ENHANCED HOMOMORPHISM ENCRYPTION TECHNIQUE FOR CLOUD COMPUTING

Rashi Sood[1], Munish Katoch[2]
[1] Research Scholar, rashi.sood93@gmail.com
[2]Assistant Professor, munishcse710@gmail.com

Abstract: ***To emphasize FHE encryption device for key management and key sharing. For cloud data security the improvement evidence is based on Diffie-Hellman, SHA-128 and OTP method. The OTP will generate through Email. In this we will undertake to formatting new modal for key sharing and key management in fully Homomorphic Encryption scheme. In this paper, we are using the symmetric key conveying algorithm named Diffie Hellman, it is kind of key replacement algorithm with create session key who endue to communicate with each other between two parties and here, SHA-128 is used for the intelligence uprightness OTP(One Time Password) is created which helps to give much security.***

Keywords: Homomorphic, Encryption, Cryptographic, Authentication, Integrity.

1. Introduction

Cloud computing is a type of web-based computing that gives shared PC handling assets and information to PCs and different resources on request. Cloud Computing is the environment which provides on-demand and convenient entrees of the structure to the computing resources like repository, hosts, routine, web and substitute services which could be discharged in minimum efficiency way. In the cloud computing environment, both diligence and resources are delivered on proceeding over the Internet as services. Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user's requirements. Client recovers message and adjusts message which is confine by node or firm in unite message called cloud. It is a design, where cloud administration ISP gives services to node on move and it is otherwise called CSP residue for "Cloud Service Provider". As the protection against the malicious services or services like recognize fakes, all service provider organizations utilize the access control and client authentication components [9]. To secure the client information, ventures utilize the security system, for example, USB port control, Full Disk Encryption (FDE). The frameworks which runs all the time the above solutions are not powerful that much. They can't keep the assailants to get to information. The services of cloud are mainly available in the three types of Public Cloud, Private Cloud and Hybrid Cloud. [3][6] Various characteristics of cloud computing are also described in the paper [7]. The cloud client applications are produced utilizing mobile application improvement platform and sent on mobile devices. The cloud client applications use the mobile network administrations, for example, wireless network (e.g. Wi-Fi, Wi-Max), cell network (e.g. 3G or 4G), or Satellite network for speaking with cloud controller.

The cloud controller handles the mobile client demands for giving relating cloud administrations. It can be finished up from the investigation of come past reports that the security and privacy change in cloud administrations may build the cloud's subscribers [8]. The essential parameters that should be considered while designing a security plan for mobile cloud processing environment are computational complexity of security plan and resource confinement of the mobile gadget. On the other hand, few security plans are concentrating on the decrease of the computational complexity of the cryptographic algorithms. Be that as it may, the decrease of the computational complexity of cryptographic algorithms may influence the privacy of the transferred information[9]. For offloading of information access operations, the majority of the current plans depend on proxy re-encryption. Despite the fact that the proxy re-encryption plans give backing to offloading of computationally concentrated re-encryption operations, the mobile client needs to play out the encryption and decryption that include huge augmentation and exponential operations of expansive numbers.

2. Cloud -Manager-Based Encryption Scheme (CMRES)

By joining the qualities of the manager based re-encryption and cloud-based re-encryption collaborate, the scheme proposed a cloud-manager-based re-encryption sketch for offloading the complex calculation ownership on the trustworthy-entity and cloud. . Moreover, from the exploratory results presented in next areas, this can be inferred that the energy consumption amid cipher and decipher is directly equivalent to the extent of the record. Increase in document size likewise increases the aggregate number of encryption and decryption operations with constant re-encryption operations. Therefore, there is a need of security plan that can offload the ciphering and deciphering venture on the cloud/outsider in a trusted mode. In the proposed CMReS, the encryption, decryption, an offload the ciphering and decryption venture on the cloud/outsider in a trusted mode. In the proposed CMReS, the ciphering, deciphering, an re-encryption assignments are appropriated between the trusted entity and cloud. There are four fundamental modules in this system, to be specific

(a) Cloud client application facilitated on the mobile users.

(b) Encryption/Decryption Service Provider (EDSP) module facilitated on private cloud inside the client association.

(c) Re-encryption Service Provider (RSP) module facilitated on public cloud.

(d) Cloud repository applications obtainable on public cloud.

The cloud service supplier offers calculation and repository applications to the mobile users. The mobile users upload/download the data to/from the data partition of the cloud through the cloud client application [1]. The EDSP is a completely trusted entity under the control of a client association whose prime responsibility is to give encryption and decryption services to the authorized mobile users. The RSP module is hosted on public cloud which is responsible for keeping up the re-encryption keys and giving the re-encryption services to each authorized mobile user. The RSP module just holds the re-encryption keys of the cloud users having a place with the same virtual association for giving re-encryption services. The exceptional feature of the plan is that the RSP is hosted on the cloud and gives re-encryption services without knowing the private keys of the mobile of this document is located in users.

