Open access Journal International Journal of Emerging Trends in Science and Technology

To Enhance Homomorphic Encryption scheme for Key Management and Key Sharing in Cloud Computing

Author
Preeti Ahuja

Punjabi University Regional Centre for I.T. and Mgmt
Mohali, India
Email*: Preetiahuja_2411@yahoo.com*

Abstract:
The cloud can offer services to the users at lower cost and services are available at anytime, anywhere, user data security is the main challenge in cloud computing. The data encryption is the best way for providing data security in cloud computing. Fully homomorphic encryption scheme is reliable and secure encryption technique. The main problem with fully disk encryption scheme is key management, key storage and data aggregation. To solve the problem of key management and key sharing various schemes are proposed in last few years. The third party auditor is the scheme for key management and key sharing. The third party auditor scheme will be failed if the third party's security is compromised or third party will be malicious. Cloud computing is very latest technology which is widely used in these days. There are some security threats in this network. The proposed scheme is used to provide security to the cloud so that attacker will unable to hack the information using Diffie- Hellman key exchange protocol. . In Diffie -Hellman algorithm, there is no provision for the storage or exchange of the PIN key. So it protects network devices from attacks.

Keywords: Cloud computing, IaaS, PaaS, SaaS, Diffie Hellman key exchange algorithm.

1. Introduction

Cloud computing is an innovative service mode [1]. Many trends are opening up the era of Cloud Computing, which is an Internet–based development and use of technology. It takes virtual infrastructure and builds upon research in distributed computing, grid computing, utility computing, autonomic computing, networking, web services and software services. It has shown tremendous potential to empowerment, agility, multi-tenancy, reliability, scalability, availability, performance, security and maintenance. 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. 'Cloud' is derived from the cloud shaped symbol used to denote a network in typical system diagrams. Cloud computing involves utilizing of shared services in terms of both hardware and applications. This concept based on the time-sharing of costly resources and advantages of the economies of scale. Cloud computing employs multiple servers networked with specialized connections to distribute tasks pertaining to data processing amongst them. The common or pooled infrastructures contain a large number of systems that linked together. End-users access the cloud through networked client devices. A large number of these cloud clients employ centralized servers for most of their applications [2].

Example, Dropbox is a service of cloud where any user either with premium account (account with some extra features) or free account can use their cloud. There is one problem exist with it, that is any user can access any other user's data without the knowledge of other user. Now the question arises that how we can prevent these kinds of issues. Standard enterprise security (such as firewall and antivirus) is adopted by organizations to ensure the security for cloud computing. As the defense against the malicious services or services like identity frauds, almost all service provider organizations use the access control and user authentication mechanisms. The best feature mostly cloud service providers are providing is user can access the cloud from anywhere in the world. To secure the user data, enterprises use the security mechanism, such as USB port control and Full Disk Encryption (FDE). But, are these mechanisms are good enough to secure the user data in cloud? The systems which runs 24*7 or all the time the above solutions are not effective that much. They cannot prevent the attackers to access data. Encryption is the only effective way to maintain the privacy and which provides the security in cloud computing.

2. Background

The most widely used definition of the cloud computing model is introduced by National Institute of Standard Technology as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or services provider interaction [3],[4]."

2.1 Cloud Computing Service Models

Cloud Software as a Service (SaaS): Application and Information clouds, Use provider's applications over a network, cloud provider examples Zoho, Salesforce.com, Google Apps.

Cloud Platform as a Service (PaaS): Development clouds, Deploy customer-created applications to a cloud, cloud provider examples Windows Azure, Google App Engine, Aptana Cloud.

Cloud Infrastructure as a Service (IaaS): Infrastructure clouds, Rent processing, storage, network capacity, and other fundamental computing resources, Dropbox, Amazon Web Services, Mozy, Akamai [5].

2.2 Cloud Computing Deployment Models

Private cloud: Enterprise owned or leased.

Public cloud: Sold to the public, mega-scale infrastructure.

Hybrid cloud: Composition of two or more clouds [5].

2.3 Fully homomorphic Encryption

Fully Homomorphic encryption (FHE) is applied on each function. The cipher text and plain text is not related but the emphasis is on the algebraic operation that works on both of them. After the invention of RSA, Rivest, Adleman and Dertouzos introduce the idea of fully Homomorphic schemes. They asked for an encryption function that permits encrypted data to be operated on without preliminary decryption of the operands, and they called those schemes privacy homomorphism [31].

Fully Homomorphic Encryption can be used to inquiry a search engine, not including, what is being searched. More accurately, FHE has the many properties. Assume that cipher text ci decrypt to plaintexts mi.

