Secure Data Transfer in Cloud Computing

Varun Srivastava[1], Rajat Srivastava[2], Mohd Salman Khan[3]
[1,2,3] *Student, SRM Institute of Science & Technology*

***Abstract*- Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security. When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a recent Cloud Security Alliance report, insider attacks are the sixth biggest threat in cloud computing. Therefore, cloud service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data centre. Additionally, data centers must be frequently monitored for suspicious activity.**

***Index Terms*- AES Encryption, Cloud Computing, Key Generation, Virtual Machines.**

I.INTRODUCTION

The proposal is to create a system that can allow a more secure and accurate sharing of data within a network on the cloud. The model will carry out encryption and decryption of the data every time the entitled user wants to access the data. This will be done with the help of a unique 16-digit key generated every time by the admin and shared only with the individual who tends to view the data. The system will have the portal to for admin, users and groups to upload and download data shared within the network but with an added level of security in the model so that the confidentiality of data can be sustained. There will also be a provision to mark the users as un-trusted and hence the data will not be accessible to the user even though he will be in the same group as others.

Fig. 1: Cloud computing advantages

The ongoing financial crisis and the increasing computational and storage needs have imposed significant changes to modern IT infrastructures. IT cost reduction is achieved by offloading data and computations to cloud computing. Cloud services vary from data storage and processing to software provision, addressing requirements for high availability and on-demand, commitment-free provision of services. Even though this economic model has found versatile ground attracting a lot of investments, many people and companies are reluctant to use cloud services because of several security, privacy, and trust issues that have emerged.

II. COMPUTATION OF ENCRYPTED DATA

Data encryption in the cloud is the process of transforming or encoding data before it's moved to cloud storage. Typically cloud service providers offer encryption services — ranging from an encrypted connection to limited encryption of sensitive data — and provide encryption keys to decrypt the data as needed. .Keeping information secure in the cloud should be your top priority. Just taking a few preventative measures around data encryption can tighten security for your most sensitive information. Follow these encryption tips to lock down your information in the cloud. Cloud cryptography is another way to secure your cloud computing architecture. Cloud computing service providers like Azure employ cryptography to offer a layer of information security at a system level and enables secure access to whoever needs shared cloud services. This layer of encryption is based on the Quantum Direct Key system, which is an advanced system of symmetric encryption keys. Users receive a public and private key pair with a specific ID. Cryptographic cloud computing can also minimize network congestion. Although cloud services providers offer redundancy and instant backups, you should always backup your most important data

locally — whether on a secured server or laptop. If your cloud-saved data gets lost or corrupted, you can rely on locally backed-up versions.

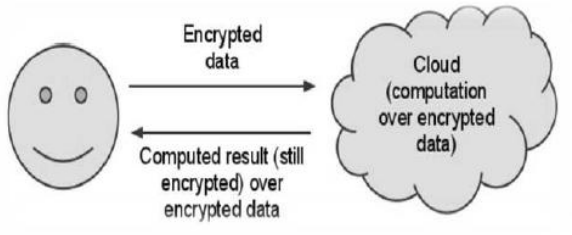

Fig. 2 Computing over encrypted data in Cloud.

III. EXISTING MODEL v/s PROPOSED MODEL

Several security schemes for data sharing on un-trusted servers have been proposed. In these approaches, data owners store the encrypted data files in un-trusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. The disadvantages associated with this system are the following:

- The file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead.
- The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.
- The single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others.
- The single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data.

Anti-collusion information sharing scheme for dynamic companies within the cloud, the customers can securely obtain their private keys from team manager certificates Authorities and secure communication channels. Also, our scheme is equipped to help dynamic corporations efficiently, when a brand new user joins within the workforce or a consumer is revoked from the group, the confidential keys of the opposite customers do not have to be recomputed and updated. Moreover, our scheme can reap at ease user revocation; the revoked customers cannot be equipped to get the usual data documents as soon as they are revoked even though they conspire with the un-trusted cloud.

