Homomorphic Encryption Scheme Analysis of Cloud Computing

Pritpal kaur
Research scholar
Pritpalkaur516@gmail.com
Swami Vivekanand Institute of Engineering & technology
Banur

Mr. Prince
Assistance Professor
Pritpalkaur516@gmail.com
Swami Vivekanand Institute of Engineering & technology
Banur

Abstract - Cloud computing is the environment which provides on-demand & convenient access of the network to a computing resources like storage, servers, applications, networks and the other services which can be released minimum efficiency way. In this user can store their data and use different services and pay according to those services. The main factor is security that how we can store our data while storing into the cloud. In this thesis, we reviewed two most popular techniques for cloud data encryption. These techniques are full disk encryption and fully homomorphic encryption. In this work, we find that fully homomorphic encryption technique is more efficient than full disk encryption. But the main problem exists in fully homomorphic encryption is of key management and key sharing which reduces the reliability of the scheme.

Keywords - Cloud computing, fully homomophic, encryption

I. INTRODUCTION

Cloud computing is 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 efficient way. Cloud is a centralized database where many clients /organizations store their data and possibly modify data and retrieve data [1]. 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. 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. There are many security issues associated with cloud computing and they can be grouped into any number of dimensions. Data segregation, regulatory compliance, data location, Privileged user access, investigative support, recovery and long-term viability Cloud Security Alliance (CSA) is gathering solution non-profits and individuals providers to enter into discussion about the current and future best practices for information assurance in the cloud [2]. The CSA has identified thirteen domains of concerns on cloud computing security. Homomorphic encryption alludes to encryption where plain texts and cipher texts both are treat with an correspondent algebraic function. Now the plain text and cipher text might also be not connected but algebraic operation that works on both of them. Structured Encryption: A structured encryption scheme encrypts structured 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 [3]. 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.

A comparison of FDE and FHE in the cloud computing situation reveals how these encryption techniques fall short of addressing the aforementioned security and maintenance challenges simultaneously.

1. 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 in the clear to any layer above it. Consequently, FDE doesn't avoid online attacks from leaking the data to an unauthorized party, which is common in the cloud setting than physical attacks. With FHE, untrusted applications can't easily learn 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 [4].

2. 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. With FDE, users must fully trust the cloud provider to enforce correct access control because the key granularity (the whole disk) doesn't line up with access control granularity (a single data unit). With FHE, because the user or third-party cloud provider employed by the user manages the encryption keys, the best way of providing access control isn't clear yet. To offer 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 [5].

3. Performance: .When FDE is implemented 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.

4. 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 practice, however, performing this translation for arbitrary programs—especially when marshaling data—could 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 [6].

5. Maintenance: Bugs are inevitable. However, availability is a primary cloud goal, so the need 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.

II. LITERATURE REVIEW

Bhavna Makhija et.al, discussed their methods of data security and privacy etc. In which they found that lack in supporting dynamic data operations, some were lack in ensuring data integrity, while some were lacking by high resource and computation cost. They also described overall clue of all existing techniques for cloud data security and methods proposed for ensuring data authentication using TPA (Third Party Auditor). Third Party Auditor Third Party Auditor is kind of inspector [7]. There are two categories: private audit ability and public audit ability. Although private audit ability can achieve higher scheme efficiency, public audit ability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information.

Dawn Song et.al**,** in this paper author described that its architecture dramatically reduces the per-application development effort required to offer data protection while still allowing rapid development and maintenance [8]. There are two technique FDE (fully disk encryption) and FHE (fully homomorphic encryption) are discussed .They compare both technique on 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 the computing platform to balance rapid development and easy maintenance with user-side verifiability. Although FDE offers excellent performance and ease of development, it does little 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 et.al, the author work to analyze data security and privacy protection issues associated with cloud computing

across all stages of data life cycle [9] 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 revenue estimation implies 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 et.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 [10]. The proposed technique perfectly stores the data and identifies at the cloud server and also executes 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 et.al, author explores various data encryption scheme like homophormic encryption, searchable and structured encryption, Identity based encryption, signature based encryption etc [11]. These are emerging technique in cloud world security to provide day night full protection to critical data information.

Sanjoli Singla et.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 [12] has been proposed. In this research paper they used the Rijndael Encryption Algorithm along with EAP-CHAP. From the customer perspective cloud computing security concerns especially privacy protection and data security issues remain the primary inhibitor for adoption of cloud computing services. 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 et.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. Three current research and test them in terms of running software-as-a-service (SAAS) example are considered as a survey [13]. They used approaches to protecting 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.

Authors' Names	Year	Description	Outcome
Bhavna Makhija		Authors discussed their methods of data security and privacy etc. In which they found that lack in supporting dynamic data operations, some were lack in ensuring data integrity, while some were lacking by high resource and computation cost.	Although private audit ability can achieve higher scheme efficiency, public audit ability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information.
Dawn Song		in this paper author described that its architecture dramatically reduces the per-application development effort required to offer data protection while still allowing rapid development and	Although FDE offers excellent performance and ease of development, it does little to protect privacy at the required granularity.FHE on the other hand, pushes the privacy envelope in the other direction

		maintenance	by removing data visibility entirely from both the server and application developer.
Deyan Chen		The author work to analyze data security and privacy protection issues associated with cloud computing across all stages of data life cycle is provided in brief in this paper.	The revenue estimation implies 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		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 paper completely described the problems of data security in cloud data storage and also provided a way out to ensure user correctness.
Simarjeet Kaur		Author explores various data encryption scheme like homophormic encryption, searchable and structured encryption, Identity based encryption, signature based encryption etc.	These are emerging technique in cloud world security to provide day night full protection to critical data information.
Sanjoli Singla		In this research paper they used the Rijndael Encryption Algorithm along with EAP-CHAP.	Even if some intruder (Unauthorized user) gets access of the data accidentally or intentionally he will not be able to decrypt it.
Mark D. Ryan		Author highlighted many issues in cloud computing security are described. Three current research and test them in terms of running software-as-a-service (SAAS) example are considered as a survey.	They explore how trusted hardware can be used to protect cloud-based data.

III. CONCLUSION

The security is the major concern in the cloud environment to ensure user privacy. The various schemes are proposed so far for the cloud security. The fully homomorphic encryption scheme is the much popular scheme to ensure data privacy. In this review paper, various schemes related to fully homomorphic encryption is reviewed and analyzed.

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

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

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

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

[7] 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

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

[9] Deyan Chen, Hong Zhao " Data Security and Privacy Protection Issues in Cloud Computing" International

Conference on Computer Science and Electronics Engineering,2012

[10] 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

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

[12] 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

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