Enhancement in Homomorphic Encryption Scheme for Key Management and Key Sharing in Cloud Security

Kiran Pal Kour Bali[1] Kestina Rai[2]
[1]M.tech Student [2]Assistant Professor
[1,2]Department of computer science engineering
[1]CGC, Landran, Mohali, India

Abstract— With the moving time, cloud computing is gaining importance, as it offers storage of data at terribly less worth and is additionally gift at all the time over the net. Cloud computing lets the users use applications void of installation and access their personal information at any laptop with the helpof internet access. Cloud computing is most propitious however it additionally has bound hindrances for storage of data. For information security, cryptography is one amongst the conventions used schemes. Cryptography stratagems area unit primarily of two types: Fully Disk Encryption Scheme (FDE) and Fully Homomorphic Encryption scheme (FHE). Comparison is completed between the two schemes on bound factors that shows the Fully Homomorphic Encryption scheme is superior than Fully Disk Encryption scheme in terms of security and privacy of information however it even have some uncertainties like key management and key sharing. In this paper, we tend to propose a complete unique technique to resolve the uncertainties of key management and key sharing. To realize this novel technique we will establish a secure channel between user and cloud server by victimization Diffie Hellman Key Exchange Algorithm and that we will also use the HMAC protocol for information integrity and information authentication.

Key words: Cloud computing, data storage, FDE, FHE, security.

I. INTRODUCTION

Cloud computing is a model for sanctioning convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) they may be chop-chop provisioned and free with stripped management effort or service supplier interaction[1]". So, in a cloud computing there is no demand to accumulate information on desktops, portables, personal devices etc. users willstore their information on the cloud server and can might access the information with the assistance of web. Cloud could be centralized info where many clients/organizations store their data and probably modify information and retrieve information [2].

Cloud computing is a model for providing convenient ,on demand network access to a shared pool of configurable resources(e.g. servers, network, applications, storage) that can provisioned and released with minimal management effort or service provider interaction. Today a large number of organizations and business units use the cloud for their day to day operations and also the adoption rate by others are also increasing [3].

The cloud computing model has three service job models and three sets up models. The three service job models are:

(1) Cloud software as a service
(2) Cloud platform as a service
(3) Cloud infrastructure as a service

Software as a service offers renting application functionality from a service provider instead of purchasing, setting up and running software by the user. Platform as a service provides a manifesto in the cloud, upon which different applications can be executed and developed whereas, infrastructure as a service offers computing power and storage space on demand.

The three set up models are:

(1) Private cloud
(2) Public cloud
(3) Hybrid cloud

In private cloud, cloud services are provided to an organization and are managed by the organization or third party. In public cloud, cloud services are available to the public and owned by an organization selling cloud services whereas hybrid cloud is a composition of different cloud computing infrastructure mainly public and private cloud. Cloud computing has many advantages that distinguishes it from other resource provisioning environment services [4]. These main advantages are as follows.

A. Cost saving:

Cloud computing shifts the location of resources in the cloud to reduce the costs associated with over-provisioning (i.e. having too many resources), under-utilization (i.e. not using resources adequately) and under-provisioning (i.e. having too little resources)[10]. Organizations can reduce their capital expenditure and use operational expenditures for increasing their computing power.

B. Maintenance:

Cloud service providers do the service maintenance and access is through APIs that do not require an application installment on personal devices or PCs, thus further reducing the requirements for maintenance.

C. Multi-tenancy:

In a cloud computing, services owned by different providers are co-located in a specific data region. The implementation and administration issues of these services are shared among service providers and the substructure providers. Multi means numerous and tenancy means customers. Thus the term multitenancy means several customers can access the applications or store their data on the cloud.

D. Utility based pricing:

Cloud computing presents pay per use pricing standard. The particular pricing standard differs from expertise to expertise [5]. For example, a SaaS contributor may charge a virtual machine from an IaaS contributor on the basis of each hour usage. On the other hand, a SaaS provider that presents on

demand customer relationship management may charge its customers based on the number of clients it assists. Thus, customers have to compensate on the basis of how much they use the cloud.