The advantages associated with the proposed system are as follows:

- We propose a secure Anti-collusion information sharing scheme for dynamic company data sharing scheme. It implies that any user in the group can securely share data with others by the un-trusted cloud.
- We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

IV. MATHEMATICAL BACKGROUND

If p is a prime number and a is co prime with p, Fermat little theorem consists of $a^{p-1} = 1 \bmod p$. Thus, we will have for every integer k $a^{k(p-1)+1} = a \bmod p$ and generally we have $a^b = a^{b \bmod (p-1)} \bmod p$.

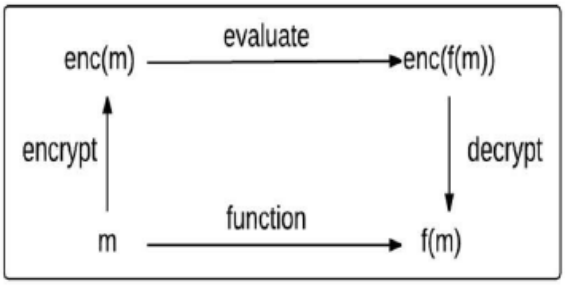

Fig. 3 Homomorphic Encryption Diagram

V. OUR FULLY HOMOMORPHIC ENCRYPTION SCHEME

Our proposed fully homomorphic encryption scheme is probabilistic, noise-free and consists of four main algorithms:

1. Key Generation
2. Encryption
3. Decryption

Cryptographic cloud computing can also minimize network congestion. Although cloud services providers offer redundancy and instant backups, you should always backup your most important data

locally — whether on a secured server or laptop. If your cloud-saved data gets lost or corrupted, you can rely on locally backed-up versions. You can also choose to back up your data on a separate cloud. For instance, you might use Drop box exclusively but backup important files on Google Drive and some situations, data security depends on your online activity. If you access cloud data on a public computer or over an insecure connection, your data may be vulnerable. Do not allow any computer to cache passwords and logins. Make sure to log out from every site or account once you're done accessing data. Avoid unsecured Wi-Fi hotspots whenever possible. These connections leave your information vulnerable to hackers.

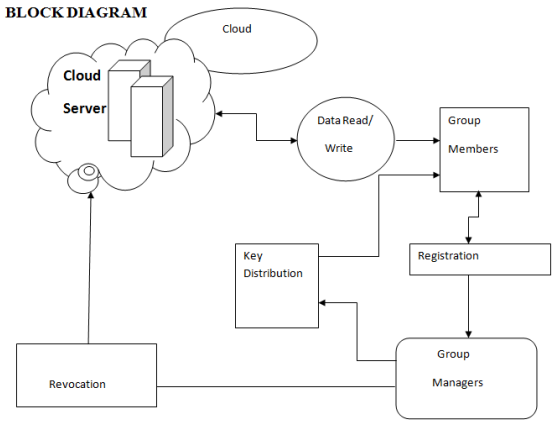

Fig.4 Block Diagram of proposed System

VII. CONCLUSION

In this paper, we presented a new fully homomorphic Encryption scheme, our proposition is an improvement of Kumar et Al's cryptosystem. Our scheme is a symmetric algorithm randomizes messages into integers. It is a noise free and probabilistic FHE scheme from integers, it can be used for data security in cloud computing. The security of this algorithm is based on the problem of factorization of big numbers. Our outlook in the future work is to apply this algorithm to data security in a cloud context.

ACKNOWLEDGMENT

This research was supported/partially supported by SRM Institute of Science & Technology. We are thankful to our faculties Mr. R Jayaraj and Ms. G. Aswini who provided expertise that greatly assisted the research, although they may not agree with all of the interpretations provided in this paper. We are also grateful to our HOD Dr. T.K. Thivakaran for assistance with unique resources and guide Ms. Chandralekha T. who moderated this paper and in that line improved the manuscript significantly.

REFERENCES

[1] R. Rivest, L. Adleman and M. Dertouzos, "On Data Banks and Privacy Homorphisms," *In Foundataions of Secure Computation, Academic Press*, pp. 169-179, 1978.

[2] C. Gentry, "A fully homomorphic encryption scheme, "https://crypto.stanford.edu/craig/craig-thesis.pdf, September 2009.