Review on Decentralized Access Control with Anonymous Authentication

Prof D.S.Thosar[1], Punam S.Jadhav[2],Shruti S.Thosar[3],Swapnali D.Sarode[4]
[1]Assistant Prof. Computer Departm[1],
[2,3,4]Student Of Computer Engineering,
SVIT Chincholi
Email ID
[1]devidas.thosar@pravara.in.
[2] punamjadhav1212@gmail.com,
[3]shrutisthosar@gmail.com,
[4]sarodeswapnali1996@gmail.com.

Abstract— In Online social networking access control is very important and only valid user must be allowed to access and store personal information, images and videos and all this data is stored in cloud.The goal is not just store the data securely in cloud it is also important to make secure that anonymity of user is ensured. Also we can use the benefits of cloud in providing certain control over corruption. People step back to take any step against corrupt actions due to fear of revealing their identity. For this anonymous authenticity is provided by cloud. In this system, distributed access control that is only approved users with valid attributes can have entry to data in cloud. Also the identity of the user is kept a secret. There are many KDCs for key management because of this the architecture is decentralized. There is no access of data for users who have been revoked. The system is flexible to replay attacks.

Keywords:-Cloud environment, Security, Privacy, Authentication, Anonymity,Key Generation Center, Attribute Based Encryption, Access Control.

I.INTRODUCTION

Now-a-days, the communication network is widely developed. Text and files can be shared in many forms. The data is encrypted for the sake of secure data storage. The data stored in cloud is frequently modified so this feature is to be considered while designing the proficient secure storage techniques. Privacy and security are very important and critical issues in cloud computing[4]. Major thing is that other users do not know the identity of any user. Anonymous authentication allow any user to access any public content without providing a user and password challenge to the client browser anonymous authentication is used to hide the identity of the user. Anonymous authentication allows user to visit to the public wall. Key is generated which generates the token id. Using AES algorithm the records are encrypted under some access policy and stored in the cloud.[1]

The goal is not just store the data securely in cloud it is also important to make secure that anonymity of user is ensured. Also we can use the benefits of cloud in providing certain control over corruption. People step back to take any step against corrupt actions due to fear of revealing their identity.

For this anonymous authenticity is provided by cloud. In this paper, distributed access control that is only approved users with valid attributes can have entry to data in cloud. Also the identity of the user is kept a secret. There are many KDCs for
key management because of this the architecture is decentralized. There is no access of data for users who have been revoked. The system is flexible to replay attacks. There is support for multiple read and write operations on data in cloud. The costs are analogous to centralized approaches and cloud performs the costly operations [4].

II. LITERATURE SURVEY

To ensure anonymous user authentication ABSs were introduced by Majietal. This was also a centralized approach. A recent scheme by Majietal.takes a decentralized approach and provides authentication without disclosing the identity of the users.In this system we are going to use KDC for generation of encrypted Tokens and encrypted keys. Key distribution is done in a decentralized way.There is KDC which generates encryption and decryption keys and keys for signing. Creator on presenting token to KDC it will provide secret keys and keys for signing. The cloud takes decentralized approach in distributing secret keys and attributes to user[1].

S. Ruj proposed a distributed access control mechanism in clouds.However, the scheme did not provide user authentication. The other drawback was that a user can create and store a file and other users can only read the file. Write access was permitted to users other than the creator[3].

In NMC (Nasik Municipal Corporation) app also complaints get registered but if user complaint is fake then also it gets registered. This may cause to fraud and there may be risk to take action against these complaints. The user wants to upload some videos, P.D.F files for evidence or proof then he can't. As only images can be uploaded as proof.NMC does not provide the anonymous authentication means it does not hide the users identity which may be dangerous for the users who are complaining. The complaints which are registered by the users and the actions which are taken by the authorized person against the

registered complaint is not displayed publically i.e. on public wall.

III. PROPOSED SYSTEM

The idea is purpose that Decentralized Access Control with Anonymous Authentication which provides user revocation and prevents replay attacks. Anonymity is the Key Element of our system[1].Anonymity ensures that the user may access resource or services without disclosing his identity. Here , The cloud does not know who stores the information on cloud, it only verifies user's credentials.

