2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)

Encryption Schemes of Cloud Computing: A Review

Saif Ali Khan
Department of Computer Engineering
National Institue of Technology Kurukshetra
Haryana, India
akgsaif@gmail.com

Dr. R.K Aggarwal
Department of Computer Engineering
National Institue of Technology Kurukshetra
Haryana, India
rka15969@gmail.com

Shashidhar Kulkarni
Karnataka, India
shashi2713@gmail.com

***Abstract*—A scenario in which the network can be accessed on- demand so that the resources available within it can be used in convenient manner is known as cloud computing. It is also possible for the user to store the data and have access to various types of services. Depending upon the usage of resources, the users have to pay. Several data encryption techniques have been proposed by researchers to ensure the security of important data available in the cloud scenarios. This study focuses on reviewing full disk encryption (FDE) as well as the fully homomorphic encryption (FHE) techniques. It is seen through the studied evaluations that the efficiency of FDE is less as compared to FHE. However, the reliability of FHE is reduced due to the key management and sharing issues faced in this technique.**

Keywords— Cloud computing, fully homomorphic encryption,fully disk encryption

I. INTRODUCTION

A scenario in which the resources can be accessed from a shared pool as per the demand and convenience of user is known as cloud computing. The management required for these resources is very less. There are several clients and organizations which store their private data within the clouds. This data can be modified or retrieved by the users as per their requirements [1]. The "pay per user" method is used here in order to provide services to the cloud users. This means that the users only need to pay for the services they access for a certain period of time. Cloud computing is basically a technology through which the wide range of applications can be accessed by users that have different topologies. The specialization for each topology is different. It is possible to have access to any user's account without its knowledge through the cloud service providers provided in this technology. However, huge data might be lost here which cannot be handled by the user. Several security problems are being faced within cloud computing and depending upon certain criterions these problems can be categorized. In order to provide security to the information available within clouds, different types of data security approaches have been developed over the years by researchers. The researchers have been discussing over the best possible solutions to be provided within certain scenarios [2]. The encryption technique in which the corresponding algebraic function is used to handle plain and cipher texts is known as homomorphic encryption. The algebraic operation which is applied on both of these texts is connected even when the texts are not connected. The technique through which the data is encrypted in such a manner that a query- specific token is used for querying it is known as structured encryption. The knowledge from secret key is used in order to generate this query-specific token [3]. Also, the information related to query or data is not revealed by the query process. Therefore, the major concern here is the representation of 'f' function which can be different for various schemes.

There are, several security and maintenance related challenges being faced by the technologies today which cannot be resolved by applying the FDE and FHE. This can be understood more clearly by highlighting the differences that exist amongst them such as:

Key management and trust: The keys might be available within the cloud platform or near to the physical drive in case of FDE. The key management process does not include the cloud application user. Even though the data of user is encrypted on the physical disk, any layer present below it can access it at any time. Thus, the access of data to unauthorized users of online attacks is not prevented by FDE approach. The data cannot be learnt or leaked easily through the untrusted applications when FHE is applied. The FHE encryption keys are owned and managed by the users. However, without seeing the data actually, computations can be performed on encrypted forms by the applications [4].

Sharing: For the cloud applications, another important feature to be considered is collaboration. To make it possible for the owner to share one or more data objects selectively with other users, it is important to include fine- grained access control. Since the access control granularity and key granularity are not lined up, it is important for a user to completely rely on the cloud provider for providing the right access control in the presence of FDE. There is no exact way defined for providing access control yet, since the encryption keys are managed by the user or third party cloud provider in case of FHE. The key management can be defined on a per- data object granularity basis such that the fine-grained encryption-based access control can be provided. It is important for the objects to be encrypted

978-1-5386-9533-3/19/$31.00 ©2019 IEEE

within similar public key for supporting homomorphic operations within the multiple encrypted objects [5].

Performance: The symmetric encryption of FDE can be performed at the complete bandwidth of disk due to which the system slows down its processing. Before being capable enough to deploy at a scale, it is important to enhance the performance of FHE.

Ease of development: There is no impact of FDE on the development of application since it is hidden behind an abstraction of physical disk. There might be the possibility of relative automaticity for FHE which states that on an abstraction of program FHE works as a circuit which is then transformed.

Maintenance: It is impossible to prevent a system from all the errors or bugs. The most important goal of clouds is availability due to which it is important to ensure that the systems are debugged. There is a need for an individual to step in and manually check the reasons when a system failure occurs randomly. There is a need to detect an unusual activity or understand the actual problem in order to determine the nature of problem. In case of FHE, this however, might be difficult [6]. It would be difficult to perform debugging if the application writer cannot inspect the application state in a meaningful manner.

II. LITERATURE SURVEY

Bhavna Makhija et.al, presented a study related to the various data security and privacy techniques applied in cloud applications. Issues such as lack in integrity of data, lack of support for dynamic data operations, and lack of availability of high resource and computation cost were identified in different techniques. Further, the TPA was applied in order to provide a clear view of all the data security techniques and methods which previously exist [7]. Higher efficiency can be provided by applying the private audit ability. However, the ability of challenging the cloud server to ensure correctness of data storage is provided through public audit ability.

Dawn Song et.al, presented that the per-application development effort using which the data can be protected is minimized by the proposed architecture called DPaaS [8]. For balancing the huge development and easy maintenance along with the verification of user-side, the key management and access control process are moved to the middle tier known as computing platform. The privacy at the required granularity is not the concern of FDE even though the performance and ease of development are provided by it. However, the data visibility is removed completely from both server and application developer by the FHE.

