Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 6, June 2019, pg.177 – 182

Analysis of Various Encryption Schemes of Cloud Computing

Satmeer Kaur
Student
Satmeeraulakh@yahoo.co.in
GGS Collage
Kharar, Mohali

Inderdeep Kaur
Assistant Professor
Kaur.inderdeep@gmail.com
GGS Collage
Kharar, Mohali

ABSTRACT: The cloud computing is the decentralized network is much vulnerable to certain security attacks. The various security techniques are proposed by researchers to improve security of the network. The fully homomorphic and fully disk encryption techniques are proposed by the researchers to increase security of the network. It is analyzed that fully homomorphic encryption is the efficient technique than the fully disk encryption. The various improvement which are proposed in the fully homomorphic encryption is reviewed in this paper in terms of certain parameters
Keywords: Fully Disk Encryption, Fully homomorphic encryption, cloud security

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. 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 [2].

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 [4]. 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.

1.1. Difference between FDE versus FHE

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 [5]. 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.
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 [6].

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 [7]. 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.
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 [8].

II. LITERATURE SURVEY

Zainab Hikmat Mahmood et.al (2018) presented an overview of security issues in cloud computing and utilization of the fully homomorphic encryption technique has drawbacks of large key size and low calculation efficiency, and it is not practical for the secure cloud computing [9]. We build up a hybrid homomorphic encryption scheme based on the GM encryption algorithm which is additively (single bit) homomorphic, and RSA algorithm which is multiplicative homomorphic. The hybridization of homomorphic encryption schemes seems to be an effective way to defeat their limitations and to benefit from their resistance against the confidentiality attacks. This hybridization of homomorphic encryption algorithm lead to increase the speed (2.9) times, reduce the computation time to 66% percentage from previous one, enhanced confidentiality of the data that is stored in the cloud by enhancing security (two layer of encryption methods used) . Since hybrid encryption is utilized high security and authentication is provided.

Xidan Song, et.al (2017) proposed a hybrid cloud computing scheme based on the Paillier algorithm which is additively homomorphic, and RSA encryption algorithm which is multiplicative homomorphic. Customer's calculation requests can be described as the combination of simple add and multiplicative operation and the operands [10]. An Encryption Decryption Machine which running in the private cloud processes the encryption according to the type of the operation and upload the cipher texts to the public cloud. The public cloud

process calculation without knowing the exact data. Then we run simulations and analyze the results, and the results show that the scheme is practical and efficient.

Peidong Sha, et.al (2016) designed a encryption system which firstly discriminates whether the values of the public key and private key generated during the encryption process contain prime number [11]. Then it combines with the Pascal's triangle theorem and RSA algorithm model and inductive methods to construct a new cryptosystem that meets homomorphic computation of some operations on cipher texts (e.g., additions, multiplications), Thus the new cryptosystem satisfies fully homomorphic encryption in cloud computing.

Ovunc Kocabas, et.al (2015) proposed an approach that eliminates data privacy concerns in the public cloud scenario, by utilizing an emerging encryption technique called Fully Homomorphic Encryption (FHE) [12]. The ability of FHE to allow computations without actually observing the data itself makes it an attractive option for certain medical applications. In this paper, we use cardiac health monitoring for our feasibility assessment and demonstrate the advantages and challenges of our approach by utilizing a well-established FHE library called HElib.

Bhavna Makhija et.al (2013) 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 [13]. 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 (2012) described that its architecture dramatically reduces the per-application development effort required to offer data protection while still allowing rapid development and maintenance [14]. 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 (2012) analyzed data security and privacy protection issues associated with cloud computing across all stages of data life cycle [15] 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.

Issues and Challenges

Following are the various issues of encryption schemes in cloud computing:-

The Cloud can provide services to the users at lower cost and services are available at any time, anywhere, users data security is the key challenge in cloud computing. The data encryption is the best way for providing data security in cloud computing. The two encryption schemes are come into existence. These encryption schemes are: Full-Disk Encryption (FDE) and Fully Homomorphism Encryption (FHE). FDE encrypts entire physical disks with a symmetric key, often in disk firmware, for simplicity and speed.

