Grenze International Journal of Engineering and Technology, July 2015

Cryptography in The Field of Cloud Computing for Enhancing Security

[1]Nikhitha K Nair, [2]Navin K S and [3]Soya Chandra C S
[1, 3]Department of Computer Science and Engineering, Sarabhai Institute of Science and Technology, Vellanad, Thiruvananthapuram, Kerala
[2]Department of Computer Science and Engineering, L.B.S. Institute of Technology for Women, Poojapura, Thiruvananthapuram, Kerala

***Abstract*—Cryptography is widely used in the field of cloud computing now days. Cloud computing provides the users with the facility to store large amount of data in the cloud from different location. Also data sharing can be done efficiently while dealing with cloud data. But these facilities can bring new challenges to users mainly concerning security and privacy. These are the main issues which can restrict the users to upload their data in the cloud and these issues can prevent users from using the cloud services for various applications. In these cases, cryptographic techniques plays a major role for enhancing security in the field of cloud computing.**

***Index Terms*— Cryptography, Encryption, Cloud, Security.**

I. INTRODUCTION

In the modern era, cloud computing is an emerging terminology. Cloud computing is believed to be considered as a metaphor for internet. The growth of cloud computing is very fast with time. This growth helped Information Technology to get diversified with services for large number of users.

Cloud computing brings forward the facility to utilize different resources that were handled by different users. Cloud acts like a storage area which helped the clients to store their files, data and resources in it instead of keeping files and data in their own hard disk. This facility also paid way for different clients to access and share the files and resources that are being stored in the cloud through the internet. This paradigm put forward the mechanism of data accessibility and data sharing more efficient. Therefore work load on individual client machines greatly reduced.

Beneath all these facilities, the main problem while dealing with the cloud computing is the security and privacy issues. In order to secure the cloud, we must secure the data stored in the cloud, calculations being carried out and the databases that are being hosted by the cloud service providers. The goal towards security includes integrity, confidentiality and availability of cloud data.

The real importance of cryptography comes with providing data security from the unauthorized users. Data cryptography deals with scrambling all the contents of the files that are to be stored in the cloud in such a way that it becomes meaningless or unreadable. This process is known as “Encryption”. The opposite process is called “Decryption” where the original data is retrieved from the encrypted contents.

In cloud computing, both symmetric and asymmetric encryption techniques can be used. But symmetric encryption techniques are found to be more efficient than the asymmetric encryption techniques since large number of databases are kept in the cloud storage.

Grenze ID: 01.GIJET.1.2.540

Cryptography is the mechanism which can be applied in any area ranging from simple applications having calculations to highly efficient cloud computing services where data sharing is involved.

II. Objectives of Cryptography

The main objectives under the study of cryptography include the following terminologies:

A. Data Integrity

The data integrity is the property which deals with unauthorized modification of data that is being stored in the cloud.

B. Non Repudiation

This property will not allow the sender and receiver in denying for sending and receiving the messages or files to each other.

C. Confidentiality

This property deals with protecting the contents in the files or messages when they are to be stored in the cloud and not allowing any third party to access the information that is being stored in the cloud.

D. Authentication

This property deals with identifying the identity of the sender and the receiver involved in transmitting the messages with each other and when the sender wants to store the data in the cloud that has to be shared with the receiver.

E. Access Control

This property deals with only allowing the authorized persons in accessing the data in the cloud while preventing other from access by using keys.

III. Issues Dealing With Security

A. Privacy

Cloud computing uses the terminology of virtual computing. The users who store the data in the cloud, that data will be scattered among various virtual data centers than being in a single physical location. Users can also leak the personal/hidden information when they access the cloud computing services. Therefore, privacy of the data that is being stored in the cloud is affected.

B. Trust

Trust in cloud computing reveals the idea of integrity and surety of data and the clients involved in the entire process of data storage and data sharing.

C. Security

The cloud service providers should employ the techniques of encryption, authorization and authentication in order to mitigate the security issues.

D. Performance and Availability Issues

Most clients who are dealing with business organization worry about the proper levels of performance and availability of applications and services that are being hosted by the clients.

E. Data Portability

Most of the people worry about the process of switching from one cloud provider to another and thereby transferring data. Porting and conversion of data depending on the nature of the cloud service provider’s data retrieval format and type. As open standards tend to become more popular, portability and conversion process slowly tends to ease by itself.

IV. CRYPTOGRAPHIC TECHNIQUES UNDER CLOUD COMPUTING

Cryptography is a technique of keeping data as secure as possible by converting them into format that is unreadable to outsiders. The broad classification of encryption techniques includes: Symmetric key (private key) encryption, Asymmetric key (Public) encryption and hybrid encryption techniques.

