International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 10 | Oct -2017 www.irjet.net p-ISSN: 2395-0072

Secure Channel establishment techniques for Homomorphic encryption in Cloud Computing

[1]Akriti Sharma, [2]Nagresh kumar

[1,2] *Meerut Institute of engineering and technology, Meerut, Uttar Pradesh, India*

Abstract: *Cloud computing is a technology or distributed network where user can move their data and any application software on it. But there is some issues in cloud computing, the main one is security because every user store their useful data on the network so they want their data should be protected from any unauthorized access, any changes that is not done on user's behalf. There are different encryption techniques used for security purpose like FDE and FHE. To solve the problem of Key management, Key Sharing various schemes have been proposed. 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, we will work on to design new modal for key sharing and key management in fully Homomorphic Encryption scheme. In this paper, we have used the symmetric key agreement algorithm named Diffie Hellman, it is key exchange algorithm with create session key between two parties who want to communicate with each other and HMAC for the data integrity OTP(One Time Password) is created which provides more security. Due to this the problem of managing the key is removed and data is more secured.*

1. Introduction

Cloud Computing is the environment which gives on-demand and convenient access of the system to the computing assets like storage, servers, applications, networks and alternate services which can be discharged least productivity way. Client recovers information and adjusts information which is put away by client or an organization in unified information called cloud. Cloud is a design, where cloud administration supplier gives services to client on demand and it is otherwise called CSP remains 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. Cloud computing is the environment which gives on-demand and convenient access of the system to a computing assets like storage, servers, applications, networks and alternate services which can be discharged least efficiency way. The five key characteristics are made by cloud design. Cloud design likewise advances the accessibility [9]. Cloud services are mainly available in the three types of cloud which are, 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. 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. 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.

This paper proposed cloud-manager-based re-encryption plot that uses the attributes of the current manager-based re-encryption and cloud-based re-encryption plans for distributing the computational assignments among mobile gadget, trusted-entity, and cloud [1]. To minimize the responsibilities of the manager in MReS, the Cloud-based Re-encryption Scheme (CReS) offloads the significant segment of data access operations on the cloud without

revealing the security keys and data contents. Moreover, in cloud-based re-encryption conspire a single key is shared among all the group members of specific data partition on the cloud. Therefore, the current/leaving group member can unscramble the transferred data on the data partition of the cloud.

2. Literature review

"Securing the Cloud Environment Using OTP" (Vimmi Pandey, 2013). In this paper, Dynamic mobile token application is presented [10]. This is the application in mobile telephones which is utilized to produce a code with the assistance of OTP (One Time Password). This OTP code is utilized just for one time to login session. In this paper, they depict one of the techniques for OTP. There are two phases in it Registration phase and Login phase. Client first registers itself by fill credentials in the structure and after that enters to the Login phase. In login phase, OTP will create for the login session. OTP is produced by three parameters: The current time, 4-digiti PIN code and Init-secret. This code is valid for three minutes as it were. This ensures protection against eavesdroppers attack and man-in-middle attack. Thus, they demonstrate OTP is extremely secure.

"Cloud Data Security using Authentication and Encryption Technique" (Sanjoli Singla, 2013 In this paper, an outline and architecture is recommended that can encrypt and decrypt the record at the user side which gives data security in both cases while user is at rest or is exchanging data [8]. In this paper they utilized the Rijndael Encryption Algorithm alongside EAP-CHAP. This calculation has five stages which should be taken after for the data security. The users are dependably worry about the privacy protection and security issues before storing their data on cloud. So in this the emphasis is on client side security in which just the authorized user can access the data. Regardless of the possibility that some intruder (Unauthorized user) gets access of the data then the data won't be decrypt. Encryption must be finished by the user to give better security Algorithm. For this, Rijndael Encryption calculation is utilized.

"Cloud Computing Security" (Ankur Mishra, 2013). In this paper, two systems are examined: Virtualization and Muti-tenancy which gives security about cloud processing [2]. Data is composed by outsider associations that offer Saas and PaaS which is essential for the security. In this way, Virtualization and Multi-tenancy procedures are utilized for the security purposes. Virtualization is a method for making a physical PC capacity as though it were two or more PCs where each non-physical or virtualized. There are two sorts of virtualization: Full virtualization and Para virtualization and two architectures of virtualization: Hosted and Hypervisor architecture. Multi-tenancy is the capacity to give figuring services to numerous clients by utilizing a typical infrastructure and code base. Multi-tenancy can be connected to different levels i.e. application level, middleware level, operating system, hardware level. At that point security of virtualization and multi-tenancy has been talked about.

"Cloud Data Protection for the Masses" (Dawn Song, 2012) In this paper the creator portrayed the data-protection-as-a-service where different services are accommodated securing data [4]. Two systems have talked about which are: FDE (Full Disk Encryption) and FHE (Fully Homomorphic Encryption). There is an examination in these systems on the premise of key management, sharing, and simplicity of advancement, upkeep, aggregation and performance. The key management and access control are moved by DpaaS (Data-Protection-as-a-service) approach for reason for balance simple support and fast advancement by user-side verification. Performance and simplicity of advancement offered by FDE is amazing.

"Data Security and Privacy Issues in Cloud Computing" (Deyan Chen, 2012). In this paper, it portrays data security and privacy protection issues occurred in cloud computing in all the phases of data life cycle [5]. There are seven phases of data lifecycle: Generation, use, transfer, share, storage, archival, destruction. They have examined some current arrangements like completely homomorphic procedure, data integrity, client-based privacy management tool, and so forth. Most likely cloud has many points of interest yet at the same time there are many issues like security should be illuminated. As indicated by the study of Gartner for cloud computing, Public and Hybrid cloud has revenue of $59 billion and by the year 2014 it will reach USD 149B with a yearly development of 20. The increase in the revenue of cloud with the time demonstrates that cloud is a reliable industry. Yet at the same time there are some issues in cloud regarding security of data which increases the threats from hackers.

"Cloud Computing Security Issues and Access Control Solutions" (Young-Gi Min, 2012). In this paper, three cloud computing models are presented i.e. SaaS, PaaS, IaaS. There are five layers in cloud computing models are specified: Client, application, platform, and infrastructure and server layer [11]. With a specific end goal to address the security issues, each level ought to have security execution. Security requirements of cloud computing and the answers for the security issues are depicted. Different security attacks are characterized which should be overcome by applying security algorithms and another

methods. To have secured cloud arrangement, areas like computing architecture, portability and interoperability, traditional security, business progression, disaster recovery, data focus operations, Encryption and key management, identity and access management must be considered. The most ideal approach to minimize the unauthorized access is utilizing Digital ID's for the representative this likewise addresses the issue of non-repudiation.

3. Cloud-Manager-Based Encryption Scheme (CMReS)

By joining the qualities of the manager based re-encryption and cloud-based re-encryption conspires, the strategy proposed a cloud-manager-based re-encryption plan for offloading the complex computational operations on the trusted-entity and cloud. Moreover, from the exploratory results presented in next areas, this can be inferred that the energy consumption amid encryption and decryption is directly proportional to the size 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 encryption and decryption operations on the cloud/outsider in a trusted mode. In the proposed CMReS, the encryption, decryption, and 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, and
(d) Cloud storage services accessible on public cloud.

The cloud service provider offers computational and storage services 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 users.

4. Proposed Technique

There are many encryption algorithms to provide security to the cloud. “Fully Homomorphic” is more reliable. It gives more privacy and security as compare to scheme of “Full Disk Encryption”. The main problem which is there in Fully Homomorphic Encryption is a key storage, key management, Access control and Data Aggregation list maintaining. To solve 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 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 model for key sharing and key management in fully Homomorphic Encryption scheme. 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. For key management and key sharing, enhancement has been proposed in the encryption scheme and enhancement is based on Diffie-hellman algorithm and HMAC and OTP is generated on the basis of secret key generated from diffie-hellman algorithm. This algorithm create session key between user and cloud. Each time new key is generated between two before communication

Selected node suppose user1
1. Login
2. Key generation
2.1 Enter prime numbers
2.2 Enter random numbers by client and cloud service provider
2.3 Secret key generation and secure channel establishment.

OTP (One Time Password) generation
3.1 cloud server will set count1=0, count2=0...count5=0 for respective user at its side.
3.2 Cloud Server will request for the OTP from user 1
3.3 user1 enter (secret key+count) as OTP
3.3 server match it because server knows both secret key and count of each user.
3.3.1: count1++; // so for user 1 it will be count1=1; for remainig user their count will be still 0;

3.3.2 if (secret_key+count(x) == secret_key+count(y))
{ Access granted;
display message by server : print ("please enter the operation");}
else{ display message by server: print(" wrong password, your login number is count1);}
4.4 clinet will enter the operation using HMAC digest
4.4.1 : hmac(already generated secret key || v, file1,ver1 || sha1)
{ if(ope==v)

{ server will check the file name and version;

if (file1,ver1== file1,ver1)

{ printf("file is valid"); }

else { print (file is invalid, please replace the file)

}}
if(ope==I) { insert new file file2 }
5. encryption/decryiton
6.data operation
7.logout;

note: // 1.at client side, user will enter prime number, random number for generating secret keys, once generating secret key user will enter otp , after inserting otp, user will enter operation(Insertion) with corresponding file name(file1 or file2).