IV. SYSTEM ARCHITECTURE

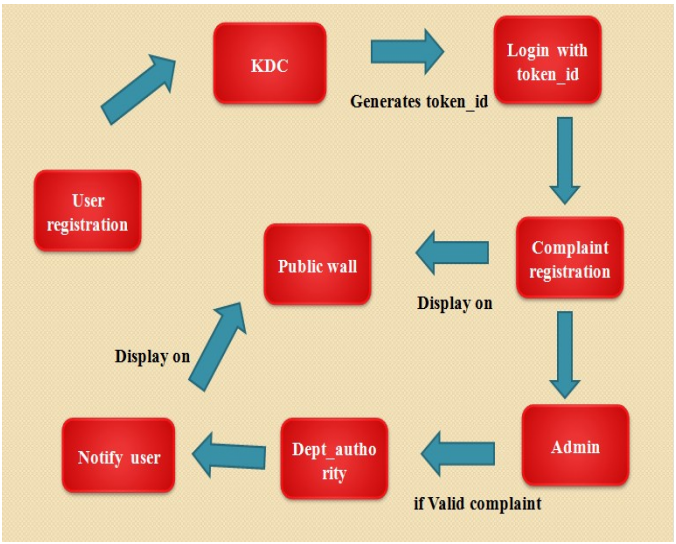

Fig 1.System Architecture

***Token Generation*:** In this method, we will generate encrypted token by KDC. A security token may be a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens. Security tokens are used to prove one's identity electronically. The token is used in addition to or in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access something.

Key Generation: After Validating the tokens we will generate the encrypted key to the user. Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted.

Product Function:

- Registration - Register user with name, email, Date of Birth and address.Token will be sent to specified email to authenticate user.If token is correct, then user will again get key on email, thereafter email and key will be the log-in credentials.
- After Logging In, user can upload files on Cloud and see list of uploaded files if uploaded before. Also user can share files from his uploaded file list through email.

V. ALGORITHM AND MATHEMATICAL MODULE

Algorithm:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES).

Operation of AES

AES is based on substitution permutation network. It consists of a series of linked operations, some of them replacing inputs by specific outputs (substitutions) and others involve shuffling bits around. This algorithm performs all it computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. In AES algorithm for 128-bit keys 10 rounds,for 192-bit keys 12 rounds,for 256-bit keys 14 rounds are performed.

i)Byte Substitution (SubBytes)

The 16 input bytes are substituted in 4 by 4 matrix i.e. four rows and four columns.

ii)Shiftrows

Rows of the matrix are shifted towards left. Shift is carried out as follow

1)First row is not shifted
2)Second row is shifted one (byte) position to the left.
3) Third row is shifted two positions to the left.
4) Fourth row is shifted three positions to the left.
5) The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

iii)MixColumns

This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column using special mathematical function. It results in another new matrix consisting of 16 new bytes. This step is not performed in the last round.

iv)Addroundkey

XORed operation is performed between round key and final matrix which is formed after mix column process . If this is the last round then the output is the ciphertext.

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order.

1)Add round key
2) Mix columns
3)Shift rows
4)Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented,although they are very closely related.

Mathematical Model:

1.Lets S be the System.
where, S = I, O, F, Success, Failure

1.I = Input to the system
I= I1, I2, I3, I4
I1: name
I2: email
I3: private key
I4: file upload
2.O = Identify Output.
O=O1,O2,O3

O1: confirmation mail
O2: file download

O3: comments
4.Lets F be the Functions.
F = Set of functions
F = F1, F2, F3, F4, F5, F6
F1: Register
F2: Login
F3: Token Generation
F4: Upload
F5: Download
F6: Email
Success = All functionality working successfully.
Failure = Internet connection unavailable or any problem in computer hardware.

VI. EXPECTED RESULT

The expected result is that the Token will be sent to specified email to authenticate user& user should use those token for login into the system. Most important is that the user information kept anonymous. After log-in into system user can register their complaints and that complaints documents must uploaded on server. If user choose particular complaint sector/division then compliant documents respective file is delivered to the authorities in any case and also displays on public wall.

VII. FUTURE WORK

In future, Not only hide the user identity we can also hide the mac address of system from where user stores information like user registration and upload files. Also the response time will be increase.

REFERENCES

[1] Sushmita Ruj, Milos Stojmenovic, and AmiyaNayak, ˆa Decentralized Access Control with Anonymous Authentication of Data Stored in Cloudsˆa, IEEE Trans. on Parallel and Distributed Systems, vol. 25, pp 1-11, 2014.
[2] H.K. Maji, M. Prabhakaran, and M. Rosulek, ˆaAttribute-Based Signatures,ˆa Topics in Cryptology CT-RSA, vol. 6558, pp 1-3, 2011.
[3] S. Ruj, M. Stojmenovic, and A. Nayak, ˆaPrivacy Preserving Access Control with Authentication for Securing Data in Clouds,ˆaProc.IEEE/ACM Intˆalsymp. Cluster, Cloud and Grid Computing, pp 1-8, 2012.
[4] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, ˆaToward Secure and Dependable Storage Services in Cloud Computing,ˆaIEEE Trans. Services Computing, vol. 5, no.2, pp 1-13, 2012.