Therefore,

Decrypt (ci) = mi

Where the mi's and ci's are elements of some ring with two operations, addition and multiplication. In FHE one has

Decrypt (c1 + c2) = m1 + m2;

Decrypt (c1 * c2) = m1 * m2

Homomorphic Encryption systems are used to execute operations on encrypted data without knowing the private key, the client is the only holder of the secret key. When we decrypt the result of some operation, it is the similar as if we had approved out the calculation on the raw data [6].

2.4 Diffie-Hellmann Key Exchange

In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to exchange data, both agree on a symmetric key. Symmetric key is used for encryption or decryption the messages. We knows that Diffie Hellman algorithm is used for only key agreement or key exchange, but it does not used for encryption or decryption. Before starting the communication, secure channel is established. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established [7].

3. Existing System

At the very lower cost, cloud provides the services which can be accessible all the time, anywhere, anytime. User data privacy is the key challenge in cloud computing. Encryption is the only effective way to maintain the privacy and which provides the security in cloud computing.

In the existing system firstly a scenario is created with a head node and the fixed number of sub nodes. The data is encrypted using homomorphic encryption. The keys used for encryption are stored by the third party. The third party auditor is the scheme used for key management and key sharing. The main advantage of this is 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 auditing scheme will be failed, if the third party's security is compromised or of the third party will be malicious.

4. Proposed System

This study is mainly focused on to develop modal for fully homomorphism disk encryption schemes. The new scheme will provide reliable key storage and key management services. This will enhance the reliability and security of the existing fully homomorphism encryption scheme.

In this new modal, secure channel establishment algorithm will used for key management and key sharing. The secure channel establishment algorithms are Diffie- Hellman and RSA. The Diffie- Hellman algorithm is most secure and reliable algorithm.

In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to exchange data. Before starting the communication, secure channel is established. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

The Diffie Hellman key exchange algorithm is embedded for the authentication procedure. In cloud network, it defines the source node and destination node. To establish secure channel between communicating parties, each party select a random prime number g and n, selected numbers become public keys of both parties.

The source node become master and destination node become slave, master and slave select their private keys 'a', 'b' respectively.

The master calculates new value "M" from their selected public and private numbers.

M= ga mod n

The Slave calculates new value "S" from their selected public and private numbers

S= gb mod n

The Master and slave exchange their calculated "M" and "S" values through intermediate nodes. When Slave receives "M" and Master receives "S" both parties will calculate mode inverse value.

When master receive value "S" from slave and calculate new value "K1" from the received "S" value.

K1=Sa mod n

Slave receives value "M" from master and calculates new value"K2" from the received "M"

K2=Mb mod n

After calculating "K1" and "K2", both parties establish secure channel, by calculated new key "K". If both communicating parties have same "K1" and

"K2" values, secure channel is established between Master and Slave.

K=K1+K2

When secure channel is established between master and slave, communication starts between both parties. The communication between Master and Slave is encrypted with public keys. Each parties use their own private keys to decrypt the communication.

5. Results

A network is deployed by creating a head node and fixed number of sub nodes. The proposed enhancement in cloud data security has been implemented in MATLAB. The proposed scheme is compared with the existing technique based on the factors delay, throughput, energy and resources used.

5.1 Comparison Graph of Delay

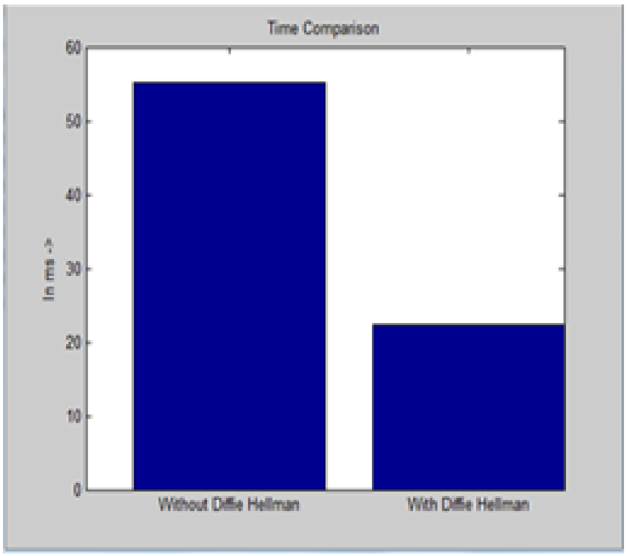

Figure 1: Comparison graph of delay

Figure 1 shows the comparison in terms of delay between the existing and proposed approach. The delay in the previous technique is more than the existing technique.

