Secure Data Sharing In Cloud Storage Using Cryptosystem

Mr. Shailesh S. Randive[1], Mr. Safal U. Tammewar[2], Mr. Suraj J. Tike[3], Mr. Ramkrishna S. Vadali[4]
Department of Information Technology
[1, 2, 3] Pimpri Chinchwad College Of Engineering.
[4]Assistant Professor & Head of Systems and IT Support Department

Abstract-*Cloud technology is very constructive and useful in present new technological era, where a person uses the internet and the remote servers to give and maintain data as well as applications. It offers smart accessibility and dependability, disaster recovery and lowest price. Though it provides flexibility of data and application accessing, sharing of data and usage, there are many security concerns related to cloud, such as how to protect data and applications in cloud from hackers and intruders. Cloud storage should be able to store and share data securely, efficiently, and flexibly with others in cloud storage. Hence to achieve cloud data security, we are proposing a constant size cipher-text key based cryptosystem that uses attribute based aggregate key. In this cryptosystem, to access the data stored over cloud.*

An aggregate key is shared based on the attributes of a user. Data owner shares an aggregate key only to those users whose attributes gets matched with the security policy. Cloud computing is the practice of using a network of remote servers that are used to store, manage and process data, rather than a local server or a personal computer. Now a days, cloud computing is one of the dominant methods used for providing computing infrastructure for Internet services. Cloud computing offers computing and software services on demand by connecting to computing resources and access to IT managed services with an ease. This flexibility of cloud based services comes with risk of security and privacy of user's data. Client privacy is a tentative issue as all clients do not have the same demands regarding privacy.

Keywords- Searchable encryption, Data sharing, Data privacy, Cloud storage.

I. INTRODUCTION

In today's era the IT world is growing very fast and generating large amount of data to store that data cloud computing system is introduce. Cloud system can be used to enable data sharing and storing and this can proven abundant of benefits to the user. This system is used as an alternative to the traditional system. Cloud storage has emerged as a promising solution for providing ubiquitous, Scalable, Convenient and on-demand accesses to large amount of data shared over the internet It has various advantages to the user i.e. Scalability , Reliability, Manageability. Accessing the data over cloud are very easy but the problem occur at the time of data sharing and storing is security. Security is the most major issue which reduces the growth of cloud computing.

To overcome this problem the data owner should encrypt the whole data before storing on cloud.

Encryption is the technique in which data is encrypted i.e. plaint text is encrypted in cipher text. It is very efficient and easy technique to hide and secure the data from theft users.

In this paper we have concentrate on the security problem to increase the cloud security we are using encryption method we have studied various encryption algorithm and compare them and used the best one to overcome this main problem.

Cloud Computing:-

Cloud computing is the recent trend in IT, takes computing from desktop computers to the whole World Wide Web and yet, the user does not need to worry about maintenance and managing all the resources. User has to bear or paid only the cost of usage of service(s), which is called pay-as-you-use in cloud computing terms. With this cloud computing, a smart phone can become an interface to large data center.

Security of cloud:-

Security is the set of control-based technologies and policies. It is associated with cloud computing fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers.

The responsibility is shared, however. The provider must ensure that the infrastructure is secure and that their clients data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.

Cloud Data Security has following three aspects:-

Confidentiality:-

Confidentiality defines as the data is not accessible to the illegal user or unauthorized user. Only the authorized users can access the sensitive or important data while others, including CSP, should not gain any information of the data. Other than CSP, data owners expect to fully utilize cloud data services, e.g., data search, data computation, and data sharing.

Access Controllability:-

It defines that a data owner can perform the selective restriction of access to his data outsourced to cloud. Legal users can be authorized by the data owner to access the data, while others cannot access it without permissions.

Integrity:-

It defines that a data owner always expect the data should be stored on cloud is correctly. It means that the data should not change or modified by any other user. If any unwanted operations corrupt or delete the data, the owner should be able to detect the corruption or loss.

II. LITERATURE SERVEY

Monica G. Charate1, Dr. Savita R. Bhosale proposed a Cloud Computing Security Using Shamir Secret Sharing Algorithm from Single Cloud to Multi Cloud. This paper is carried out to design single and multi-cloud using secret key sharing algorithm which will result in deduction of the cost for the physical infrastructure, reducing the cost entry and execution as well as the response time for various associated applications. In this paper, I have referred the solution for performance of the Shamir secret sharing scheme, is used in a multi cloud environment [1].

Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee, and Wenjing Lou, design a Secure Deduplication with Efficient and Reliable Convergent Key Management. In this paper, I have referred Proof of ownership, Convergent encryption, Key management, Security of Convergent Encryption Key [2].

Dawn Xiaodong Song, David Wagner, Adrian Perrig[3], proposed a Practical Techniques for Searches on Encrypted Data. In this paper, I have referred Searching on Encrypted Data, Sequential Scan, Controlled Searching and Support for Hidden Searches.