As every good side has also its bad side therefore, cloud computing has many disadvantages also. The main disadvantages are discussed as follows.

E. Security:

The security issue has played the most important role in hindering cloud computing acceptance. Various security issues, possible with cloud computing are: accessibility, veracity, confidentiality, authentication, data isolation, privacy, repossession, accountability, multi-tenancy issues and so on. Solution to various cloud security issues vary through cryptography, especially public key infrastructure (PKI), use of multiple cloud providers, standardization of APIs, improving virtual machines support and legal support [14], [17].

F. Difficult to migrate:

It's not very easy to move the applications from an enterprise to cloud computing environment or even within different cloud computing platforms because different cloud providers support different application architectures which are also dissimilar from enterprise application architectures [14].

G. Continuously Evolving:

Other ingredients are uninterruptedly emerging, as are the needs for interfaces, linkage and storage capacity. This states that a cloud, in particular a public one, does not remain stationary and is also continually developing.

H. Internet dependency- performance and availability:

A cloud computing service relies fully on the accessibility, speediness, characteristics and functioning of internet as it works as a carrier in between consumer and service provider [14]. In business applications, downtime is a common concern because every minute of downtime is a minute in which important business application can't be performed which degrades the performance of the organization as well reputation also [14].

II. LITERATURE SURVEY

Although cloud computing has many plus points, but there still exist many difficulties that need to be solved [6]. According to a survey about cloud computing, the profits in market size for public and hybrid cloud is $59 billion and it will go on to USD 149B by 2014 with a compound annual growth rate of 20. The income assessment implies that cloud computing is an auspicious industry. To prevent data admittance from unconstitutional access, a distributed technique was projected. The projected techniques [7] perfectly stores the data and identifies at the cloud server and also execute some of the tasks such as data deleting, data inserting and data updating. For data protection, various data encryption schemes [8] like homomorphic encryption, searchable and designed encryption, individuality based encryption, sign based encryption are proposed. These are emerging techniques in cloud world security to provide day night full protection to critical data information.

To encrypt and decrypt the file at the user side various designs and architectures are proposed which provide security to data at rest as well as while transferring. One of the architecture proposed is a Rijndael Encryption Algorithm along with an EAP-CHAP [9]. From the customer perspective cloud computing security concerns especially privacy protection and data security issues remains the primary inhibitor for the adoption of cloud computing services. So in this architecture only authorized user can access the data. Even if some intruder (unauthorized user) gets access of the data accidentally or intentionally he will not be able to decrypt it. Also it is proposed that encryption must be done by the user to provide better security algorithm. There are many techniques that can be used for data privacy and security in cloud computing. One of the techniques used for cloud data security is by using Third Party Auditor. Third Party Auditor [16] is a kind of inspector. There are two groupings: private audit ability and public audit ability. Although, private audit ability achieves a higher amount of efficiency whereas public audit ability allows anyone not just the user or client to question the cloud server about the correctness of data storage while keeping no private information.

With the increase in the use of the cloud applications, any personal information that facilities in the cloud can be found on any other device. In order to provide the user's data privacy, Siani Person puts forward some principles [11] in the design process of cloud computing services to ensure that the user's data and organizational information would not leak out. These rudiments are as follows:

(1) Transmit and store the user's information as little as possible. After systematic analysis, cloud computing applications will collect and store the important information only.
(2) Security measures will be adopted to prevent unauthorized access, copying, or modifying personal information.
(3) Allow users to make a choice. Users have the right to select the use of personal information. Besides, they can join or leave freely.
(4) Establish feedback to ensure that safety tips and detailed measures of the service will be provided to the timers.
(5) Make clear and limit the purpose of use of data.

Cloud storage is a model of networked enterprise storage, where data is not stored only in the user's computer, but also in virtualized pools of storage which are generally hosted by third party. Hosting companies operate large data centers, and users who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualized the resources according to the requirements of the custom and expose them as storage pool, which the customers themselves use to store files or data objects. Physically, the resource may span across multiple servers. The safety of the files depends on the hosting websites [12]. Many organizations in the industry have jumped into cloud computing and implemented it. Amazon has played a key role and launched the Amazon Web Services (AWS) in 2006. Also Google and IBM have started their projects in research of cloud computing.

