Analysis of Various Cloud Data Encryption Techniques

[1]Payal Thakur, [2]Kusum Sharma, [3]Amandeep Kaur

[1]Computer Science Department,
[1]Sri Sukhmani Institute of Engineering And Technology, India

Abstract : Cloud computing is the environment which provides on-demand and convenient access of the network to computing resources like storage, servers, applications, networks and other services which can be released in minimum efficient way. In this user can store their data and use different services and pay according to those services. The main factor is security that is how we can secure our data while storing into the cloud. There are two most popular techniques for cloud data encryption. These techniques are full disk encryption and fully homomorphic encryption. In this review paper, both the techniques are reviewed and analyzed.

IndexTerms **- Cloud computing; fully homomorphic encryption; fully disk encryption**

I. INTRODUCTION

Cloud computing is an environment which provide convenient and on-demand network access to a shared pool of computing resources like servers, networks, applications, storage and services that can be rapidly released with minimum management in efficient way. Cloud is a centralized database where many clients /organizations store their data and possibly modify data and retrieve data [7]. Cloud is a model where services are provided by CSP (Cloud Service Provider) on pay per user base to user. Means here client has to pay only for what he is using or being served. Cloud computing is a technique which provides a huge range of applications under different kind of topologies and every topology derives some new specialized threats. Even cloud service providers like Dropbox could accidentally allow anyone to access any user's account without user's knowledge. This would potentially lead to massive data breaches which are beyond user's control [4].
To fortify the security for cloud computing most organizations adopt standard enterprise security solutions like firewall, IPS and anti-virus. Since users can now access cloud services from anywhere around the world some organizations may implement strong user authentication and access control solutions as a defense against identity frauds. Unfortunately, these solutions do not actually protect the user's data in the cloud.

The cloud computing model NIST defined has three service models and four deployment models. The three service models are:

- Cloud Software as a service
- Cloud Platform as a Service (PaaS) and Cloud
- Infrastructure as a Service (IaaS**)**

The three deployment models are:

- Private cloud,
- Public cloud
- Hybrid

A. Security Issues Associated with the Cloud

Cloud computing has various security issues associated with it and these issues can be grouped into any number of dimensions like data segregation, data location, privileged user access, regulatory compliance, investigative support, recovery and long-term viability. Cloud Security Alliance (CSA) is trying to gather solutions from non-profits organizations and individual providers by making them enter into the discussion about the current and future best practices for information assurance in the cloud [9]. Thirteen domains of concerns on cloud computing security have been identified by CSA.

B. Fully Homomorphic Encryption

Homomorphic encryption refers to the type of encryption where plain texts and cipher texts both are treated with a correspondent algebraic function. The plain text and cipher text may also be not connected but algebraic operation works on both of them. The structured encryption scheme encrypts the data in such a way that it can be queried through the use of a query-specific token that can only be generated with knowledge of the secret key [10]. In addition the query process reveals no useful information about either the query or the data. The representation of the function f is an important issue. Since the representation can vary between schemes, we leave this issue outside of this syntactic dentition.

C. Difference between FDE versus FHE

Fully Disk Encryption and Fully Homomorphic Encryption are equated in the cloud computing condition and the results disclose how these encryption techniques fall short of addressing the above-mentioned security and maintenance challenges simultaneously.

- *Key management and trust*: With FDE, the keys may be located in with the cloud platform, generally on or close to the physical drive: the cloud application user isn't involved in key management. While user data is encrypted on the physical disk, it is always accessible clearly to any layer above it. Therefore, FDE doesn't avoid online attacks from leaking the data to an unauthorized party, which is common in the cloud setting than physical attacks [5]. In the FHE, untrusted applications cannot easily acquire or leak data. Users typically own and manage FHE encryption keys, while applications compute on encrypted forms of user data without actually "seeing" the data [11].

- *Sharing*: Collaboration is often cited as a "killer feature" for cloud applications. Fine-grained access control is necessary to let a data owner selectively share one or more data objects with other users. In the FDE, the users should have full faith in the cloud provider to impose correct access control because the key granularity (the whole disk) doesn't line up with access control granularity (a single data unit). In FHE, the user or third-party cloud provider employed by the user manages the encryption keys so the best way of providing access control isn't clear yet. In order to provide the fine-grained encryption-based access control, we might need to define key management on a per data object granularity basis or over collections of data objects. However, to support homomorphic operations across multiple encrypted objects, those objects must still be encrypted under the same public key [10].

- *Performance*: When FDE is applied in disk firmware, its symmetric encryption can run at the disk's full bandwidth, successfully avoiding a slowdown. Although researchers have made important advances in improving FHE's performance since Gentry's original proposal, it has a long way to go before becoming efficient enough to deploy at scale.

- *Ease of development*: Because FDE is hidden behind an abstraction of the physical disk, it typically has no impact on application development. In theory, FHE could also be relatively automatic: it works on an abstraction of the program as a circuit and transforms that circuit. In exercise, executing this translation for random programs—especially when marshaling data—can be quite complex. At a minimum, programming tools would need to evolve dramatically. FHE doesn't allow developers to input data-driven judgments into the development cycle. Specifically, application developers can't look at the data, making debugging, A/B testing, and application improvements more difficult [12].