Adi Shamir [4] is proposed a cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party and other user. Scheme assumes the existence of trusted key generation centers, whose purpose is to give each user a personalized smart card when he first joins the network. The information stored on card enables the user to sign and encrypt the messages he sends and to decrypt and verify the messages he receives in a totally independent way, regardless of the identity of the other party. Firstly issued cards do not have to be updated when new users join the network, and the various centers do not have to coordinate their activities or even to keep a user list. The centers can be closed after all the cards are issued, and the network can continue to function in a completely decentralized way for an indefinite period .

Dan Boneh et al. [5] also proposed a Hierarchical Identity Based Encryption (HIBE) system, where the cipher text consists of just three group elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth. Hierarchical IBE (HIBE) is a generalization of IBE that mirrors an organizational hierarchy. An identity at level k of the hierarchy tree can issue private keys to its descendant or low level identities, but cannot decrypt messages intended for other identities.

Luan Ibraimi et al. [6] proposed an efficient CP-ABEscheme which extends the basic CP-ABE scheme. This scheme uses Shamir's (k; t) threshold secret sharing technique. The access tree is an n-ary tree represented by ^ and V Boolean operators.

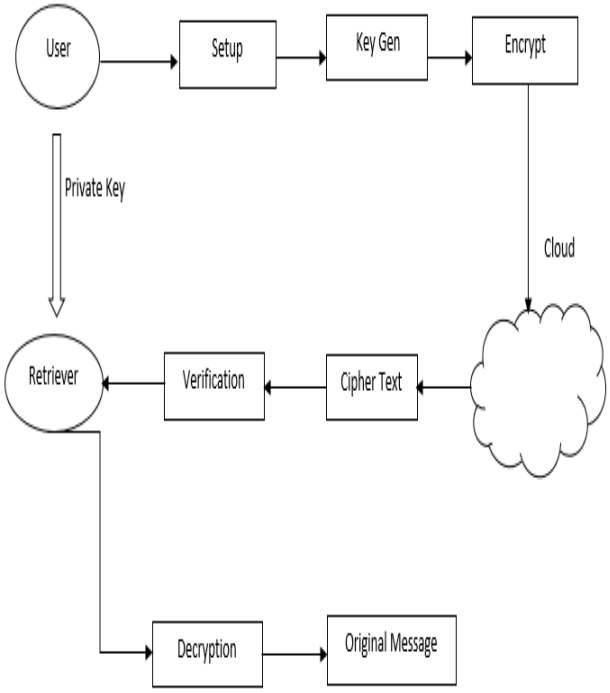
Kan Yang and Xiaohua Jia [7] Come up with an access control framework for multi-authority systems and proposed an efficient and secure multi-authority access control scheme for cloud storage. An efficient multi-authority CP-ABE scheme does not require a global authority and can support any LSSS access structure.

S. Ruj et al. [8] proposed a DACC (Distributed Access Control in Clouds) scheme for data storage and access in clouds. This scheme avoids storing multiple encrypted copies of same data. Cloud stores encrypted data (without being able to decrypt them) for secure data storage. The main feature of this scheme is addition of key distribution centers (KDCs). In DACC one or more KDCs distribute keys to data owners and users. KDC may provide access to particular fields in all records. Thus, a single key replaces several separate keys from owners. Owners and users are assigned certain set of attributes. Owner encrypts the data with the key attributes it

has and stores them in the cloud. The users with matching set of attributes can retrieve the data from the cloud.

Prof. B. M. Kore[9] ,proposed a basic architecture of cloud data sharing and storing to secure this system they use key aggregate cryptosystem with the help of this owner can share only one aggregate key with user and it is more efficient and secured as compared to other.

