International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 01 | Jan-2018 www.irjet.net p-ISSN: 2395-0072

Employment Feedback by Securing Data Using Anonymous Authentication

Manish Dilip Chaudhari[1], Suraj Haridas Bodkhe[2], Yash Suresh Bedse[3]

[1,2,3]Student,Dept. Of Computer Engineering, R. H. Sapat College of Engineering Management Studies and Research, Nashik, Maharashtra, India

---

Abstract - *Now-a-days, the communication network is widely developed. Text and files can be shared in many forms. 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. People step back to take any step against corrupt actions due to fear of revealing their identity. For this anonymous authenticity is provided. The goal is not just store the data securely, it is also important to make secure that anonymity of user is ensured. Another problem that arises is that what if some evidence is uploaded and the authentic user is not able to post it or it is not send to the organization. To overcome this the proofs should directly go to the head of a certain organization with the help of emails ex- companies, government sectors, etc. Also the identity of the user is kept a secret. There is no access of data for users who have been revoked.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.*

Keywords: **Authentication, Attribute-based encryption, Cryptography,. Attribute based signatures, AES(Advanced Encryption Standard), Security.**

1. INTRODUCTION

The communication network is widely developed. In Online social networking access control is very important and only valid user must be allowed to access and store personal information. People step back to take any step against corrupt actions due to fear of revealing their identity.For this anonymous authenticity is provided.

Another problem that arises is that what if some evidence is uploaded and the authentic user is not able to post it or it is not send to the organization. To overcome this the proofs should directly go to the head of a certain organization with the help of emails ex-companies, government sectors, etc. Also the identity of the user is kept a secret. There is no access of data for users who have been revoked. The system is flexible to replay attacks.

1.1 Attribute-Based Signatures Achieving Attribute Privacy and Collusion Resistance anonymous.

To ensure user authentication ABSs were introduced. This was also a centralized approach. A recent scheme takes a decentralized approach and provides authentication without disclosing the identity of the users. People step back to take any step against corrupt actions due to fear of revealing their identity. For this anonymous authenticity is provided. The goal is not just store the data securely , it is also important to make secure that anonymity of user is ensured. Another problem that arises is that what if some evidence is uploaded and the authentic user is not able to post it or it is not send to the organization. To overcome this the proofs should directly go to the head of a certain organization with the help of emails ex- companies, government sectors, etc. Also the identity of the user is kept a secret. 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.[1][2]

1.2 Privacy Preserving Access Control with Authentication for Securing Data in Clouds.

This presents a distributed access control mechanism in clouds. The scheme did not provide user authentication. And the other drawback was that a user can create and store ale and other users can only read the file. Write access was permitted to users other than the creator. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.[2]

2. KDC [Key Distribution Centre]

KDC: Key Distribution Center is consolidated system where a lone KDC scatters secret keys and it attributes to all customers that are accessible. Single KDC is a solitary reason for disillusionment; with single riddle key frustration, a whole structure can fall. KDC is difficult to keep up as a consequence of a generous number of customers that are accessible in the cloud for information sharing or limit. Accordingly, this underline fogs should take decentralized procedure for passing on riddle keys.

Instantly days it's extremely trademark that fogs have various KDCs in different remote spots in the framework. In every one of these cases, unscrambling at client's end is

calculation escalated. Along these lines, this system may be wasteful when clients access utilizing their cell phones.

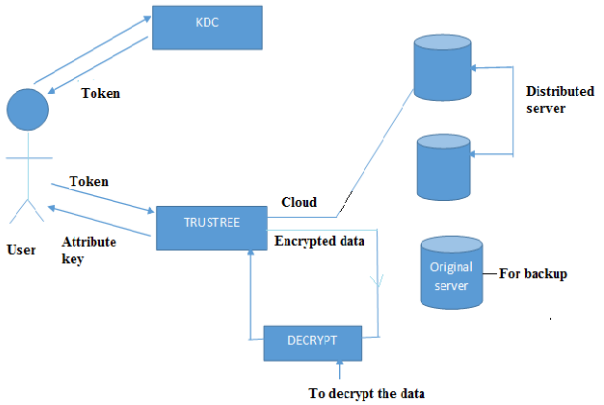


Fig-1 KDC Working

To get over this issue, work proposed to outsource the unscrambling assignment to an intermediary server so that the client can rival least assets (for instance, handheld gadgets). Nonetheless, the vicinity of one intermediary and KDC makes it less effective than decentralized methodologies. Both these methodologies had no real way to approve clients, namelessly. Changes of verified clients, who need to stay unknown while getting to the cloud. As of late distinctive procedures take a shot at the decentralized approach and gives confirmation without uncovering the character of the clients. As said in the past segment it is inclined to replay assaults.