3. Literature Review

“**Cloud Computing Security Using Encryption Technique” (Geethu Thomas, 2010).** In this paper they presented that the cloud computing is very efficient technology or important field used for data storage due to its efficiency and flexibility. The cloud provides different types of services to the user and the architecture is also based upon those services. The data is stored on to data centers having a large size of data storage. The data as well as processing is somewhere on servers.

“Cloud Computing Security” (Sean Carlin, 2011). In this paper, cloud computing is the distributed architecture that centralizes the resources of server on a scalable platform which provides services on demand. Various cloud deployment models are discussed i.e. public, private and hybrid. The main security issues and risks are discussed; sharing of resources is one of them. Customers are not satisfied with the data security on cloud. Cloud service providers must tell the customers about the deployment models. They need to use the third party auditor so that they can gain the trust of customers. For this, new techniques need to be developed and older should be removed for easy work in cloud architecture.

“Ensuring Data Storage Through A Novel Third Party Auditor Scheme in Cloud Computing” (Shui Han, 2011). In this paper, trustful third party is introduced in which the user can operate and store their data securely in cloud. There is a problem of data storage security in cloud computing. For more security of the cloud new scheme is introduced i.e. novel third party auditor. The advantage of this scheme is that 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 auditor provides techniques like RSA and Bilinear Diffie-Hellman. By using RSA algorithm encrypted data is flow from sender to the receiver and by using Bilinear Diffie-Hellman keys are exchanged for security purposes. With the exchanging of keys, data is always sent to the valid and authorized users only.

“Cloud Computing Security Issues and Access Control Solutions” (Young-Gi Min, 2012). In this paper, three cloud computing models are introduced i.e. SaaS, PaaS, IaaS. There are five layers in cloud computing models are mentioned: Client, application, platform, and infrastructure and server layer. In order to address the security problems, every level should have security implementation. Security requirements of cloud computing and the solutions for the security problems are described. Different security attacks are defined which need to be overcome by applying security algorithms and another techniques. To have secured cloud deployment, areas like computing architecture, portability and interoperability, traditional security, business continuity, disaster recovery, data centre operations, Encryption and key management, identity and access management must be considered. The best way to minimize the unauthorized access is using Digital ID's for the employee; this also addresses the issue of non-repudiation.

"Cloud Computing Security Case Studies and Research" (Chimere Barron, 2013). In this paper they discussed different issues related to cloud computing security. To protect cloud computing system and to prevent various attacks many security mechanisms have been developed. To improve the security of cloud computing new technologies has been developed by the researchers. Different types of attacks like SYN flood, malware injection, account hijacking are discussed in this paper. The main focus of this paper is on detecting and preventing SYN flood in cloud computing. The author developed two algorithm one detecting algorithm and one preventing algorithm. They will implement and test these algorithms on cloud computing.

"Enhanced Data Security in Cloud Computing with Third Party Auditor" (Bhavna Makhija, 2013) In this paper they proposed different techniques and their merits and demerits like Message Authentication Code(MAC) which protect the data from integrity. The owner of any information verified the data integrity by recalculating the message authentication code of data received by others but recalculation is possible if the amount of data is very large. A hash tree is used for large files. Third party auditor is used to relieve the large data into small parts of maintenance and security. The proposed algorithm describes data integrity and dynamic data operations. They use encryption to ensuring the data integrity. Public key is also defined which is based on homomorphic authenticator. A hash function is used for proof of irretrievability. The proposed algorithm has a main drawback that it require implementation of the higher resources cost.

"Secured Hash Algorithm-1" (Chaitya B. Shah , Drashti R. Panchal,2014) The SHA i.e. Secure Hash Algorithm is basically based on the concept of hash function. The basic idea of a hash function is that it takes a variable length message as input and produces a fixed length message as output which can also be called as hash or message-digest. The trick behind building a good, secured cryptographic hash function is to devise a good compression function in which each input bit affects as many output bits as possible [2]. It is used with the Digital Signature Standard (DSA) for digital signature so it has a particular importance. SHA-1 has a set of cryptographic hash functions very similar to the MD family of hash functions. But MD family uses more bits in hash function. That is the main difference between MD and SHA-1.

"Secure and Efficient Integrity Algorithm based on Existing SHA Algorithms"(Snigdha Soni Sandeep Pratap Singh,2015) There is always a demand of modification or replacement of existing algorithms with the modified or latest algorithms. This paper discussed one of the problems faced in integrity algorithms that all the existing algorithms are either proven breakable or not time efficient. This paper studied all such algorithms and also proposed its own integrity algorithm which is not only secure but also time efficient too. This paper shows its implementation results and also proved that proposed algorithm is the efficient and better option to be used in places where data integrity is considered essential. Authors have tested the above results on number of sample files and proposed there results.