Eucalyptus became the first open source manifesto for adopting private clouds [13].

Cloud computing provides a comprehensive service management solution to simplify the customer's cloud journey to deliver cloud services with flexibility, speed, scale and security. Applications are no longer installed locally on a user's desktop PC, instead, upgrades, licensing and vision control, support and provisioning are all managed at the server level [15]. Saas eliminates customer worries about application servers, storage, application development and enable global access, significant cost reduction and simplified operations for clients.

III. FULLY HOMOMORPHIC ENCRYPTION SCHEME

Fully Homomorphic Encryption offers the potential of general computation on cipher texts. At a basic level any function in a plain text can be rehabilitated into an equivalent function in cipher text, the server does the genuine effort, in default of knowing the data it is operating on. This distinctive

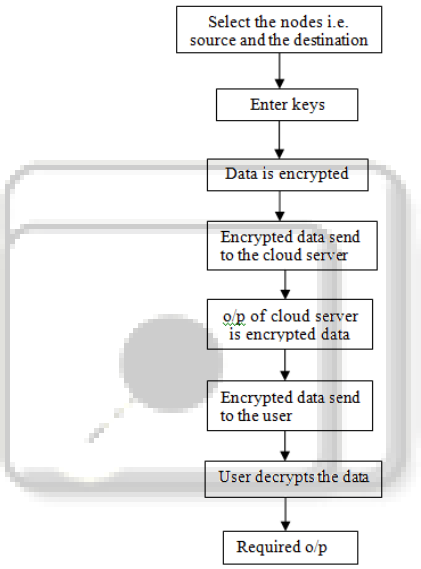

Fig. 1: general framework of fhe

property provides dedicated confidentiality guarantees when computing on secretive data, but the question of its practicality for the general cloud remains. An FHE scheme allows user to perform non- interactive secure computation. In several appliances, this attribute can be fundamental. Within a cloud settings, should a cloud service provider be treacherous, the user is faced with a choice either to deposit confidential data at threat, or encrypt the data sooner than uploading. Homomorphic encryption [8] offers operations on encrypted data without access to the original data. Figure 1 shows a general frame work of Fully Homomorphic Encryption Scheme.

In homomorphic encryption scheme keys are entered for encryption. Data is encrypted before it is being sent to the cloud server. The cloud server performs the operations on the encrypted text. The cloud server provides the results in encrypted form to the user. After receiving the results the user finally decrypts the results to obtain the final original results. Since FHE offers the privacy of user's data but it lacks in certain issues like key management, key sharing and performance.

IV. PROBLEM STATEMENT

The emphasis of cloud computing is to increase the capacity or add capacities on the top without investing in new infrastructure, training new personnel or licensing new software. Cloud computing comprehend any payment based or pay per use service and is instantaneous used with the help of internet. Everything is perfect with the cloud computing, but everyone is gifted with mixed blessing i.e. advantages and disadvantages. In cloud computing users are usually worried about the security and privacy of their confidential data on the cloud server. To provide data security, we usually focus on cryptography. The two main cryptography techniques used are: Fully Disk Encryption scheme and Fully Homomorphic Encryption scheme. Due to certain factors (key management, key sharing, aggregation, performance, ease of development and maintenance), [18] it is concluded that Fully Homomorphic Encryption scheme has improved security and privacy of data over the Fully Dusk Encryption scheme. But Fully Homomorphic Encryption scheme still lacks in certain issues like key management and key sharing because in FHE encryption keys are typically managed and owned by the user. Here raises the question about how users can store their keys, particularly in presence of sharing. To solve the problem of key management and key sharing different schemes has been proposed in recent years. One of the proposed techniques to solve the issues of key management and key sharing is Third party auditor. The Third party scheme falls short, if the third party security is compromised or the third party is malicious. To solve this problem, we propose a novel technique using secure channel establishment between the user and the cloud server with the help of a Diffie Hellman algorithm for key exchange and we also use H-mac protocol to provide authentication and integrity of user's data.

