A FULLY HOMOGRAPHIC ENCRYPTION MECHANISM TO PROVIDE SECURITY IN CLOUD COMPUTING

Mr. Harish Mamillapalli[1]
3rd Year Student,
Department of Computer Science,
SV U CM & CS, Tirupati.

Prof. S. Rama Krishna[2],
Professor,
Department of Computer Science,
SV U CM & CS,, Tirupati.

Abstract: Cloud computing is a technology that involves a large number of computers connected through Internet or it is a distributed computing over a network. This technology consists of large database, services, applications, software and resources.

Cloud computing technology is a concept of providing dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to users. It provides optimized and efficient computing also has become the next logical step for the IT industry.

Although the cloud computing offers a great deal of benefits, such as, cost reduction, dynamic virtualized resources, store large amount of data and improved productivity, but at the same time it has many security risks. The research aims to build a strong authentication system to restrict the unauthorized users as well as many kinds of possible attacks, such as, Denial-of-Service (DoS) attack & Compromised node attack , wormhole attacks, spoofing attack , man-in-the middle attack and worms injection attack. Apart from the above said , we also tend to concentrate on Quality of service parameters in terms of traffic , congestion , delay , jitter.

INTRODUCTION

Cloud Computing has become the center of attention in the IT world. It provides powerful computing services to individuals and organizations via the Internet, and enables them to access a pool of shared resources such as storage servers and applications.

Businesses of all sizes are adopting cloud computing at an increasing rate as it provides them with great benefits like cost efficiency, since they do not actually have to buy the hardware and software resources, but simply pay per use.

Cloud service providers offer network services, infrastructure and applications in the cloud to both companies and individuals. Moreover, it provides a set of great advantages like mobility, cost efficiency, storage, backup and disaster recovery.

These advantages are the reason as to why an immense number of people are migrating to IT solutions that include cloud computing.

Cloud computing permits clients to use the applications, but do not have Internet on their computers. This technology conveys well-organized computing by merging storage, memory, process and information measure.

Even though, the virtualization and Cloud Computing delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud which makes the users to resist themselves in adopting the technology of Cloud Computing.

METHODOLOGY

Cloud Computing is an advanced process for data distribution through proper authentication as well as it needs high security for which we tried to frame the following objectives

1) The Primary aim of the proposal is to authenticate the users while providing the data through a cloud.

(Here we use the various encryption algorithms such as RSA & AES)

2) The Proposal also concentrates on overcoming / ceasing the attacks by applying advanced techniques

3) Also evaluate the efficiency & performance levels in the network cloud indicating the QoS.

4) Finally comparison of the existing algorithms with the proposed technique to prove the efficiency.

Method : Homomorphic Encryption:

To solve some of these issues in a cloud environment, we propose simple and yet powerful framework using homomorphic encryption of data to store and perform secure operations in the cloud.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must encrypt the file and then store the file to the cloud. If a third person downloads the file, he/she may view the record if he/she had the key which is used to decrypt the encrypted file. Sometimes this may be failure due to the technology development and the hackers. The problem that arises now is that while data can be sent to and from a cloud provider's data centre in an encrypted form; we can't do any work on it without decrypting it. Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and obtain an encrypted result which when decrypted matches the result of operations performed on the plaintext.

The aim of homomorphic cryptography is to ensure privacy of data in communication and storage processes, such as the ability to delegate computations to untrusted parties. Fully Homomorphic Encryption combines security with usability. It can help preserve customer privacy while outsourcing various kinds of computation to the cloud, besides storage. There are two aspects of the computation considered: the data itself (confidentiality) and the function to be computed on this data (circuit privacy).

We propose a fully homomorphic encryption which allows us to carry computations on encrypted data (cipher text), leads to encrypted results. When the results are decrypted will match the actions performed on plain data.

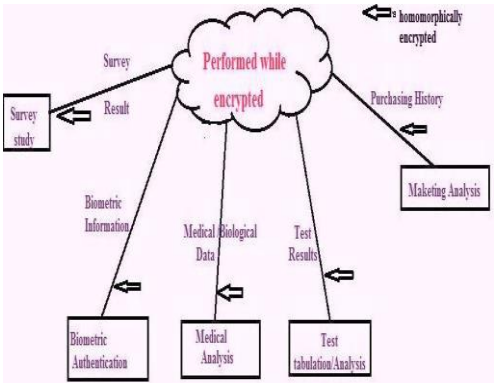

Figure. Overview of the proposed framework

The proposed framework shows the block diagram of the proposed framework to be implemented in a cloud environment. The proposed framework consists simple steps to achieve better security and solve many of the ethical and security issues in a cloud environment.

Homomorphic encryption is a form of encryption that allows computation on cipher texts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. The purpose of homomorphic encryption is to allow computation on encrypted data.

Cloud computing platforms can perform difficult computations on homomorphically encrypted data without ever having access to the unencrypted data. Homomorphic encryption can also be used to securely chain together different services without exposing sensitive data.