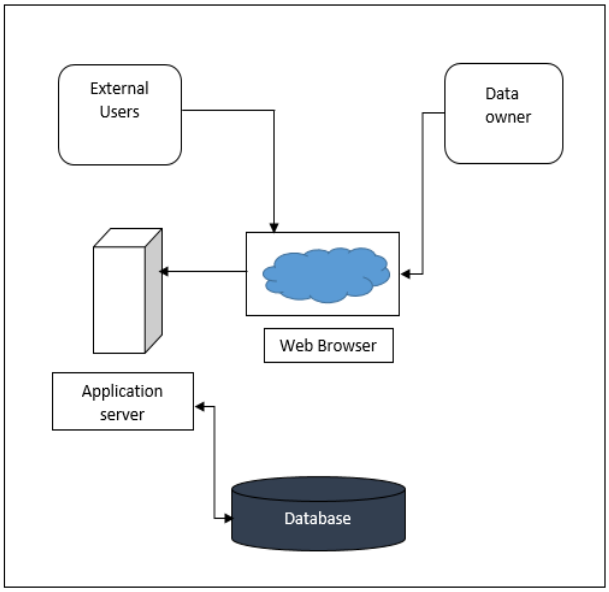
III. EXISTING SYSTEM



3.1 Existing System Architecture

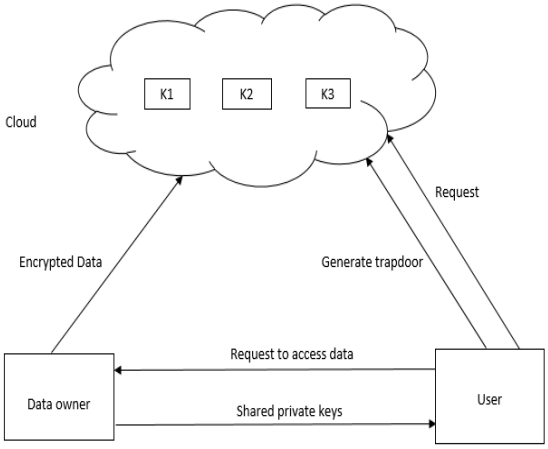
In this existing system[9] data owners store the data in encrypted format over cloud with the help of key generation algorithm. Plain text is converted into cipher text with the help of public keys generated by the algorithm. At the client side this encrypted data is decrypt with the help of private keys. This private key is shared by data owner when user wants to retrieve or access the data from cloud at that time the data owner checks the authentication of user and sends or shared to the retriever. Retriever takes the keys and decrypt the file and obtain the data in original format. But this system has one problem i.e. in this system user searchable method is not present. For ex:-If one user wants to retrieve the data over cloud but on cloud various file are stored but user wants to search a specific file that time it is not able search a specific file in this system this is the most specific problem in this system. This drawback of system is covered in our proposed architecture with the help of trapdoor key.

IV. PROPOSED SYSTEM



4.1 Basic Architecture

A high level proposed architecture of the system is as shown in Figure 4.1. All the various components and their communication with each other are clearly shown here. External users or data owners are those who have authorization to login to the website to store and manage their data. They communicate with the web browser to move data on to the cloud. The web browser connects with the application server which is responsible for efficient execution of programs, scripts that support this application. This will execute the homomorphic algorithms needed to secure the user's data. Data is moved through the application server to the database. Also, whenever a user requests for a file, the database is queried appropriately to extract the data and display the same on the website via the application server.
It has basic overall structure of our work now our original proposed architecture are as follows:-



4.2 Proposed system Architecture

The drawback of an existing system we will recover with the help of trapdoor generation. Trapdoor is a key which is used by the user for searching a keyword over any number of shared files on cloud.

A user or client can perform a keyword search operation over the files stored on cloud by using a trapdoor. In this proposed architecture the user only needs to submit single aggregate trapdoor (instead of group of trapdoors) to the cloud. But with the help of trapdoor key user can only search a specific file over cloud. If a user finds a specific file over cloud, at that time he will request a data owner to access the data store on cloud. When a data owner receives a request to access data stored over cloud it sends a private key to the user. Private key is shared to the user is basis on the attributes that consider by data owner after matching the attributes or authentication of user after recognizing valid user data owner shared the private key to that user. After getting the private key from data owner he will request to access the file over cloud. In response to the request, cloud sends an encrypted data to user. At user side he will decrypt the data with the help of private keys shared by data owner this system or architecture will achieve maximum data security over cloud.

V. CONCLUSION

In this paper, we had understood a solution to achieving secure data sharing in the cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information-theoretically secure against the Cloud provider and other malicious users and also implement searchable method to saving the searching time of file over cloud. It will improves the efficiency of system with respect to time.

REFERENCES

[1] Monica G. Charate1, Dr. Savita R. Bhosale," Cloud Computing Security Using Shamir's Secret Sharing Algorithm From Single Cloud To MultiCloud", Volume No 03, Special Issue No. 01, April 2015.

[2] J.Li, X.F. Chen, M.Q. Li, J.W. Li, P. Lee, Wenjing Lou."Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Transactions on Parallel and Distributed Systems, 25(6): 1615-1625, 2014.

[3] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp.44C55, 2000.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology: Conf. of CRYPTO 84, LNCS 196, pp: 47-53, 1984.

[5] D. Boneh, X. Boyen and E.-J. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext", EUROCRYPT '05: Prof. Advances in Cryptology, R. Cramer, ed., vol.3494, pp: 440-456, 2005.

[6] L. Ibraimi, Q. Tang, P. Hartel and Q. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes", Information Security Practice and Experience: 5th Inter-national Conf.(ISPEC 2009),LNCS5451, pp:1-12, 2009.

[7] Kan Yang, Xiaohua Jia, "Attributed-based access control for multiauthority systems in cloud storage", in Proceedings of IEEE 32nd International Conference on Distributed Computing Systems. IEEE, 2012, pp. 536–545.

[8] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds", in Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2011, pp. 91–98.

[9] Prof. B. M. Kore, Archana Jadhav, Prof. V. V. Pottigar "A Literature Survey on Secure Data Sharing in Cloud Storage with Key Aggregate Cryptosystem".in proceedings of the (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1511-1513.