V. DEVELOPED SOLUTION

The central point of our developed solution is to solve the issues of key management and key sharing in the Fully Homomorphic Encryption scheme. This can be achieved by establishing a secure channel between user and cloud server i.e. we use Diffie Hellman key exchange algorithm. We also use H-mac protocol for authentication and integrity of data. In this novel technique there is no need to store and manage the keys of encryption of FHE by the users. Keys are automatically created when needed and automatically get destroyed when their work completes and also the keys are not stored anywhere. So, the users do not need to worry about the storage and management of keys as keys are automatically created and destroyed depending on their use. In H-mac protocol we use read/write permission so that no one except the original owner can read and write the data.

In Diffie Hellman Key Exchange Algorithm, the two parties who want to communicate securely agree on symmetric key. To establish a secure channel two parties select two large prime numbers. These two numbers need not to be kept secret. Now the two parties say A and B select their private numbers, these numbers are 'a' and 'b' respectively. Both the parties calculate two numbers J and K

from their selected public and private numbers. After calculating these two numbers both parties exchange J and K through intermediate nodes in the network. When A receives K and B receives J, both the parties calculate modulus. If the values of modulus calculated by both the parties are similar, a secure channel is established between the two. The secure channel is established between the source and destination and encrypted is exchanged between the two parties.

HMAC stands for hash based message authentication code. HMAC can be used for the security implementation of internet protocol security and is also used in the secure socket layer which is mainly used on the internet. It is an authentication technique based on cryptography which often provides integrity of data during transaction. It also prevents unauthorized reading and writing of data. In this we reused already existing algorithm like MD5 or SHA.

The general framework of our proposed technique is defined in figure 2. In our proposed scheme we use HMAC protocol which offers security in terms of integrity and authentication of confidential data. In our scheme we use read/write permission of HMAC so that nobody except the owner of the data can read and write the secret data. In our scheme we do not need to store and manage keys as keys are created and destroyed as per their use with the help of implementation of Diffie Hellman Key Exchange Algorithm. Thus the proposed schemes solve the issues related to the Fully Homomorphic Encryption scheme i.e. the key management and key sharing issues. Now, the user does not need to worry about the storage and management of keys because there is no requirement to store and manage keys by using Diffie Hellman Key Exchange Algorithm. Also with the use of HMAC protocol users need not to worry about the integrity and authentication of their secret data during transactions.

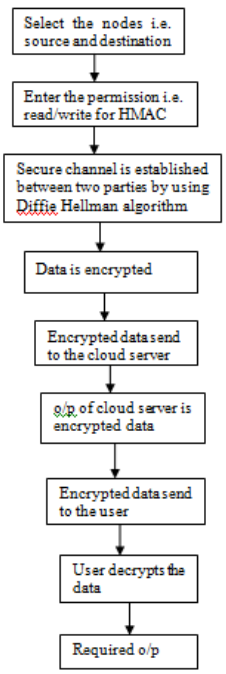

Fig. 2: general framework of developed solution

VI. RESULTS

After completion of the implementation we compare between the two schemes i.e. the already existing scheme and developed scheme. Comparison is made on the basis of time and energy graphs. In figure 3, the comparison graph between the previous and proposed approach is shown in terms of time.