Homomorphic encryption can also be used to create other secure systems such as secure voting systems, collision-resistant hash functions, and private information retrieval schemes.

Homomorphic encryption schemes are inherently malleable. In terms of malleability, homomorphic encryption schemes have weaker security properties than non-homomorphic schemes.

IMPLEMENTATION OF HOMOMORPHIC ENCRYPTION SCHEMA :

Homomorphic encryption is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services. Suppose we want to do computation on but want to utilize cloud server for the computation. Since we do not want to give cloud server access to data itself, homomorphic encryption method proves to be best option.

CONCLUSIONS

There is no doubt that cloud computing is the present and future of the IT industry. Cloud computing imposes great benefits that makes it one of the most talked about topics in recent years. According to the analysis of cloud computing it was found that security should be the core operation rather than an add on operation.

AWS(Amazon Web Service) has an outstanding performance in cloud computing because of the its excellent work in the area of Security of data. Cloud computing provides many advantages for individuals and small organizations; it can also create some serious security issues with personal and confidential data.

REFERENCES

[1] Grance, P. Mell and T. ""The NIST Definition of Cloud Computing,"." National Institute of Standards and Technology, U. S. Department of Commerce, 2011.

[2] Correia, F. Rocha and M. "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud." IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops, 2011: 129-134.

[3] Y. Shen, W. Cui, Q. Li and Y. Shi. "Hybrid Fragmentation to Preserve Data Privacy for SaaS." EighWeb Information Systems and Applications Conference (WISA), 2011: 3 - 6.

[4] HCL TECHNOLOGIES: http://www.hcltech.com/blogs/transformation-through-technology/rise-cloud.

[5] R. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public key cryptosystems." Communications of the ACM, 1999.

[6] Boneh, D. & Freeman,D .M . "Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures." Public key Cryptography, 2011.

[7] Suresh, K.Revana. "Ensuring Data Security Using Homomorphic Encryption In Cloud Computing." 2014.

[8] S. Sobitha Ahila, Dr.K.L.Shunmuganathan. "State Of Art in Homomorphic Encryption Schemes." Int. Journal of Engineering Research and Applications, 2014.

[9] Lattices, Fully Homomorphic Encryption Using Ideal. "Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC'09)." ACM Press, New York, NY, USA., 2009.

[10] Smart, N. & Vercauteren. "Fully Homomorphic SIMD Operations." Design Codes and Cryptography, Springer, USA, 2012.

[11] Gentry, C. & Halevi, S. "Implementing Gentry's Fully-Homomorphic Encryption Scheme. In: Advances in Cryptology." Proceedings of EUROCRYPT'11, Lecture Note in Computer Science, 2011.

[12] Stehle, D. & Steinfeld, R. "Faster Fully Homomorphic Encryption." In: Advances in Cryptology – Proceedings of ASIACRYPT'10,, 2010.

[13] Brakerski, Z. & Vaikuntanathan, V. "Efficient Fully Homomorphic Encryption from (Standard) LWE." Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS'11). ACM Press, New York, NY, USA.

[14] Brakerski, Z. & Vaikuntanathan, V. "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages." In Advances in Cryptology- Proceedings of CRYPTO'11, by Springer-Verlag, 505-524. 2011.

[15] Brakerski, Z., Gentry, C., & Vaikuntanathan. "Fully Homomorphic Encryption without Bootstrapping." Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS'12), 2011: 309-325

. [16] Vaikuntanathan, V. "Computing Blindfolded: New Developments in Fully Homomorphic Encryption." Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS'11),, 2011.

[17] Chun-sheng, Gu. "Attack on Fully Homomorphic Encryption over the Integers." International Journal of Information & Network Security (IJINS), 2012.

[18] Rouse, M. (2011, August). Search Security. Retrieved from http://searchsecurity.techtarget.com/definition/homomorphic-encryption.

Authors Profile

Mamillapalli Harish, received Bachelor of Computer Science degree from Sri Venkateswara University, Tirupati in the year of 2013-2016. Pursuing Master of Computer Applications from Sri Venkateswara University, Tirupati in the year of 2016-2019. Research interest in the field of Computer Science in the area of Big Data Analytics , Cloud Computing and Software Engineering.

Prof Dr S. Ramakrishna, working as a Professor in Dept of Computer Science, Sri Venkateswara University College of Commerce Management and Computer Science, Tirupati, (AP)-India. Received M.Sc, M.Phil, M.Tech (IT) and Doctorate in Computer Science from S.V University, Tirupati, having 27 years experience in teaching field. Additional Assignments Working as Dean of Examinations for S.V University, Worked as Additional Convener for S.V University RESET Examinations, Worked as Coordinator for M.Sc Computer Science, Worked as BoS Chairman in Computer Science. Research Papers Published in National & International Journals :99, Total Number of Conferences participated :33, Total number of Books Published:7, Total number of Training Programs Attended : 3, Total number of Orientation & Refresher Courses Attended : 4.Number of research degrees awarded under my guidance :- M.Phil: 20,Ph.D:20.