"Multilevel Security for Cloud Computing using Cryptography"(K.Satyanarayana,2016) Cloud Computing is a set of Information Technology Services, like network, software system, storage, hardware, software, and resources and these services are provided to a customer over a internet. These services of Cloud Computing are delivered by third party provider who owns the infrastructure. The advantages of cloud storage are easy access means access to your knowledge anywhere, anytime, scalability, resilience, cost efficiency, and high reliability of the data. Because of these advantages each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So it is required to protect that data against unauthorized access, modification or denial of services etc. Hence security of cloud means securing the operations and storage of the cloud providers.

4. Results and Discussions

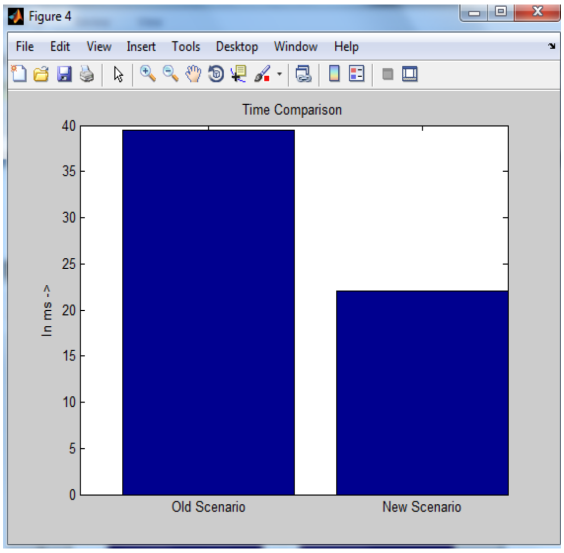

Figure1: Comparison Graph of Delay

Comparison Graph of Delay: As shown in figure1. The differentiation between existing and suggested approach is shown regarding delay. The suspension in existing method is increasing, when numbers of substitute messages are increased. In the proposed method the obstruct is less due to increasing the number of message. The suspension is the time taken by the branch (node) to complete operation which is allocated. Time is calculated by subtracting time at which tasks completed and virtue at which merit is start executed.

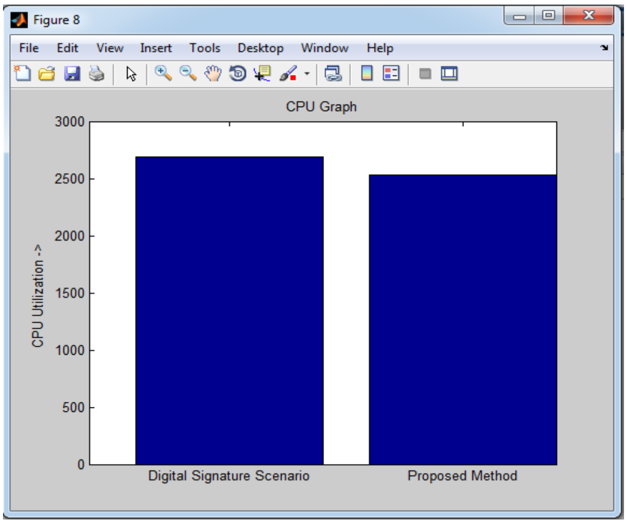

Figure 2: Comparison graph of CPU Utilization

Comparison Graph of CPU Utilization: The CPU utilization is compared in figure 2 in terms CPU utilization. It is analyzed that CPU utilization of proposed technique is less than existing technique.

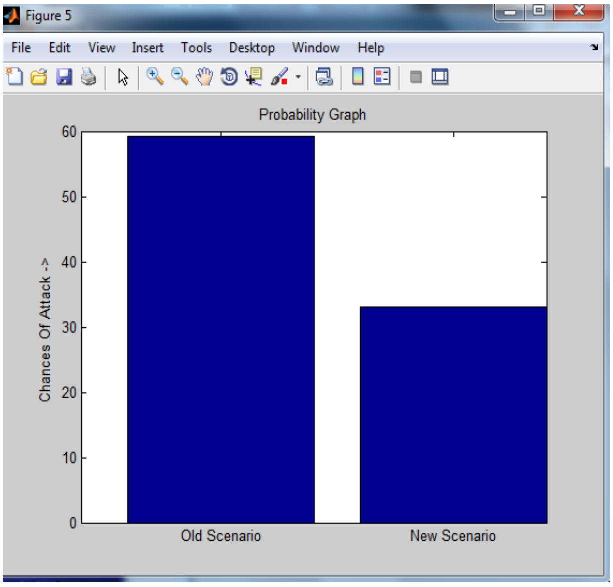

Figure3: Comparison Graph of Attack

Comparison Graph of Attack: The comparison is made between probability of existing and proposed algorithm. It is analyzed that probability of proposed technique is less than existing algorithm.

