Attributed Users for Anonymous Authentication In Distributed Cloud Data-storage.

Karan Dahima, Mandar Bhosale, Darshan Devrai, Madhav Sharma

***Abstract*- The paper proposes a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication to registered users. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing data. The Cloud itself has no idea of what data is been stored. This scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading the data stored in the Cloud. The paper also addresses user revocation. The data when stored on Cloud is divided and stored on multiple databases. Cloud does the part of storing and retrieving data without knowledge of its contents.**

***Index Terms*-Access control, Authentication, Attribute-based signatures, Attribute based encryption, Distributed Cloud storage, Decryption, File Encryption, Role Based Access.**

I. INTRODUCTION

The current trend towards Cloud and the ongoing research in cloud computing is receiving a lot of attention from both academic and industrial worlds. The beneficiary of cloud computing for users who can outsource their processing computations and storage to servers. [1]This relives users from the hassles of maintaining resources on-site. Clouds is divided into multiple criteria's depending upon services they provide. Several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures E.g. Amazon'sEC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon'sS3, Windows, Azure). Mostly data stored in clouds is highly sensitive, private medical records and social networks. Thus making Security and privacy a 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. The cloud Service provider can hold the user accountable for the data it outsources, and likewise, the CSP itself accountable for the services it provides.

Ensuring security and privacy, there is also a need for law enforcement. Recently, addressed secure and dependable cloud storage. Cloud servers prone to Byzantine failure, where a server can fail in many ways. The cloud is also prone to various data modification and server related attacks. To provide secure data storage, the data needs to be encrypted.

***Karan Dahima,** Computer Engineering, SKN SITS, Lonavala,Pune, India,7738194522 .*
***Mandar Bhosale**, Computer Engineering, SKN SITS, Lonavala,Pune, India, 7350219911.*
***Darshan Devraye**, Computer Engineering, SKN SITS, Lonavala,Pune, India, 8308344885.*
***Madhav Sharma**, Computer Engineering, SKN SITS, Lonavala,Pune, India, 9421941575.*

II. LITERATURE SURVEY

[1] Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds (2014)

Author : Sushmita Ruj , Milos .S , Amiya Nayak

In this proposed scheme the cloud verifies the authenticity of any user without having knowledge of his /her identity before storing the Data over Cloud. The authentication and access control scheme of this paper in centralized and the user are given rights which also can be revoked later, also it allows data to be written multiple times. They have used attributed based signature scheme for authentication. The scheme is resilient to replay attacks. The drawback here is that the data stored in Cloud is in a centralized location. Also the Decryption of database takes place as users end which leads to lag at system.

[2] Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control (2014)

This paper proposes access control scheme for data storage, which supports anonymous authentication and performs decentralized key management. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against replay attacks.

[3] Privacy Preserving Access Control with Authentication for Securing Data in Clouds (2012)

Author : Sushmita Ruj , Milos .S , Amiya Nayak

This is the Base paper for Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds by the same authors. The papers discusses on user authentication who store and modify their data on cloud. The identity of user is protected from cloud during authentication. The architecture is decentralized meaning there are multiple KDC for key management. The protocol Supports multiple read and write on the data stored in the cloud .The cost is comparable to the existing centralized approaches. The only drawback was the authentication of validating the message without revealing the identity of the user who has stored the information.

[4] Toward Secure and Dependable Storage Services in Cloud Computing (2012)

Auhtor : C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou

Cloud allows users to store data in a remote location and enjoy on demand high quality cloud resources ,even if the benefits are clear ,such a service is also relinquishing users mindset towards their stored data which brings in new security risks. This paper proposes a design of distributed storage integrity, using the homomorphic token and distributed erasure coded data. It

ISSN: 2278 – 1323

allows detecting misbehaving server's .It also allows operation like block modification, deletion and append. This scheme is highly efficient against Byzantine failure, malicious data modification and server colluding attacks.

III. PROBLEM STATEMENT

In cloud computing, the data stored in cloud is highly sensitive which can be snooped by the cloud owner and also can be hacked. The confidentiality of the data is always the scanner and vulnerable to threads. The data stored in the cloud contains corporate organizational level information which requires high end security from malicious attacks. Hence encryption is required before the data is stored in the cloud. Secondly another point of concern is anonymity of user who desires to store the data on the cloud staying anonymous. The user if wants to upload sensitive and confidential data on the cloud and wants no recognition.

Goal and Objectives:
_ Encryption of the data at the cloud end to keep the data safe from intruders.
_ Partition of the encrypted data adding to additional security.
_ To keep the user anonymous providing a middleware which uses a secure recognition protocol for covert uploading of data.
_ Secure and easy retrieval the original data if the partitioned server goes down.

Cloud Computing :

1. Achieve economies of scale: Increasing the productivity by using less people.(Workforce for handling servers ,maintenance is reduced)

2. Investment reduction on spending on Infrastructure. Maintaining easy access to user information

With minimal spending. Policies: Pay as you go and based on demand.

3. Globalize your workforce on the cheap. People worldwide can access the cloud, provided they have an Internet connection.

4. Streamline processes. Get more work done in less time with less people.

5. Reduce capital costs. Initial investment on hardware ,storage or licensing fees is required.The

cloud rent covers everything.

6. Improve accessibility. You have access anytime, anywhere, only Internet connection is mandatory.

7. Monitor projects more effectively. Stay within budget and ahead of completion cycle times,etc.

IV. WORK CASE

Key Distribution Center (KDC) : It is responsible for Taking in Information from the user an providing it with a Token . Information gained is mostly Name, Address, D.O.B, Signature, and Social Security Number. The Token is then used for getting access into Trustee software for verification.

Trustee Software :- The user enters its Token in the Trustee Software which tells the software that the user is a authenticated user, this then gives the user a Attributed Key which can be used by the user later for gaining access into cloud and storing data.

V. FLOW MECHANISM

The exact working of the system is explained in through the figure: 1 with the control flow mechanism.

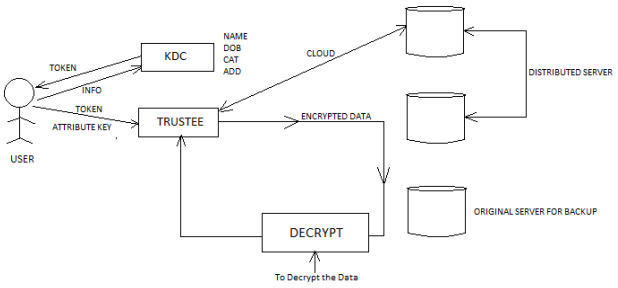

Fig No: 1

1. As we can there is user who provides information like NAME,DOB,ADD etc to the Key Distribution Centre(KDC).
2. The KDC in return gives Token to the user.
3. The user provides the token to the trustee middleware, the later validates it with the shared database of KDC.
4. The trustee then provides with authentication key and login details for further login.
5. The user then uploads data on the cloud through the trustee.
6. The trustee is responsible for encryption of data and forwarding it to the cloud database.
7. The data is stored in a distributed database.With a duplicate copy of original data in backup server.
8. The user if wants to retrieve the data . LOGS IN. the trustee and the data is decrypted and provided back.

VI. APPLICATION

Government Organization:- The data related to a department can be shared among the same department to only people who have right to read it. Any government

ISSN: 2278 – 1323

employee can share data related to any malpractices or corruption in the office to report to the higher authority.

International Security Agencies: - Any individual person can upload data regarding terrorism on the Cloud, hiding his own information and mentioning to whom to share this data.

Universities: - The data can be stored on a shared Server and can be access on any device through Internet.

VII. SUMMARY

1. Distributed access control of data stored in Cloud.
2. Authentication of user who store Data on Cloud.
3. Decentralized Architecture for KDC ,Cloud and Trustee Software.
4. Users that are revoked ,cannot access data later.
5. Cloud has no idea who is storing data and what data is been stored.
6. Attribute Based Encryption is used along with Attributed Based Signature for authentication.
7. Key Distribution center for providing with Tokens to users.
8. Distributed Servers for storing data.
9. Single Server as Backup with the original Copy.

VIII. CONCLUSION

As the technology is advancing every day the need to keep the data secure from intruders is imminent. The intrusion of privacy is also an important fundamental cause for increasing preparedness to tackle such kind of problems. With the use of this middleware the user gets an upper hand over intruders and it helps them to use the cloud anonymously. The cloud seems to be possibly unsecured and monitored data technology, which can cause privacy invasion and data leaks. Thus with the middleware the possible hurdle can be tackled efficiently.

IX. ACKNOWLEDGMENT

We take this opportunity to thank our project guide Prof.PraveenKumar Keskar and Head of the Department Prof. V.D Thombre for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this survey. We are also thankful to all the staff members of the Department of Computer of SKNSITS College of engineering, Lonavala, pune for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

[1] Sushmita Ruj, Milos Stojmenovic , Amiya Nayak. "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" IEEE Vol:25 NO:2 Year:2014

[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T. Services Computing*, vol. 5,no.2,pp.220–232,2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *IEEE INFOCOM*. , pp.441–445, 2010.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography Workshops*, ser. Lecture Notes in Computer Science, vol.6054. Springer,pp.136–149,2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-ased authentication for cloudcomputing," in *CloudCom*, ser. Lecture Notes in Computer Science, vol.5931. Springer,pp.157–166,2009.

[6] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation,Stanford University, 2009,http://www.crypto.stanford.edu/craig.

[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," in *TRUST*, ser. Lecture NotesinComputer Science,vol.6101.Springer, pp.417–429,2010.

[8] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg,Q. Liang, and B. S. Lee, "Trustcloud: A framework for accountability and trust in cloud computing," HP Technical Report HPL-2011-38.Available http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," in *ACM ASIACCS*, pp.282–292,2010.

[10] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in *15th National Computer Security Conference*, 1992.

Karan Dahima is in his 4th year of B.E Computer Engineering of Savitribai Phule Pune University,Pune.He is an avid enthusiast in the latest computer science research work and works for his family business on Home automation

Mandar Bhosale is in his 4th year of B.E Computer Engineering of Savitribai Phule Pune University,Pune.He has gained knowledge is networking domains and administrations. He has certifications is CCNA routing & switching, MCSA with private cloud, RHCE with private Cloud .and VMware cloud. Management and Deployment.

ISSN: 2278 – 1323

Darshan Devraye is in his 4th year of B.E Computer Engineering of Savitribai Phule Pune University,Pune.and loves coding in his past time.He has his skill set in JAVA and ASP.NET.

Madhav Sharma is in his 4th year of B.E Computer Engineering of Savitribai Phule Pune University,Pune.and loves coding in his past time.And has successfully completed his internship at BARC and C-DAC.

ISSN: 2278 – 1323