International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

March- 2015 Volume 2, Issue-2

Email: editor@ijermt.org www.ijermt.org

Preventing Data From Unauthenticated Use Over The Clouds

Analp Pathak, Monika Johari
Assistant Professor
Department of Computer Science & Engineering
SRM University, NCR Campus
Modinagar

Kslaykishore, Shashank Shekhar Tiwari
M-Tech Scholar
Department of Computer Science & Engineering
SRM University, NCR Campus
Modinagar

ABSTRACT—
This paper studies the authentic use of data over the clouds by using the encryption and decryption techniques. Here the server is kept at the half knowledge of authentication it just uses the keys given to the user without knowing its identity. This scheme inhibits the various attacks and supports alteration, creation and reading of the data that is stored over the clouds. Here the paper is proposing the decentralized method for access control over the clouds, which uses the key generation and management with more than one key distribution centre (KDC).

Keywords—cloud; decryption; encryption;

I. INTRODUCTION

The computing world is changing day by day with emerging new technologies of the cloud. The cloud is a space over the internet which provides the online storage of data, this helps in reducing the bearing for the pendrives, hard disks and other material. One can directly login to the cloud account to use the information needed. Various types of services like SaaS (Software As A Service) which runs applications such as Google Apps, Microsoft online, IaaS (Infrastructure As A Service) such as Amazon's EC2, Eucalyptus, Nimbus and etc, last but not least PaaS (Platform As A Service) such as Amazon's S3, Windows Azure and etc. different layers that are provided by the clouds to help the users.

This ubiquitous technology is helping the people with anytime and anywhere availability of the data. Just take a real time example of drop box, (a cloud service utility to store the data online) where a user used to store the data, this data can be sensitive some personal information, now what if somebody logged in your account and can use that data then this puts a direct question over the security of data which is stored over the clouds.

A. User Privacy in Cloud Computing

The cloud can hold the client accounts for the information over it, and in like manner, to give benefits of real-time usage itself is responsible. The legitimacy of the client who stores the information is additionally confirmed. There is moreover a requirement for law implementation separated from the specialized answers for guarantee security and protection.

B. Encryption in Cloud Computing

The cloud is likewise inclined to information change and server intriguing mangle. The opponent can barter storage servers in server intriguing attack, so that server can change information records despite the fact that the servers are inside consistent. The information necessities to be encoded to give secure information capacity. Nonetheless, the information is regularly encrypted; this property needs to be taken into care while working on the productive secure capacity strategies.

C. Security and privacy protection on cloud data

Clients Authentication plan utilizing public key cryptographic procedures as a part of distributed computing. Numerous homomorphism encryption methods have been discretionary to guarantee that the cloud is not ready to peruse the information while performing reckonings on the data. By utilizing this encryption plot, the cloud gets cipher content of the information and performs calculations on the cipher content and returns the encoded estimation of the outcome to client then the client has the capacity translate the outcome, despite the fact that the cloud does not realize what information it has worked on. In such circumstances, it must be likely for the client to confirm that the cloud returns right results.

Access control is fundamental when unauthorized clients try to access the information from the capacity, so that just approved clients can get to the information. It is additionally huge to check that the data originates from a dependable source. We have to tackle the issues of access control, verification, and security insurance by applying suitable encryption systems given in [1] [2] [3].

There are three sorts of right to use controlling policies such as : user-based access control (UBAC),

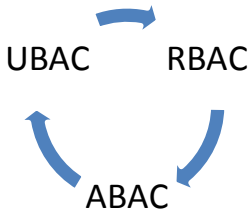

Fig. 1 Access Control

Role-based access control (RBAC), and attribute-based access control (ABAC).

In UBAC, the entrance control list contains the rundown of clients why should approved access information. This is unrealistic with various clients over the cloud.

In RBAC users are categorized based on their own roles. Data should be accessed by the users who satisfy the role matching constraint. There exist various roles that are used by the system such as for e.g., only faculty members and senior secretaries might have access to data but not the junior secretaries.

ABAC is more reached out in extension, in which clients are given properties, and the information has joined access approach. Just clients with legitimate arrangement of traits and fulfilling the accessing approach, can get to the information. Just when the clients have coordinating arrangement of properties, they have decoding the data put away in the cloud. The merits and demerits of RBAC and ABAC are discussed and compared in [4]. There has been some related work on ABAC in clouds for authentication (for example, [5], [6], [7], [8]).

This is not only just confined up to the storing of the data it has wide range where the user who want to upload some sensitive data over the cloud without being acknowledge his identity. This anonymous action can be done via keeping cloud untouched about the identity of the user but the user should be validated so the key must be generated by another trusted third party just like online banking system where the transactions done through a third party that is called as the merchant site.

Complete process is handled by this merchant or one can say the trusted third party (TTP).