Deyan Chen et.al, provided a study related to the various issues being faced by the data when it crosses the data life cycle in terms of maintaining its security and privacy [9]. The future research of the data security and privacy protection problems being faced in cloud is also presented here. There is still the need to solve various problems of cloud computing even though it provides several benefits. There is a revenue estimation conducted for cloud computing which shows that its demand is increasing with the passage of time. The threats from hackers are increasing however, due to the presence of existing vulnerabilities within the cloud model.

Deepan chakaravarthi et.al, proposed a distributed approach through which the data stored in clouds can be secured. It is ensured here that the unauthorized access of data is not performed here. The homomorphism token is applied along with distributed verification of the erased coded data to provide security [10]. The data is stored, recognized at the cloud server and few of its tasks are executed by applying the proposed technique. This paper also ensures the collision attacks are avoided such that the unauthorized users do not make modifications on the server. The various problems being faced on the security of data within cloud data storage are studied here so that proper measures can be taken.

Simarjeet Kaur et.al, studied the different data encryption techniques that have been developed by researchers over the past few years [11]. The critically important information is ensured to be protected here at all times with the application of such secure techniques within the cloud applications.

Sanjoli Singla et.al, proposed an architecture using which the file at user's end can be encrypted and decrypted such that the security of data during transmission can be exchanged [12]. The Rijndael Encryption Algorithm is used along with EAP-CHAP within this paper. Cloud computing security is the major concern of clients today due to which adopting the cloud computing services to provide privacy protection and data security is necessary. Therefore, the client side security is ensured in this paper. The data can only be accessed by the authorized user by the proposed system. The decryption of data is not possible by the intruder even though he gets access to the data. Therefore, by applying the proposed technique better security algorithm is provided through encryption.

Mark D. Ryan et.al, presented various problems related to the security of cloud computing. The cloud computing security is separated from other computing security techniques since the data shared with CSP is recognized as

core scientific issue [13]. In order to protect the data from cloud infrastructure provider different techniques have been utilized by researchers. Further, the FHE techniques are applied within the cloud applications to highlight the few difficulties. A technique through which the SAAS application is run with huge confidentiality from the service provider is proposed here. The manner through which the cloud-based data can be protected using trusted hardware is explored here.

Authors' Names	Year	Description	Outcome
Bhavna Makhija	2013	A study related to the various data security and privacy techniques applied in cloud applications is presented.	The ability of challenging the cloud server to ensure correctness of data storage is provided through public audit ability.
Dawn Song	2012	The per-application development effort using which the data can be protected is minimized by the proposed architecture called DPaaS.	The data visibility is removed completely from both server and application developer by the FHE.
Deyan Chen	2012	A study related to the various issues being faced by the data when it crosses the data life cycle is provided in terms of maintaining its security and privacy	There is a revenue estimation conducted for cloud computing which shows that its demand is increasing with the passage of time.
Deepan chakaravarthi	2012	A distributed approach is proposed through which the data stored in clouds can be secured.	The various problems being faced on the security of data within cloud data storage are studied here so that proper measures can be taken.
Simarjeet Kaur	2012	The different data encryption techniques are studied here that have been developed by researchers over the past few years.	The critically important information is ensured to be protected here at all times with the application of such secure techniques within the cloud applications.
Sanjoli Singla	2013	Architecture is proposed using which the file at user's end can be encrypted and decrypted such that the security of data during transmission can be exchanged. The Rijndael Encryption Algorithm is used along with EAP-CHAP within this paper.	The decryption of data is not possible by the intruder even though he gets access to the data. Therefore, by applying the proposed technique better security algorithm is provided through encryption.
Mark D. Ryan	2013	A technique through which the SAAS application is run with huge confidentiality from the service provider is proposed here.	The manner through which the cloud-based data can be protected using trusted hardware is explored here.

III. CONCLUSION

For ensuring that the privacy of user is maintained within cloud systems, the major concern is to include security techniques. The cloud security is provided by proposing different schemes. In order to ensure the data privacy, the most popularly applied technique is the fully homomorphic encryption technique. The different FHE techniques are studied and analyzed in this review paper.

REFERENCES

[1] Zvika Brakerski, Vinod Vaikuntanathan "Effcient Fully Homomorphic Encryption "LWE, 2010

[2] Sigrun Goluch, "The development of homomorphic cryptography" Vienna University of Technology, 2009

[3] H. Anandakumar and K. Umamaheswari, "Supervised machine learning techniques in cognitive radio networks during cooperative spectrum handovers," Cluster Computing, vol. 20, no. 2, pp. 1505–1515, Mar. 2017.

[4] Security Considerations" Cyber Security Operations Centre, vol. no. 2, Issue 5, 2011

[5] Ponemon Institute "Encryption in the Cloud" Thales e-Security, 2009

[6] Anthony T. Velte Toby J. Velte, Ph.D. Robert Elsenpeter, 2010 "Cloud Computing: A Practical Approach", 2011

[7] Fraunhofer Verlag "These curity Of Cloud Storage Services" Fraunhofer Institute for Secure information Technology, 2012

[8] Bhavna Makhija , VinitKumar Gupta "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, 2013

[9] Dawn Song, Elaine Shi, "Cloud Data Protection for the Masses" IEEE Computer Society, 2012

[10] Dawn Song, Elaine Shi, "Cloud Data Protection for the Masses" IEEE Computer Society, 2012

[11] Deepanchakaravarthi Purushothaman and Dr.Sunitha Abburu "An Approach for Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, 2012
[12] Simarjeet Kaur "Cryptography and Encryption In Cloud Computing" VSRD-IJCSIT, Vol. 2 (3), 2012, 242- 249, 2012
[13] Sanjoli Singla, Jasmeet Singh "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013
[14] Mark D. Ryan, "Cloud Computing for Enterprise Architectures: Concepts, Principles and Approaches", 2013, edition 4th.