International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

i-LOON: The Cloud Application for Secure Data Transmission and Auto-data Deletion

Ashwini Zanzad[1], Anjali Selokar[2], Nandini Jain[3], Sneha Godbole[4], Sarita Sakure[5]

[1234] *Student, CSE, Dr. Bababsaheb Ambedkar college of engineering and research, Maharashtra, India*

[5] *Assistant professor, CSE, Dr. Bababsaheb Ambedkar college of engineering and research, Maharashtra, India*

Abstract - ***This i-Loon is a cloud application for a group of people or an organization where user can send their confidential data to other user. To create a cloud application that store, share and access data from anywhere over the internet. The data can be shared with multiple authorized users at same instance of time using cryptography. The data encrypts before sending to other users. The unused and secure data gets deleted after user specific time. The user can specify the TTL for any document, text or image. TTL for document will provide the expiration time for any document, so that it will refresh the memory. This project will also focus on maintenance of cloud storage as it will delete data after TTL. The application uses a public key encryption method with time specific attribute. It is the secure auto deletion scheme associated with time instant. In this scheme the cipher text contains the time interval generated from the time server. The cipher text can only decrypted if it is in the allowed time interval.***

1. INTRODUCTION

The cloud is a growing technology which uses network and servers to maintain data and applications. Securing cloud is most threatening issue of cloud computing services. Specially, where user wants to share their private data to other users using cloud. The cloud security is an important aspect to share data over cloud. It is not possible to maintain full lifetime privacy security for data over cloud. The growing hacking and cracking industry will create a problem for private data which is kept over the cloud.

Suppose a user want to sends his ATM pin to other user. The data is sent using only encryption technique. The sender reads that data but not delete it after viewing .then after some days if someone hacks his account then all private data including ATM pin would be known by the hacker. So to avoid such situation the encryption method with TTL for document is used.

The project uses public attribute encryption based technique, which takes the public data of the user for encryption. The data is encrypted from the different combination public attributes. According the encryption is performed, the data is sent to that user whose attributes are used. Here private keys are not generated. The data is sent only to those users whose attributes are used for encryption. Other users belonging to this group receives only cipher text.

This attributes based encryption technique combines with the auto deletion scheme. In this technique, the cipher text is assigned with an time interval. The time instance is generated from the time server which is present at the host computer. The cipher text is present in the cloud only till the Time-to-live for the document is valid. This attribute based encryption technique solves the problem of security by providing authorized time interval to the document. After the time expires, the data self deleted, which maintains the memory and lifetime privacy security measures and also reduces human efforts to delete the data. This project will aim at combining cryptography method with time of expiry of data over an application which is installed in the cloud.

2. LITERATURE REVIEW

[1] Mediated certificate less public key encryption (MCL-PKE).Earlier MCL-PKE scheme encryption methods are not

very efficient because it uses the costly pairing operations and also dangerous to partial decryption attacks. So this paper uses MCL-PKE scheme without pairing operation. User encrypts the private data using cloud created public keys .upon successful authorization, cloud partially decrypt and then user fully decrypt.

[2]A key-policy attribute-based encryption with time-specified attributes (KP-TSABE), is a self data deletion method in cloud computing. In the KP-TSABE method, each cipher text is assigned with a time interval while private key is labeled with a time instant. The cipher text can only be decrypted if both the time instant is in the permitted time interval and the attributes involved with the cipher text satisfy the key's access structure.

[3] Integrity in the cloud computing environment is the most important issue. Co-operative provable data possession is a mechanism for proving the integrity of data in the cloud storage. This paper addresses design of an efficient CPDP scheme and it audits services dynamically for distributed cloud environment and also ensures the integrity of an outsource cloud storage which enhances the scalability and data transmission.

[4] Certain methods have been constructed to allow both data uses and public verifiers to efficiently and successfully audit cloud data integrity without accessing the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information—identity privacy—to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud.

[5] This paper presents a novel Multi-message Cipher- text Policy Attribute-Based Encryption (MCP-ABE) technique, and employs the MCP-ABE to design an access control scheme for sharing scalable media based on data consumers' attributes (e.g., age, nationality, or gender). The scheme is efficient and flexible because MCP-ABE allows a content provider to specify an access policy and encrypt multiple messages within one cipher text such that only the users whose attributes satisfy the access policy can de- crypt the cipher text.

3. PROPOSED SYSTEM

The proposed cloud application has following objectives:

- To create a cloud application, which is used to store, share and access data from anywhere over the internet.
- The data can be shared with authorized users at a same instance of time using cryptography.
- The data encrypts before sending to other users.
- The unused and secure data can get destroyed after given interval of time. So that it will refresh the memory.

The requirements for the project are:

- Visual studio
- SQL Database
- Tomcat apache server
- Windows OS
- Min 2GB storage space
- 1GB RAM

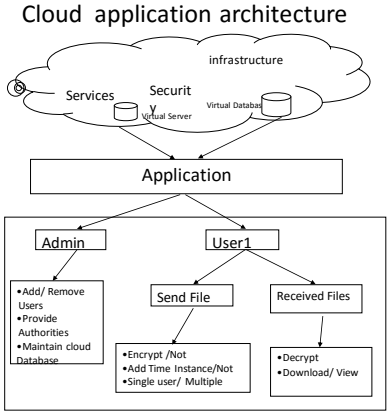

Fig (1.0) represents the architecture of the i-Loon cloud application. The following entities play major role:

I. ADMIN: The admin is responsible for granting the authorization to different users. The users can only use this application if he is authenticated by the admin. The admin can add or remove users. Admin provides session to different users.

II. USERS: User can send data to other users within an organization. Users can also receive the data. User can add time to live to the data so that data self destroyed after the expiration time.

III. CLOUD SERVER: i-Loon web application is deployed on the cloud. The users can access the application anywhere over the internet. Cloud provide complete virtual environment such as platform, infrastructure and varieties of application and system software.

IV. APPLICATION: This application is the user interface written in .net framework. This user interface allows the user to use services and functionalities provided by the cloud.

4. CONCLUSION

- With this cloud application user can able to share data with other user in private group.
- Authorized User can select the user whom the he wants to send data.
- Authorized user can encrypt its sensitive data before sending it over cloud.
- User can set expiry time for data on cloud so that it will refresh memory.
- If data gets expired receiver can request back to sender for resending.

REFERENCES

1.“An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds” Seung-Hyun Seo, *Member IEEE, Mohamed Nabeel, Member IEEE,* Xiaoyu Ding, *Student Member IEEE, and Elisa Bertino, Fellow IEEE*.

2. “A Secure Data Self-Destructing Scheme,” in Proc. ACM Conf. Comput. Commun Security, 2013, Jinbo Xiong, Ximeng Liu and Zhiqiang Yao, Jianfeng Ma, Qi Li, Kui Geng, and Patrick S. Chen.

3.“Framework of data integrity for cross cloud environment using CPDP scheme“, IJARCS-volume-IV ,March-April-2013,By sarita motghare, P.S mohod, S.P khandait, Anil Jeiswal.

4. “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud” Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE.

5. “Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks “by Yongdong Wu, Zhuo Wei, and Robert H. Deng,members IEEE.

BIOGRAPHIES

Ms. Ashwini Zanzad is pursuing her BE in CSE from Dr.Babasaheb Ambedkar college of engineering and research, wanadongari. Dist.-Nagpur, Maharashtra, India.

Ms. Anjali Selokar is pursuing her BE in CSE from Dr. Babasaheb Ambedkar college of engineering and research, wanadongari. Dist.-Nagpur, Maharashtra, India.

Ms .Nandini Jain is pursuing her BE in CSE from Dr. Babasaheb Ambedkar college of engineering and research, wanadongari. Dist.-Nagpur, Maharashtra, India.

Ms. Sneha Godbole is pursuing her BE in CSE from Dr.Babasaheb Ambedkar college of engineering and research,wanadongari. Dist.-Nagpur, Maharashtra, India.

Mrs. Sarita Sakure has completed her B.E from PCEA, Nagpur and M.tech from GHRIET.W, Nagpur and currently working as assistant professor in CSE department in Dr. Babasaheb Ambedkar college of engineering and research, wanadongari. Dist.-Nagpur, Maharashtra, India. She has 4.5 years teaching and 2 years industrial experience.