Experimental results

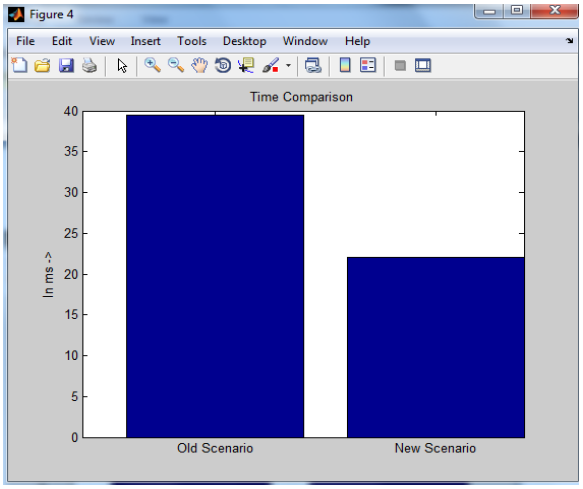

Figure 4.16: Comparison graph of delay

As shown in figure 4.16, the comparison between previous and proposed approach is shown in terms of delay. The delay in previous technique is increasing, when numbers of exchange messages are increased. In the proposed approach the delay is less due to increasing the number of message.

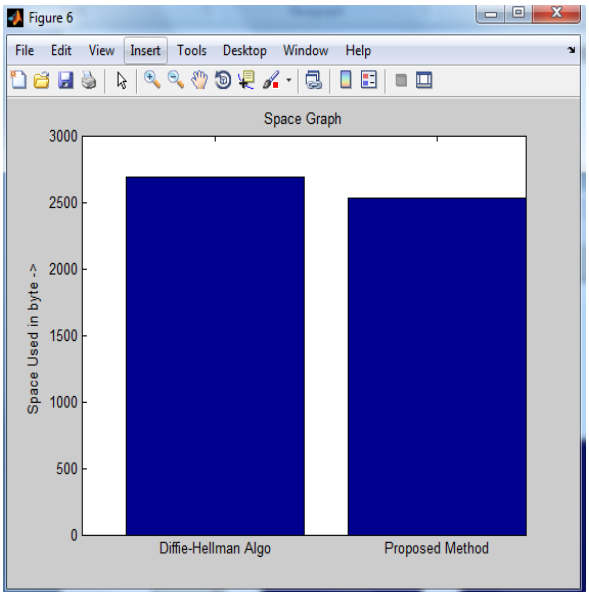

Figure 4.17: Comparison graph of Space

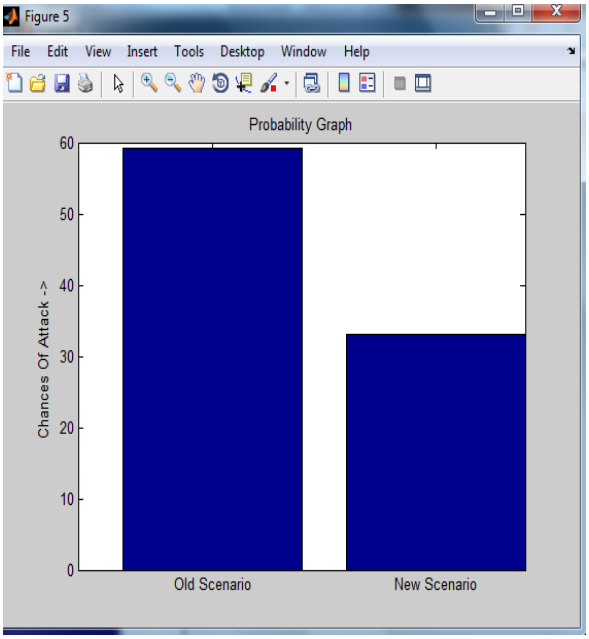

Figure 4.18: Comparison graph of space

Conclusion

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. For key management and key sharing, enhancement has been proposed in the encryption scheme and enhancement is based on Diffie-hellman algorithm and HMAC and OTP is generated on the basis of secret key generated from diffie-hellman algorithm. This algorithm creates session key between user and cloud. Each time new key is generated between two before communication. This reduces the time takes place in management and sharing of keys and secure channel is established between both i.e. user and the cloud service provider. The simulation shows that proposed enhancement is more efficient and reliable than the existing one.

5. References

[1] Abdul Nasir Khan, M. L. Mat Kiah · Mazhar Ali, Shahaboddin Shamshirband, Atta ur Rehman Khan," A Cloud-Manager-Based Re-Encryption Scheme for Mobile Users in Cloud Environment: a Hybrid Approach", 2015 Springer Science + Business Media Dordrecht

[2] 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

[3] 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

[4] Dawn Song, Elaine Shi, 2012 "Cloud Data Protection for the Masses" IEEE Computer Society, pp 39-45

[5] 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

[6] Dr Nashaat el-Khameesy, Hossam Abdel Rahman, 2012 "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" vol-3

[7] John Harauz, Lori M. Kaufman,Bruce Potter," Data Security in the World of Cloud Computing " IEEE Security and Privacy July 2009. pp. 61-64

[8] 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

[9] 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

[10] Vimmi Pandey, 2013 "Securing the Cloud Environment Using OTP" International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4

[11] 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