II. LITERATURE SURVEY.

[6] A. Sahai and B. Waters, worked on “Fuzzy Identity-Based Encryption”, In Identity Based Encryption (IBE) plot, a client has an arrangement of traits notwithstanding its novel ID. A Fuzzy IBE scheme can be connected to empower encryption .In Fuzzy scheme biometric data utilized as personality, which has highlights of lapse control and solid against arrangement assaults.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, worked on “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data “.This paper puts emphasis on ABE, the sender has an approval to encode data. A renounced characteristics and keys of clients can't compose again to stale data. The attribute power

gets traits and secret keys from the recipient and he/she finds it able to decode data on the off chance that it has coordinating attributes.

[8] J. Bethencourt, A. Sahai, and B. Waters, worked on "Cipher text-Policy Attribute-Based Encryption". By utilizing this approach the beneficiary has the entrance strategy as a tree. The tree contain attributes as leaves and monotonic access structure with AND, OR and other edge gates.

[9] M. Chase worked "Multi-Authority Attribute Based Encryption". This plan portrays a few Key Distribution Authorities (facilitated by a trusted power) which disperse attributes and secret keys to clients. Multiauthority Attribute Based Encryption convention which obliges no trusted authority which requires each client to have attributes from at all the KDCs.

[3] H.K. Maji, M. Prabhakaran, and M. Rosulek, worked on "Attribute-Based Signatures," This system takes a decentralized approach and gives validation without uncovering the attribute of the clients furthermore gives security against a harmful attribute authority.

III. PROPOSED SYSTEM

The data put away in cloud takes after Distributed access control strategy so that just approved clients with substantial characteristics can get to the information. Confirmation of clients performs store and adjustment of the information in the cloud. Amid verification the identity of the client is shielded from the cloud. The cloud architecture is decentralized, which implies that there can be a few KDCs for key administration. The both access control and verification plans are conspiracy safe. The plot safe attack implies that no two clients can intrigue and access information or verify themselves, despite the fact that they are independently not approved. Unauthenticated clients can't get to information after he/she have been denied. The proposed plan is adaptable to replay attacks. This proposed protocol additionally boosts various read and write on the information put away in the cloud. The expenses of decentralized methodology ought to be less similar to the current centralized methodologies.

IV. SYSTEM ARCHITECTURE

The architecture of proposed framework portrayed in Fig.2.There is three clients, a creator, a writer, and reader. The creator gets a token from the trustee, who is expected to be fair. A trustee can be somebody like the government who oversees social protection numbers and so on. On exhibiting his/her id (like wellbeing/social protection number), the trustee issues her a token. There are numerous KDCs (here 2), which can be scattered. Case in point, these can be servers in distinctive parts of the world. A creator on exhibiting the token to one or more KDCs gets keys for encryption/decryption and signing. In the Fig. 2, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encoded under the entrance policy X. The entrance policy chooses who can get to the information put away in the cloud. The creator settles on a case policy □, to demonstrate her realness and signs the message under this case. The figure content C with sign is c, and is sent to the cloud. The cloud confirms the signature and stores the figure content C. In the event that the client has traits coordinating with access strategy, it can decrypt and get back unique message.

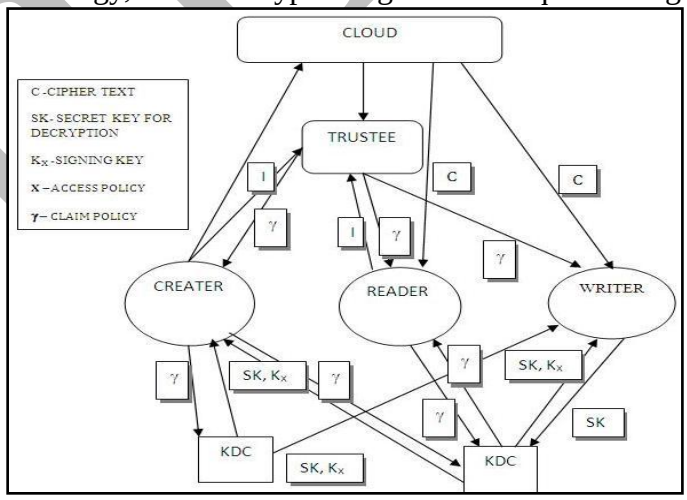

Fig. 1 Data Storage on Clouds

A. Access Control Management

1) Signature Generation

Each user gives their identity to the trustee which is an honest element in the whole system, based on which the token is generated with respect to each user's identity.

KDC only generate the public key [PK[i]] and secret key [SK[i]], they are used for encryption and decryption; and also it generates the ASK[i] and APK[i], they are used for sign verification. Then user creates an access policy X to access the files using a Boolean function. This policy also contains the attributes of the user then the whole message is complied by using Extended Paillier algorithm.

C= Extended Paillier. Encrypt (Message, X)

Timestamp T is used to defend the replay attacks.

In this scheme a writer whose rights have been cancelled cannot create a fresh mark with new time stamp and thus it is not possible to write back stale information.

Signing the message and calculating the message signature as

σ = Paillier. Sign (PK_T, PK_K, T_K, SI_K, MSG, □).

PK_T: - Public Key of Trustee,

PK_K: - Public Key of KDCs,

T_K: - Token,

MSG: - Message,

SI_K: - Signing Key,

□ □ □ □ Access Claim□ □

Once the user's information is stored over the server's database, the reply of the token is generated and received from the trustee, which is considered as an honest entity in the system.