3. 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.

4. PRILIMANARIES

4.1 Identity

4.2 Privacy

4.3 Anonymity

4.4 Anonymous communication: case of Tor Network

4.1 Identity

The identity of a Cloud user, his electronic identity User ID, Pseudonym or his PII "Personally Identifiable Information". This later includes any information that could be used to identify or locate an individual e.g. name, address or information that can be correlated with other information to identify an individual e.g. credit card number, postal code, IP address The protection of PIIs of unwanted or unauthorized dissemination is often a legal requirement, and belongs to the domain of protection of Privacy.

4.2Privacy

In the context of our work, privacy is the ability of a system to protect the identity and the location of its users from unauthorized disclosure. Privacy is the right of individuals to determine where, when, and how their personal information is shared with other parties. Cloud Computing service consumers have little knowledge about the inner workings of the Cloud Service Provider system. Privacy in cloud Computing can be defined as the ability of an entity to control what information it reveals about itself to the cloud (or to the CSP), and the ability to control who can access that
information.

4.3Anonymity

Anonymity ensures that the user may use a resource or service without disclosing his identity. The requirements for anonymity ensure the user's identity protection related to a subject or an operation.

4.4Anonymous communication: case of Tor Network

Instead of taking a direct route between the source and the destination, in an anonymous communication, data packets follow a pre-selected random trajectory. This path defines the intermediate points through which will pass the data packet (which are number three relays in case the Tor network) outside its routing on the Internet (the packet passes through routers real network but must be routed in each case to a relay node to make it decryption and header modification before injecting it into the network). No one can be deduced from the observation of a single point, where came from or where will the data.

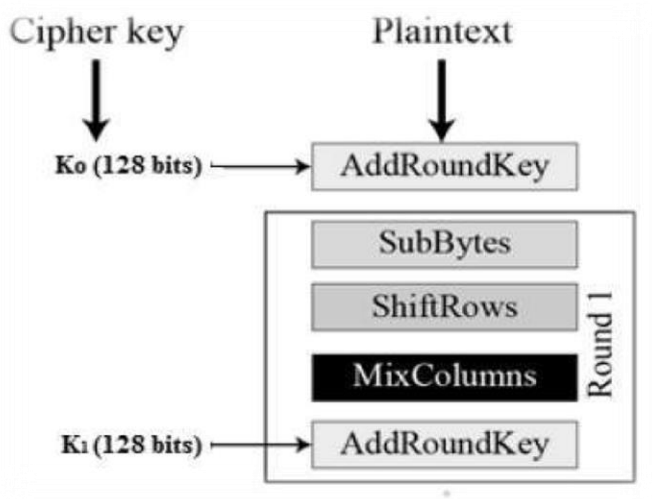
5. AES (ADVANCED ENCRYPTION STANDARD)

The more popular and widely adopted symmetric encryption algorithm likely to be encountered now a days is the Advanced Encryption Standard *AES*. It is found at least six time faster than triple DES.[5] A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

1. Symmetric key symmetric block cipher.
2. 128-bit data, 128/192/256-bit keys.
3. Stronger and faster than Triple-DES.
4. Provide full specification and design details.
5. Software implementable in C and Java.

5.1Encryption Process



Byte Substitution *Sub Bytes :*

The 16 input bytes are substituted by looking up a fixed table *S – box* given in design. The result is in a matrix of four rows and four columns.[3]

Shiftrows :

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

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.

MixColumns :

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey :

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.[3]

6. CONCLUSIONS

We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. We have added a timer function which will automatically upload the file after a certain period of time, if any failure. As soon as any news, evidences,etc are uploaded , they are immediately send to the head of particular organization.

REFERENCES

[1] M. Chase, "Multi-Authority Attribute Base Encryption," Proc.Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007. .

[2] N. Park, "Customized healthcare infrastructure using privacy weight level based on smart device", Int. Conf. on Hybrid Info. Technology., *2011.*

[3] B. Fabian, T. Ermakova, P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds", Information Systems, *2015.*

[4] P. S. Mukesh, M. S. Pandya and S. Pathak, "Enhancing AES algorithm with arithmetic coding," 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), pp. 83–86, IEEE, 2013.

[5] K. Lala, A. Kumar and A. Kumar, "Enhanced throughput AES encryption," IJECSE, vol. 1, p. 2132–2137, 2012.