shared within the cloud. This revocable multi-authority data access scheme with verifiable outsourced decryption and it's secure and verifiable. This scheme are a promising technique,
which might be applied in any remote storage systems and online social networks etc.

RESULT :

This research work is to implement a web-based application for the social community to prevent various attacks of user's confidential data records storage and transmission time.

This result section system proposes a safe information sharing plan, which can accomplish secure key appropriation and information sharing for element bunch . The primary commitments of this plan consist of:

1. The system gives a safe approach to key dispersion with no protected correspondence channels. The clients can safely acquire their private keys from the gathering director with no Certificate Authorities because of the check for people in the general key of the client.
2. This plan can bring about fine-grained access control, with the assistance of the gathering client list, any client in the acquisition can utilize the source in the cloud and disclaim clients can't get to the cloud again after they are renounced.
3. It suggests a safe information sharing plan which can be protected from plot attack. The repudiated clients cannot have the capacity to get the first information documents once they are denied although they plan with the untrusted cloud. Our plan can achieve secure client renouncement with the help of polynomial capability.
4. The proposed plan can support dynamic gatherings effectively, when another client joins within the collecting or client is disavowed from the gathering, the private keys of alternate clients don't should be recomputed and upgraded.

Protection examination to demonstrate the security of our plan. In extension, the system additionally performs re-enactments to exhibit the ability of our plan and recover of data plan.

ACKNOWLEDGEMENT:

We would like to express our sincere gratitude to our guide Prof. S. V. Shinde , Dr. R. V. Patil, PDEA'S COLLEGE OF ENGINEERING for his irreplaceable guidance and for always giving us useful input and encouragement that encouraged us to work harder.

REFERENCES:

[1] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2017.

[2] Jianan Hong, Kaiping Xue and Wei Li, "Comments on "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi-Authority Data Access Control for Cloud Storage Systems", IEEE transactions on information

forensics and security, VOL. 10, NO. 06, June 2017.

[3] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, “Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption”, IEEE transactions on information forensics and security, VOL. 10, NO. 01, January 2017.

[4] Kan Yang and Xiao huaJia, “Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage”, IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.

[5] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th Financial Cryptography and Data Security. Springer, 2010, pp. 136-149.

[6] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no.1, pp. 69-73, 2012.

[7] B. Wang, B. Li, and H. Li, “Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud,” IEEE Transactions on Services Computing, vol. 8, no. 1,pp. 92-106, 2015.

[8] J. Yuan and S. Yu, “Public Integrity Auditing for Dynamic Data Sharing with Multiuser Modification,” IEEE Transactions on Information Forensics and Security, vol. 10,no. 8, pp. 1717-1726, Aug. 2015.

[9] Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J.Hu, “Dynamic Audit Services for Outsourced Storages in Clouds,” IEEE Transactions on Services Computing, vol.6, no. 2, pp. 409-428, 2013.