5.Conclusion

Cloud computing is the surroundings which provides by order and appropriate access of the network to a computing means like espionage, servers, services, networks and the other applications which can be released minimum efficiency way. In this exploiter tins and use different services and store their information and pay according to those services. How we tins store our data while storing into the cloud is the main factor of security. In this paper, we reviewed two most popular techniques for cloud information encryption. These techniques are full disk encryption and fully homomorphic encryption. In this work, we find that fully homomorphic ciphering way is more efficient than full discus encryption. But the main problem exists in fully homomorphic encryption is of key management and key sharing which reduces the reliability of the scheme. Improvement has been proposed in the ciphering devices and improvement is based on Diffie-Hellman algorithm and SHA-128 and OTP is generated on the foundation of secret key generated from Diffie-Hellman algorithm for key management and key sharing. OTP will generate through email which will provide more security among the communication between sender and receiver. Session key between exploiter and cloud is created by this algorithm. Every time between two before communication new key is generated. Secure channel is established between both i.e. exploiter and the cloud service provider which reduces the time takes place in regulation and sharing of keys. The counterfeit shows that proposed enhancement is more efficient and reliable than the existing one.

6. Acknowledgement

I sincerely express my deep gratitude Er. Munish Katoch (Assistant Professor, CSE Department, Sri Sai University Palampur (H.P), India for his constant encouragement, motivation and supervision throughout my work. His endless support helped me in channelling my efforts and ideas in proper direction.

References

[1] Geethu Thomas, 2010 “Cloud computing security using encryption Technique” researchgate.net/publication.
[2] Sean Carlin, Kevin Curran, 2011 “Cloud Computing Security” International Journal of Ambient Computing and Intelligence, pp 14-19.
[3] Shui Han, Jianchuan Xing, 2011 “Ensuring Data Storage Through A Novel Third Party Auditor Scheme in Cloud Computing” IEEE computer science & Technology, pp 264-268.
[4] Dr Nashaat el-Khameesy,Hossam Abdel Rahman, 2012 “A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems”, IEEE computer science & Technology vol-3.
[5] Dian-Yuan Han, Feng-qing Zhang, 2012 “Applying Agents to the Data Security in Cloud Computing” International Conference on Computer Science and Information Processing(CSIP), pp 1126-1128.
[6] Simarjeet Kaur, 2012 “VSRD-IJCSIT, Vol. 2 (3), 2012, 242-249. Cryptography and Encryption In Cloud Computing, pp 242-249 IOSR Journal of Engineering (IOSRJEN).
[7] Young-Gi Min, Hyo-Jin Shin and Young-Hwan Bang, 2012 “Cloud Computing Security Issues and Access Control Solutions” Journal of Security Engineering, pp 135-140
[8] Deyan Chen, Hong Zhao, 2012 “Data Security and Privacy Protection Issues in Cloud Computing” International Conference on Computer Science and Electronics Engineering, pp 647-651.
[9] Dawn Song, Elaine Shi, 2012 “Cloud Data Protection for the Masses” IEEE Computer Society, pp 39-45.
[10] Barron, C., Yu, H., & Zhan, J., 2013 “Cloud Computing Security Case Studies and Research”. Proceedings of the World Congress on Engineering 2013 Vol II.
[11] Punithasurya K, Esther Daniel, Dr. N. A. Vasanthi, 2013 “A Novel Role Based Cross Domain Access Control Scheme for Cloud Storage” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013, pp 942-946.
[12] Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore, 2013 “Cloud Computing Security” International Journal on Recent and Innovation Trends in Computing and Computation, pp 36-39.
[13] Sanjoli Singla, Jasmeet Singh, 2013 “Cloud Data Security using Authentication and Encryption Technique” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013, pp 2232-2235.
[14] Vimmi Pandey, 2013 “Securing the Cloud Environment Using OTP” International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4.
[15] Bhavna Makhija, VinitKumar Gupta, 2013 “Enhanced Data Security in Cloud Computing with Third Party Auditor”, International Journal of Advanced Research in Computer Science and Software Engineering, pp 341-345.
[16] Chaitya B. Shah , Drashti R. Panchal,2014 “Secured Hash Algorithm-1” International Journal For Advance Research In Engineering And Technology.

[17] Manreet Kaur, Monika Bharti,2014 “Securing user data on cloud using Fog computing and Decoy technique” International Journal of Advance Research in Computer Science and Management Studies.
[18] Snigdha Soni Sandeep Pratap Singh,2015 “Secure and Efficient Integrity Algorithm based on Existing SHA Algorithms” International Journal of Computer Applications (0975 – 8887.
[19] K.Satyanarayana,2016 “Multilevel Security for Cloud Computing using Cryptography” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET).