Survey on Cloud Data Security

Jadhav Chitralekha Arun[1], Prof. Vikas B. Maral[2]
Department of Computer Engineering
[1, 2]KJCOEMR , Pune

Abstract-*Now days, more and more users store their important data in cloud. To ensure the security of the remotely stored data, users need to encrypt important data. From the point of data security which has always been important aspect of quality of service, cloud computing cause's new challenging security threats. Identity-based proxy re-encryption schemes have been proposed to shift the burden of managing numerous files from the owner to a proxy server. The existing solutions suffer from several drawbacks. First the access permission is determined by the central authority, which makes the scheme impractical. Second, they are insecure against collusion attacks .The existing solutions do not actually solve the motivating scenario, when the scheme is applicable for cloud computing. Hence, it remains an interesting and challenging research problem to design an identity-based data storage scheme which is secure against collusion attacks and supports intra-domain and inter-domain queries.*

Keywords-Identity-based encryption (IBE), revocation, outsourcing, cloud computing.

I. INTRODUCTION

From the past couple of years, there has been a persistent development in Cloud Computing. Cloud Computing provides various resources such as computational power, computational platforms, storage and applications to number of users by making use of web. Cloud computing gives a pool which is centralized of configurable computing resources and outsourcing mechanisms that empower distinctive computing services to various individuals in a way similar like utility-based frameworks, for example, electricity, water, and sewage. In electricity, for instance, individuals began to connect with central grids, supported by power utilities as opposed to depending all alone electricity production capabilities.

There is several cloud providers currently in market section such as Amazon, Google, IBM, Microsoft, Salesforce, and so on. With a growing number of associations falling back on use resources in the Cloud; there is a requirement for securing the data of various users.

A few challenges that are being gone up against by Cloud Computing are to secure, protect and prepare the data which is the user's property. Next, we have explained the two guideline expresses that hold your data is out in the Cloud: when the data is in movement (travel) and when the data is rest, where the data is very foreseen that would be more secure. The underneath spoke to are the two essential conditions which we have focused to appreciate the security of the data in the Cloud.

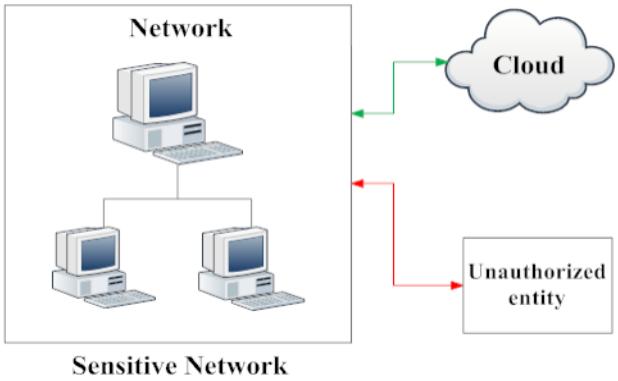

Fig. 1: Network & cloud: unauthorized access of data

In Figure 1, demonstrates the first case in which cloud is a part of the network and a few information of the system is set on cloud. In this situation cloud supplier can't get to the information stored on the network yet now and again cloud may need to get access on a portion of the information stored on network, while getting to this access there will a probability of unapproved access of resources present on the local network.

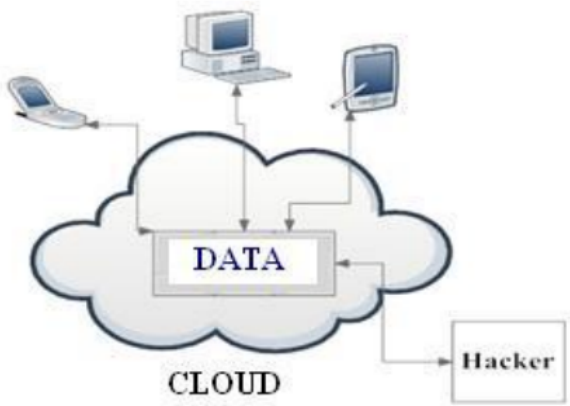

Fig. 2: Cloud hack for unauthorized data

Figure 2 demonstrates the second situation in which the aggregate information of system is put on the cloud for this

situation user can retrieve information from the cloud. At the point there is a probability that the unapproved user to get the information stored on the cloud. In such cases, virtual machines are apportioned to the user of the cloud, which are provided with the substantial logins. Be that as it may, the given logins can be hacked.

Cloud computing as well as storage solution gives ability to user to store as well as process their information in third party data centers. For protecting data and making it more confidential the use of algorithm as well as secret key is done for encrypting data. Once data is encrypted it is then transformed to the cipher text. For the purpose of decryption of cipher text similar algorithm is used for retrieving the original data. Identity-Based Encryption (IBE) is a substitute for public key encryption. It makes key management in certificate based public key infrastructure (PKID) easy by making use of human intelligible identities like name which are unique, email address, ip address as a public keys as well as certificate instead exactly encrypts message with receivers identity. Respectively, receiver getting the private key related with the related identity from private key generator (PKG) can decrypt cipher text. Revocation mechanism is realized by appending validity periods to certificates or using involved combinations of techniques.

This survey presents the different researches by several authors on the data security in cloud.

II. LITERATURE REVIEW

In paper [1], authors have implemented outsourcing computation into IBE and also developed a revocable system in that the revocation operations are delegated to CSP. With the aid of KU-CSP, the developed system is full-featured: It accomplishes constant efficiency for both computation at PKG and private key size at user; User needs not to contact with PKG amid key update, as such, PKG is permitted to be offline after it sends the revocation list to KU-CSP; Nosecure channel or user validation is needed while key-upgrade amongst user and KU-CSP.

In paper [2] authors have developed a privacy preserving authenticated access control system which provides security to the data in clouds. In the developed system, the cloud confirms the authenticity of the client without knowing the client's character before storing data. Proposed system also has the added feature of access control in that only authenticated users can decrypt the stored data. The system is able to stop replay attacks as well as supports creation, modification, also reading data stored in the cloud.

In paper [3] authors has designed flexible distributed storage integrity auditing mechanism, making use of the homomorphic token as well as distributed erasure-coded data. The developed system allows users to audit the cloud storage with very lightweight communication as well as computation cost. The auditing outcomes not only conforms strong cloud storage correctness guarantee, but also concurrently achieves fast information error localization, i.e., the identification of misbehaving server. Taking the cloud information are dynamic in nature, the developed system also supports secure as well as efficient dynamic operations on outsourced data, including block modification, deletion, and append.

In paper [4] authors have developed a novel primitive, known as IBPRE+, that is an identity based proxy re-encryption (PRE) system. It can be seen as the dual of the traditional identity based proxy re-encryption. In designed system, the data owner is able to control sharing capability in a flexible way by making use of random numbers utilized in the encryption process.

In paper [5] authors have developed a big data driven, cloud based ICT system for smart grid. Considering the security needs of every message, they developed an ID based signcryption security system for the system. The implemented IBSC system performs concurrently the functions of encryption as well as digital signature. Hence, intimacy, non-repudiation and integrity of data are given. The designed IBSC system was also maximized to an ID-based digital signature system as well as a key distribution system.

In paper [6] authors have concentrated on the issue of private matching on the outsourced encrypted datasets under identity-based cryptosystem (IBPM) as well as formalize the security of the designed IBPM. Authors developed a concrete construction of the IBPM that makes possible the cloud users to critical private matching operations to cloud as well as realizes fine-grained authorization of matching privileges to the cloud.

In paper [7] authors have developed a technique for cloud data storage gives an efficient method of attribute revocation as well as fault tolerance with the data security. Developed system provides security from different attacks and also minimizes revocation computation overhead. In this system, at the time when a user is revoked the UL is modified as well as when the user get back all the privileges the user name is deleted from the UL. In such way the designed technique minimizes frequent attribute revocation of all users at the time of specific user is revoked.