2) Data Storage On Clouds

The clouds receiving the information verify the access claim using paillier algorithm to verify the signature. If the authentication is failed the message is discarded, else the message (C, T) is stored in the cloud. Users presenting the token to KDC and receive keys for encryption and decryption. After receiving the key from user, the message (MSG) is encrypted under the access policies; and also the message is encrypted by means of secret keys that are generated by KDC. The access policies decide who can access the data stored in the cloud.

3) Data Access Control

When a reader wants to read the data, the cloud sends C. If the user's attributes get matched with access policy, then it can decrypt and get back the original message. Write proceeds in the same way as file creation. Once the cloud verification is done then it gives bypass to the other time consuming verification processes.

4) Authentication process

This method uses four types of keys to work with the proposal. Fig3. Each key has its own specific function, which provides the constraint control over the system.

V. IMPLEMENTATION

The whole work is implemented in the Netbeans which gives the GUI to the work that upload and download the file from and to the server respectively. Fig.4 the trusted third party (TTP) interface which calls for the authentication steps and also do work in collaboration with KDCs, Signature Policy, Claim Policy and cipher text. The RSA algorithm is used to encrypt and decrypt the keys with key size of 2048 bits; these keys are split and stored in different places. Hence these four sets are needed to work with data, this makes the system complex and decreases the chances of security breaching.

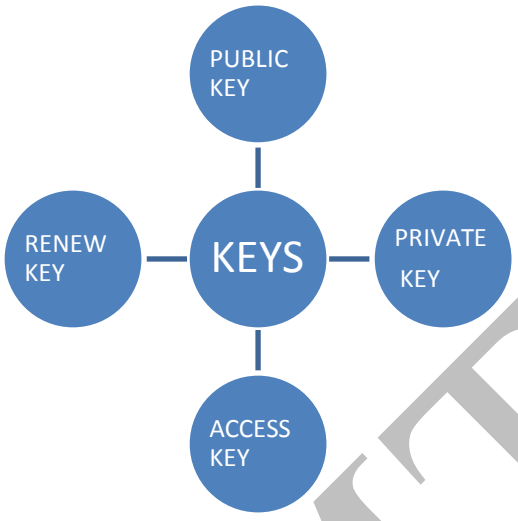

Fig. 3 Keys in the System

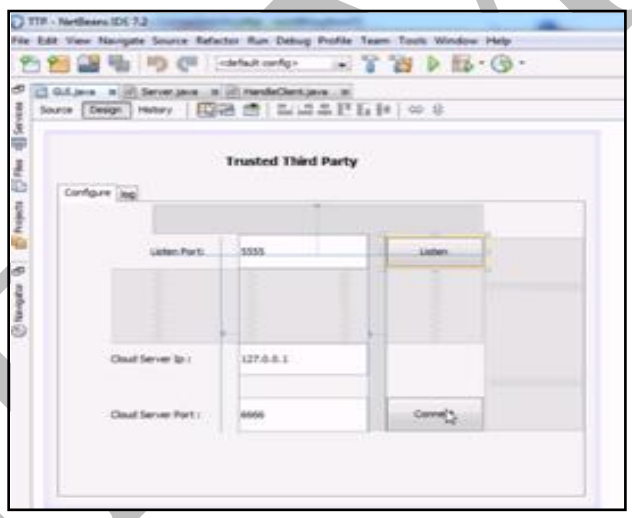

Fig. 4 Trusted Third party Interface

Table I shows the comparative analysis with the existing and the proposed work.

TABLE I. ANALYSIS RESULTS

TABLE II.

Technique	**Existing**	**Proposed**
Approach	**Centralized**	**Decentralized**
Key Encryption	ABE for Secret Key	KDC Method for Key encryption
Authentication	Not Provided	Validity without revealing the user's identity
Type of Key	Symmetric Key	Asymmetric Key
Attack Resistance	Resistant to Replay Attacks	Resistant to Collusion Attacks.

VI. CONCLUSION

The secured way of working with cloud is proposed in which the anonymous user can also upload /download the data without being let his/her identity revealed. The server only known to the keys which are generated by the third party, that is considered as the most honest object in the whole work. This system has its own merits and demerits because the data with which one is working can be very sensitive or this technique can be used in a negative way, so its whole on user's responsibility how he/she handle this or work with this technique. Since now-a-days everything is moving to the clouds this proposal can be proved as a boon for the new era of this technology.

REFERENCES

1. A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.
2. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABECiphertexts," Proc. USENIX Security Symp., 2011
3. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and CollusionResistance," IACR Cryptology ePrint Archive, 2008.
4. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.
5. Sushmita Ruj, Member, Ieee, Milos Stojmenovic, Member, Ieee, And Amiya Nayak," Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds" IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014
6. A. Sahai and B. Waters, "Fuzzy IdentityBased Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005
7. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
8. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
9. M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515- 534, 2007.
10. V.R.Mani Megalai, R.Mekala M.E. , "A Literature Survey On Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds Using KDC" ,IJARECE, Vol 3, Issue-12, Dec 2014