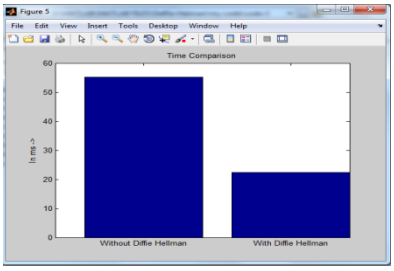

Fig. 3: time comparison graph

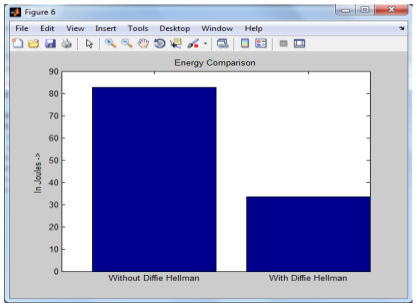

Fig. 4: energy comparison graph

The delay in previous scheme is increasing, when numbers of exchanged messages are increased. In the proposed schemes delay is less due to increasing the number of messages. The figure 4 shows the energy consumption in new and previous technique as shown below. Due to the much number of message exchange in previous technique, energy graph take hike. In new approach, as increasing the number of exchange messages it require less energy

VI. CONCLUSION

Cloud computing is gaining importance day to day but the main challenge in cloud computing is data security. Two techniques are used for data security: Fully Homomorphic Encryption scheme and Fully Disk Encryption scheme. Comparison between these two schemes concluded that the Fully Homomorphic Encryption scheme is better than Fully Disk Encryption Scheme but there are certain issues in Fully Homomorphic Encryption Scheme. These issues are key management and key sharing. In our proposed solution we work on these two issues with the help of HMAC protocol and by using Diffie Hellman Key Exchange Algorithm. With the help of this scheme users need not to worry about the management of keys and this scheme also provides security in terms of authentication and integrity of data.

REFERENCES

[1] National Institute of Standards and Technology-Computer security Resource Center - www.csrc.nist.gov

[2] Mark D. Ryan , "*Cloud Computing for Enterprise Architectures: Concepts, Principles and Approaches*", 2013

[3] Ponemon research study infographic: Whos minding your cloud? *http://www.ca.com/us/collateral/white-papers/cloud-ponemon-research-study-infographic-whosminding*- your-cloud.aspx, 2013.

[4] Ajay Jangra, Renu Bala "*Spectrum of Cloud Computing Architecture: Adoption and Avoidance Issues*", International Journal of Computing and Business Research, Volume 2, Issue 2, May 2011.

[5] C. Braun, M. Kunze, J. Nimis, and S. Tai, "*Web-based Dynamic IT-Services"*,Springer Verlag, Berlin, Heidelberg, 2010.

[6] Devan Chen, Hong Zhao "*Data Security and Privacy Protection issues in Cloud Computing*" International Conference on Computer Science and Electronics Engineering, 2012

[7] Deepanchakaravarthi Purushothaman and Dr. Sunitha Abburu "*An Approach for Data Storage Security in Cloud Computing"* IJCSI International Journal of Computer Science Issues, Vol.9, Issue2, No 1.,2012

[8] Simarjeet Kaur " *Cryptography and Encryption In Cloud Computing"* VSRD-IJCSIT, Volume 2(3), 2012,242-249, 2012

[9] Sanjoli Singla, Jasmeet Singh "*Cloud Data Security using Authentication and Encryption Technique"* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013

[10] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "*A view of cloud computing*" April 2010.

[11] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, *"Cloud security issues*" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009

[12] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "*Ensuring Data Storage Security in Cloud Computing",* In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.

[13] Yashpalsinh Jadeja and Kirit Modi, "Cloud Computing -Concepts, Architecture and Challenges", International Conference onComputing, Electronics and Electrical Technologies [ICCEET],IEEE-2012

[14] Ajay Jangra, Renu Bala "*Spectrum of Cloud Computing Architecture: Adoption and Avoidance Issues*", International Journal of Computing and Business Research, Volume 2, Issue 2, May 2011.

[15] Godse, M., and Mulik, S. 2009, "An Approach for Selecting Software-as-a-Service (SaaS) Product," In Proc. of IEEE International Conference on Cloud Computing, pp.155-158.

[16] 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.

[17] Kuyoro S. O., Ibikunle F. & Awodele O, "*Cloud Computing Security Issues and Challenges*", International Journal of Computer Networks (IJCN), Volume 3, Issue 5, pp 247-255, 2011.

[18] Song Dawn, Shi Elaine "*Cloud Data Protection for the Masses*"IEEE Computer Society, 2012.