Table 1: Survey Table

Sr No.	**Title**	**Publication& Year**	**Description**	**Advantages**	**Limitations**
1.	Identity-Based Encryption with Outsourced Revocation in Cloud Computing	IEEE, 2015	Identity-based encryption	Efficient	---
2.	Privacy Preserving Access Control with Authentication for Securing Data in Clouds	IEEE, 2012	This method has privacy preserving Authenticated access control scheme for securing data in clouds. The cloud verifies the authenticity of the user without knowing the user's identity before storing information.	decentralized and robust	cloud knows the access policy for each record stored in the cloud
3.	Toward Secure and Dependable Storage Services in Cloud Computing	IEEE, 2012	Allows users to audit the cloud storage with very lightweight communication and computation cost and achieves fast data error localization. It secures dynamic operations on outsourced data, including block modification, deletion, and append.	highly efficient and resilient against Byzantine failure	rely on erasure-correcting code
4.	Identity Based Proxy Re-Encryption Scheme (IBPRE+) for Secure Cloud Data Sharing	INCoS, 2016	Data owner can control sharing capability in a flexible way by using random numbers used in the encryption process.	appropriately adapted to some applications for content sharing	Efficiency can be increased
5.	An Identity-Based Security Scheme for a Big Data Driven Cloud Computing Framework in Smart Grid	IEEE, 2015	proposed a big data driven, cloud based ICT framework for smart grid	perform efficiently with security guarantee	Few security systems are studied

III. PROPOSE SYSTEM

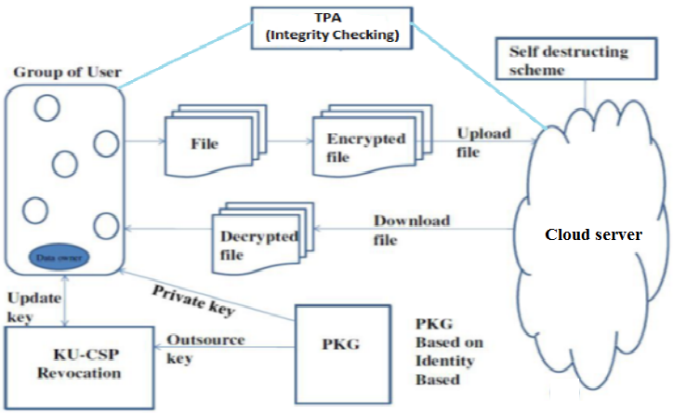

Fig 1. Propose System

Figure 1 shows architecture of the proposed system. Proposed system has TPA which takes place while checking integrity of the data stored on cloud. Also revocation system is used for providing as well as for revocation of permission given to the data users. In proposed system the data which is to be stored on the cloud is in encrypted format for providing security to the data. In case any user is enters or removes from the group entry to the data owner are updated accordingly.

IV. CONCLUSION

This survey gives the detail study of the topic of Cloud Data Security also presents the different methods developed by various researchers with their advantages and disadvantages and used methods. At last, proposed a technique to protect data present on cloud from unauthorized access.

REFERENCES

[1] J. Li, J. Li, X. Chen, C. Jia and W. Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing," in IEEE Transactions on Computers, vol. 64, no. 2, pp. 425-437, Feb. 2015.

[2] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak," Privacy Preserving Access Control with Authentication for Securing Data in Clouds" 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 556-563,2012

[3] Cong Wang, Qian Wang, Kui Ren, Ning Cao, Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Services Computing, vol.5, no. 2, pp. 220-232, Second 2012.

[4] X. A. Wang, F. Xhafa, Z. Zheng and J. Nie, "Identity Based Proxy Re-Encryption Scheme (IBPRE+) for Secure Cloud Data Sharing," 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS), Ostrawva, 2016, pp. 44-48.

[5] F. Ye, Y. Qian and R. Q. Hu, "An Identity-Based Security Scheme for a Big Data Driven Cloud Computing Framework in Smart Grid," 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, 2015, pp. 1-6.

[6] S. Qiu; J. Liu; Y. Shi; M. Li; W. Wang, "Identity-Based Private Matching over Outsourced Encrypted Datasets," in IEEE Transactions on Cloud Computing , vol.PP, no.99, pp.1-1

[7] D. Ramesh and R. Priya, "Multi-authority scheme based CP-ABE with attribute revocation for cloud data storage," 2016 International Conference on Microelectronics, Computing and Communications (MicroCom), Durgapur, 2016, pp. 1-4.