CORRUPTION UNMASKING SYSTEM WITH ANONYMOUS AUTHENTICTION OF DATA STORED IN CLOUD

Neha Doshi (doshineha9@gmail.com), Prajakta Dhaygude, Priya chavan

DEPARTMENT OF COMPUTER ENGINEERING D. Y. Patil Institute of Technology,Pimpri,411018

ABSTRACT

In this project, we are proposing corruption unmasking system using anony- mous authentication in cloud. Along with that we are asserting decentral- ized access control scheme for secure data storage in cloud which support anonymous authentication, by hiding the identity of user we can upload and publish the confidential data along with attributes such as email id, which is medium for notification. Our scheme has features of access control in which concerned authorities has read only access. Moreover, our authentication and access control is decentralized and robust.

I. INTRODUCTION

In today's world, the communication network is widely developed, you can send the texts as well as files, also it can be shared in one or many form. While communicating with the other person via medium the registered de- tails become transparent to the third party; what if we could demolish the transparency? Much of the data stored in clouds is highly sensitive, for ex- ample, medical records and social networks. Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement. We propose a cloud system where user can upload, download, view and also share data by keeping his identity anonymous. The application can be an anonymous sharing system for gov- ernment where user can bring into notice the certain issues of government by keeping his identity anonymous.

II. LITERATURE SURVEY

1. S. Ruj et al[1] Dacc: "Distributed Access Control In Cloud" has pro- posed a data storage and access in which the multiple encrypted copies of data can be avoided. The main novelty of this paper is producing the key distribution centers where one or more KDCs distribute keys to data owners and users. KDC provide access to particular fields in all records. Single keys separates the data and the data owners, using this technique the user own the data by having the attribute it had, and this can be retrieved only if the attribute matches the data. The Author apply the attribute based encryption (ABE) based on bilinear pairings on elliptic curves. This scheme is collusion secure in which two users cannot together decode any data, that no one has individual right to access.

2. H.K.Maji et al[2] "Attribute-Based Signatures: Achieving Attribute- Privacy Collusion Resistance" has proposed an Attribute based Sig- nature in which the signature attests not to identify the individual of the message by a user instead it claim regarding the attribute that produced by the user. The signature was produced by a single party whose attributes satisfy the claim being made i.e. it is not colluding the all individuals instead it just make the attribute together who pooled it. The author explains the security requirements of ABS as a crypto- graphic primitive, and then tells that efficient ABS construction based on groups with bilinear pairings. Thus by proving the construction is secure in the generic group model, ABS fills a critical security require- ment in attribute-based messaging (ABM) systems. A powerful feature of ABS construction is that unlike many other attribute based crypto- graphic primitives, it can be readily used in a multi-authority setting, wherein users can make claims involving combinations of attributes issued by independent and mutually distrusting authorities.

3. W. Wang et al[3] "Secure and Efficient Access to Outsourced Data" has proposed by providing secure and efficient access to outsourced data should be must in cloud computing .To encrypt every data block with a different key the flexible cryptography-based access control is used.

Through this key derivation methods, the owner should maintain only a few secrets in the storage, and this key derivation procedure is used in hash functions which will introduce very limited computation

.Thus to use over-encryption and or lazy revocation to prevent revoked users from getting access to updated data blocks. A Mechanism is used to handle both updates to outsourced data and changes in user access rights. Hence it is investigated in the overhead and safety of the proposed approach an encryptor can choose, for each authority, a number do and a set of attributes. Thus this scheme tolerate an arbitrary number of corrupt authorities.

4. A. Beimel[4] "Secured Scheme For Secret Sharing And Key Distribu- tion" has proposed the sharing of data, now a days take place in Com- puter Networks, and the data which is been communicated inside the network may affected through the bad users, to overcome this user users two Cryptographic tools such as Generalized Secret Sharing scheme and Key distribution scheme. This make it possible to store only the se- cret information in the network such that only good users can access the information, the secret sharing scheme mostly received through the threshold secret sharing schemes, only through the certain threshold

the information can accessed and can used by the user. In generalized secret sharing it is capable of arbitrary monotone collection whereas in Key distribution scheme the keys can be used Communication key Dis- tribution scheme does not help in unrestricted scheme on other hand secured and restricted scheme can be accessed only through limits. Lin- ear Secret Sharing Scheme, Monotone Span programs, Secret sharing the public reconstruction computation function of shared secret keys are used.

5. J. Bethencourt et al[5]"Cipher text-Policy Attribute-Based Encryp- tion" has proposed certain distributed system the user can access the data only if the data consist of credential or attributes. Only way of en- forcing such data in Cloud can be performed through the trusted server to store the data and accessing the cloud. In this paper the complex access control on the encrypted data is performed in which the Cipher text policy Attribute-Based Encryption is used. By using this scheme the storage data can be kept confidential even when the storage is un- trusted, and this method secures against the collusion attack. The Previous Attribute Based Encryption systems used attributes to de- scribe the encrypted data and even to build policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

III. IMPLEMENTATION

AES (acronym of Advanced Encryption Standard) is a symmetric encryp- tion algorithm. The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of con- figurable computing resources that can be rapidly provisioned and released with minimal management effort. Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and un- predictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

Algorithm

- Cipher(byte in[16], byte out[16], keyarrayroundk ey[N r + 1])begin
- byte state[16];
- state = in;
- AddRoundKey(state, roundk ey[0]); fori = 1toN r − 1stepsize1do
- SubBytes(state);
- ShiftRows(state);
- MixColumns(state);
- AddRoundKey(state, roundk ey[i]); endfor
- SubBytes(state);
- ShiftRows(state);
- AddRoundKey(state, roundk ey[N r]); end

IV. CONCLUSION

We have presented a decentralized access control technique with anonymous authentication.No one knows the identity of the user who stores informa- tion.Key distribution is done in a decentralized way. The user credentials are known by cloud who store the data but cloud does not know who the user is. We have presented a decentralized access control technique with anonymous authentication.No one Knows the identity of the user who stores informa- tion. Key distribution is done in a decentralized way.The user credentials are known by cloud who store the data but cloud does not know who the user is.

V. REFERENCES

1.https://www.scribd.com/doc/246359066/Decentralized-Access- Control- With-Anonymous-Authentication- of-Data- Stored-in- Clouds-Parallel- Distributed-Systems
2.http://www.ijritcc.org/download/1430463081.pdf
3.http://www.slideshare.net/IGEEKS/decentralized-access-control-with- anonymous-authentication- of-.Data- stored-in- clouds-38612620
4.http://www.ijarcce.com/upload/2013/november/21-H-Ranjith-SECURE- FINAL.pdf
5.Hyun-Suk Yu, Yvette E.Gelogo,K J Kim, Securing Data Storage in Cloud Computing,
J.of Security Engineering, June 2012,pp,252-259.

6.V. Paranjape and V. Pandey, An approach towards security in private cloud using otp.
7.https://iraj.in/upproc/pdf/127−142528046912−17.pdf.ww w.tutorialspoint.com/crytography/ad