- *Maintenance*: Bugs are unavoidable so the necessity to debug quickly is a top priority. Systems often fail for some unforeseen reason, requiring someone to step in and manually take action. Determining the nature of the problem might require detecting unusual activity or understanding exactly what went wrong, which isn't easy with FHE. If the application writer can't inspect application state meaningfully, debugging could be a real challenge [13].

II. REVIEW OF LITERATURE

Bhavna Makhija el al, They discussed their methods of data security and privacy etc. In which they found the lack in supporting dynamic data operations, some were lacking in ensuring data integrity, while some were lacking by high resource and computation cost. They also defined overall evidence of all existing techniques for cloud data security and methods proposed for ensuring data authentication using TPA (Third Party Auditor). Third Party Auditor is kind of inspector [1]. There are two categories: private audit ability and public audit ability. Private audit ability can attain higher scheme efficiency but the public audit ability allows anyone, not only just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information.

Dawn Song el al**,** explained that design intensely decreases the per-application development effort needed to provide data protection while still allowing rapid development and maintenance [2]. Two techniques FDE (fully disk encryption) and FHE (fully homomorphic encryption) are discussed. They compare both technique on the basis of key management, sharing, ease of development, maintenance, aggregation and performance. The DPaaS approach moves key management and access control to a middle tier computing platform to balance rapid development and easy maintenance with user-side verifiability. Though FDE provides ease of development and excellent performance, it does slight to protect privacy at the required granularity. FHE on the other hand, pushes the privacy envelope in the other direction by removing data visibility entirely from both the server and application developer.

Deyan Chen el al, they worked to analyse privacy protection and data security issues associated with cloud computing across all stages of data life cycle [3] is provided in brief in this paper. Finally this paper explained about future research work about data security and privacy protection issues in cloud. Although cloud computing has many advantages, there are still many actual problems that need to be solved. According to a Gartner survey about cloud computing revenues market size for Public and Hybrid cloud is $59 billion and it will reach USD 149B by 2014 with a compound annual growth rate of 20. The income approximation infers that cloud computing is a promising industry. But from another perspective, existing vulnerabilities in the cloud model will increase the threats from hackers.

Deepan Chakaravarthi el al, It is described in this paper how to prevent data access from unauthorized access so they proposed a distributed technique to provide security of the data in cloud. This could be achieved by using homomorphism token with distributed verification of erasure coded data [4]. The proposed technique perfectly stores the data and identifies at the cloud server and also execute some of the tasks such as data deleting, inserting and data updating. In this paper process to avoid collusion attacks of server modification by unauthorized access is also given. The proposed techniques have been implemented

by them. This paper completely described the problems of data security in cloud data storage and also provided a way out to ensure user correctness.

Simarjeet Kaur el al, author explores various data encryption scheme like homomorphic encryption, searchable and structured encryption, Identity based encryption, signature-based encryption etc. [5]. These are emerging technique in cloud world security to provide day night full protection to critical data information.

Sanjoli Singla el al**,** author design architecture that can help to encrypt and decrypt the file at the user side which provide security to data at rest as well as while transferring [6] has been proposed. In this research paper they used the Rijndael Encryption Algorithm along with EAP-CHAP. The data security issues and privacy protection remain the primary inhibitor for adoption of cloud computing services from the client viewpoint. So in this we focused on client side security. In their proposed system only the authorized user can access the data. Even if some intruder (Unauthorized user) gets access of the data accidentally or intentionally he will not be able to decrypt it. Also it is proposed that encryption must be done by the user to provide better security algorithm.

Mark D. Ryan el al, author highlighted many issues in cloud computing security are described. As we know data are shared with the cloud service provider (CSP) is identified as the core scientific problem that separates cloud computing security from other topics in computing security. They did current research and test them in terms of running software-as-a-service (SAAS) example are considered as a survey. They used approaches to protect data from a cloud infrastructure provider. They describe some difficulties with using fully homomorphic encryption in cloud computing applications. They proposed a method in which in-browser key translation allows a software-as-a-service (SAAS) application to run with confidentiality from the service provider. They explore how trusted hardware can be used to protect cloud-based data.

III. CONCLUSION

In this paper we conclude that fully homomorphic encryption technique is more efficient than the full disk encryption. But the main problem that exists in fully homomorphic encryption is of key management and key sharing which reduces the reliability of the scheme. In this paper certain methods are being reviewed to enhance the security of fully homomorphic encryption technique.

REFERENCES

[1] 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*

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

[3] Deyan Chen, Hong Zhao "*Data Security and Privacy Protection Issues in Cloud Computing"* International Conference on Computer Science and Electronics Engineering,2012

[4] 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

[5] Simarjeet Kaur "*Cryptography and Encryption In Cloud Computing"* VSRD-IJCSIT, Vol. 2 (3), 2012, 242-249, 2012

[6] 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

[7] Mark D. Ryan, "Cloud Computing for Enterprise Architectures: Concepts, Principles and Approaches", 2013, edition 4th.

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

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

[10] Defence Signals Directorat "Cloud Computing Security Considerations" *Cyber Security Operations Centre*, vol. no. 2, Issue 5, 2011

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

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