Symmetric key algorithms works by using only a single key (private key) .Here both the sender and the receiver uses the same private key for encryption and decryption process. Symmetric key encryption algorithms include both block ciphers and stream ciphers. These algorithms are very fast and easy to implement. Some examples of symmetric key encryption techniques include DES, AES, Triple DES, Blowfish and IDEA.

Asymmetric key algorithms use two different keys (private key and public key) for encryption and decryption process. Here the receiver's public key is used by the sender to encrypt the plain text into cipher text. Receiver on the other hand uses its own private key to decrypt the cipher Text plain text. Some of the examples of this type of encryption technique include RSA, DSA, Diffe-Hellman and ElGamel.

Now days, several encryption techniques are combines and applied in a hybrid manner. Using several encryptions for a particular task increases the way of handling the data security more efficient.

V. RELATED WORK

In paper [4] provides an overview about various cloud deployment models including public private, hybrid cloud and community cloud. It also mentions about various issues dealing with the cloud data. This paper tried to bring out in building a repository for storage and sharing along with data confidentiality across the cloud.

In paper [5], gives an idea about the benefits of using cloud computing which includes cost savings, reliability, flexibility and mobile access. This paper also focuses on various existing symmetric and asymmetric key encryption techniques. The mentioned symmetric key algorithms include blowfish, DES, 3DES, RC5 and AES. Asymmetric encryption techniques covered under this paper includes DSA, RSA, Diffe-Hellman and ElGamel.

In paper [6] provides more detailed survey on various encryption techniques. This paper tries bringing the information about homomorphic encryption technique dealing with additive and multiplicative homomorphic encryption technique.

The paper [7] mentions about attack detection and proactive resolution in a single cloud environment. It also mentions about the proposed approach for enhancing data security in cloud focusing on motivations and method of implementation.

VI. OBJECTIVE OF PROPOSED WORK

The main objective of proposed work is to provide tight security to the data being stored in the cloud. So encryption techniques such AES and XOR encryption schemes are being conducted both by the data owner side and data user side. This paper also attempts to bring in front the scenario of public auditability by a third party auditor in order to verify the integrity of cloud data.

VII. PROPOSED WORK

The proposed work aims in bringing out the different concepts related to cloud computing and cryptography. Cryptography deals with the study of providing security to data and Cloud computing deals with the main concern of data security and privacy.

Different encryption techniques can be clustered and combined at several levels for providing security. While dealing with an organization, encryption techniques can applied at the data owner side, data user side, cloud side and even ad third-party auditor side.

By utilizing different encryption techniques at the same time, increases security on the cloud data. Since cloud provides an environment where large users' gets involved and large number of data gets stored each time, strict cryptographic methods should be used each time relating to privacy concern.

The Objectives of this proposed work includes

a. To design a system which will aim to handle security related issues and provide privacy concerns.

b. To develop a system which is based on different encryption techniques at various levels.
c. To develop a system where the data user can upload their required files in the cloud in a secure manner.
d. To develop a system where user can create signature in order to identify the proper owner of that file by the receiver.
e. To develop a system where cloud performs additional encrypted on the already encrypted data.
f. To develop a system where user can download the encrypted data from the cloud and decrypt it using the cloud key and the private key.

VIII. Conclusion

Cryptography deals with study of encrypting data which can be used in the cloud computing for providing additional security on the data that is being stored in the cloud. Various encryption techniques both symmetric and asymmetric encryption techniques can be used to enhance security. The proposed system develops scenario of providing high security and efficiency with the help of cryptographic techniques.

References

[1] Cong Wang ,Chow, S.S.M., Qian Wang ,Kui Ren ,” Privacy-Preserving Public Auditing for Secure Cloud Storage”, IEEE Transactions on computers, Vol. 62, No. 2, February,2013.

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829837, Apr, 2011.

[3] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[4] Mohit Marwaha, Rajeev Bedi, “ Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing” IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.

[5] Randeep Kaur1 ,Supriya Kinger,” Analysis of Security Algorithms in Cloud Computing , International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 3, March 2014 ISSN 2319 – 4847.

[6] Rashmi Nigoti, Manoj Jhuria, Dr.Shailendra Singh,” A Survey of Cryptographic Algorithms for Cloud Computing”, International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS) ISSN (Print): 2279-0047 ISSN (Online): 22790055 .

[7] Aysan Shiralizadeh, Abdulreza Hatamlou and Mohammad Masdari, “Presenting a new data security solution in cloud computing” Journal of Scientific Research an Development 2 (2): 30-36, 2015 , ISSN 11157569.