2. Although FDE is effective in protecting private data in certain scenarios such as stolen laptops and backup tapes, the concern is that it can't fulfill data protection goals in the cloud, where physical theft isn't the main threat.FHE offers the promise of general computation on ciphertexts. Basically, any function in plaintext can be transformed into an equivalent function in ciphertext: the server does the real work, but it doesn't know the data it's computing. Naturally, this property gives strong privacy guarantees when computing on private data, but the question of its practicality for general cloud applications still remains.

3. The comparison is made between the two data security schemes on basis of certain factors. These factors are: Key management and Trust, Sharing, Aggregation, Performance, Ease of development and Maintenance. From all the above factors, it concluded that Fully Homomorphism encryption scheme is more reliable and provide more security as compared to Full Disk Encryption scheme. The main Problem in Full Disk Encryption scheme is key management, key Storage, Data Aggregation, Access Control list maintaining.

4. To solve the problem of Key management, Key Sharing various schemes have been proposed in last years. The various security attacks are possible in these schemes. The third party auditor is the scheme for key management and key sharing. The main advantage of this is the cloud service provider can offer the functions which were provided by the traditional third party auditor and make it trustful. So it indeed reduces the constitution's complexity in Cloud Computing. The third party auditing scheme will be failed, if the third party's security is compromised or of the third party will be malicious. To solve this problem, In this thesis we will work on to design new modal for key sharing and key management in fully Homomorphism Encryption scheme.

Conclusion

In this paper, it is concluded that security is the major issue of the cloud computing. The encryption schemes are proposed by the various researchers to increase security of the network. The fully disk encryption and fully homomorphic encryption are most efficient schemes for cloud computing. The fully homomorphic encryption scheme is the efficient scheme than fully disk encryption. In future, secure authentication scheme will be proposed to increase security of cloud.

References

[1] Zvika Brakerski, Vinod Vaikuntanathan "Efficient Fully Homomorphic Encryption "LWE, 2010
[2] Sigrun Goluch, "The development of homomorphic cryptography" Vienna University of Technology, 2009
[3] Mehmet K Aktas, Abrar H Shah, and Toshio Akiyama, "Dofetilide induced long qt and torsades de pointes," Annals of Noninvasive Electrocardiology, vol. 12, no. 3, pp. 197–202, 2007.
[4] J.P. Couderc, J. Xia, X. Xu, S. Kaab, M. Hinteeser, and W. Zareba, "Static and dynamic electrocardiographic patterns preceding torsades de pointes in the acquired and congenital long qt syndrome," in Computing in Cardiology, 2010, 2010, pp. 357–360.
[5] Defence Signals Directorat "Cloud Computing Security Considerations" Cyber Security Operations Centre, vol. no. 2, Issue 5, 2011
[6] Anthony T. Velte Toby J. Velte, Ph.D. Robert Elsenpeter ,2010 "Cloud Computing: A Practical Approach", 2011
[7] Ovunc Kocabas and Tolga Soyata, "Towards privacy-preserving medical cloud computing using homomorphic encryption," IGI Global, 2015.
[8] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," in ITCS, 2012, pp. 309–325.
[9] Zainab Hikmat Mahmood, Mahmood Khalel Ibrahem, "New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing", 2018 1st Annual International Conference on Information and Sciences (AiCIS), Pages: 182 – 186
[10] Xidan Song, Yulin Wang, "Homomorphic cloud computing scheme based on hybrid homomorphic encryption", 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Pages: 2450 – 2453
[11] Peidong Sha, Zhixiang Zhu, "The modification of RSA algorithm to adapt fully homomorphic encryption algorithm in cloud computing", 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), Pages: 388 – 392
[12] Ovunc Kocabas, Tolga Soyata, "Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing", 2015 IEEE 8th International Conference on Cloud Computing, Pages: 540 – 547
[13] 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
[14] Dawn Song, Elaine Shi, "Cloud Data Protection for the Masses" IEEE Computer Society, 2012
[15] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering, 2012