5.2 Comparison Graph of Energy

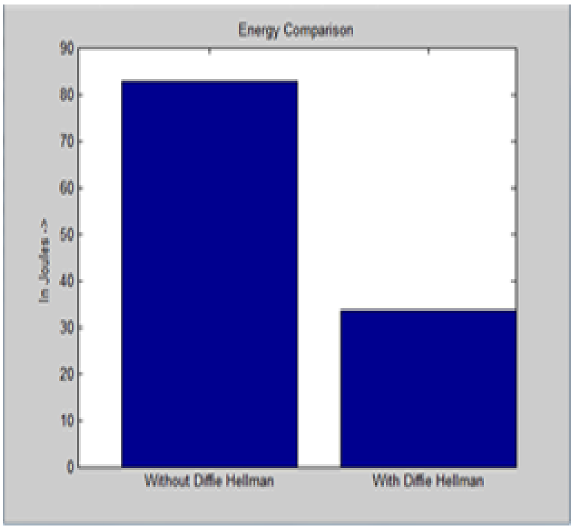

Figure 2: Comparison graph of energy

Figure 2 shows the energy consumption in the proposed and the existing technique. The proposed technique takes less energy than the existing technique so it is more efficient technique.

5.3 Comparison Graph of Throughput

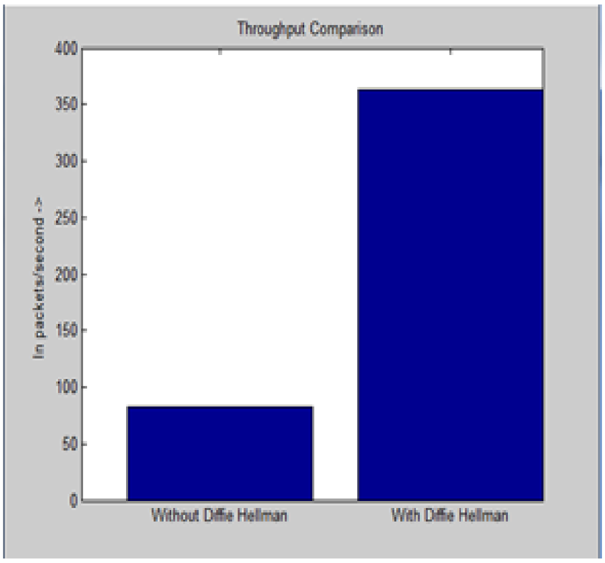

Figure 3: Comparison graph of Throughput

Figure 3 shows the throughput of proposed and existing technique. The throughput of the proposed technique is more as compared to the existing technique.

5.4 Comparison Graph of Resources Used

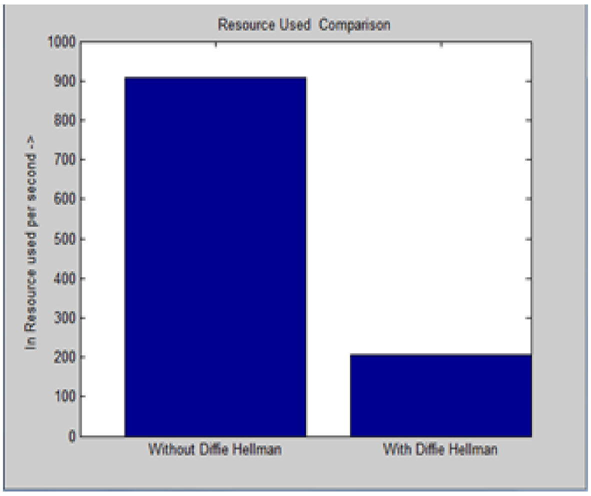

Figure 4: Comparison graph of Resources Used

Figure 4 shows that the resources used in the existing technique are more as compare to the proposed technique. The proposed technique is better than the existing technique.

6. Conclusion

Cloud computing is relatively a new concept which provides users with a large number of benefits. However cloud computing also has some pros mainly the security problems. Security problems can be solved by using encryption schemes. In this dissertation various security issues has been discussed associated with the cloud computing.

In this dissertation, we conclude that FHE offers more data security to the cloud. But there are some security issues which arise in FHE. The main motive behind this research is to propose a solution for key management and sharing in FHE. To provide security a technique has been proposed using Diffie-Hellmann approach.

Apart from designing the proposed solution, its implementation is done using MATLAB. In order to reflect the efficiency of the proposed technique in comparison to the existing technique, performance analysis has been done on the basis of delay, throughput, resources used and energy consumed. The outcome is graphically reflected and thoroughly discussed. The proposed technique is more efficient as compare to the existing technique.

References

1. Feng Zhao, Chao Li, Chun Feng Liu, “A cloud computing security solution based on fully homomorphic encryption,” International Conference on Advanced Computing Technology, pp. 485–488, 2014.
2. Suneel Wattal and Ajay Kumar, “Cloud Computing - an Emerging Trend in Information Technology,” International Conference on Issues and Challenges in Intelligent Computing Techniques, pp. 168-173, 2014.
3. Rajkumar Chalse, Ashwin Selokar and Arun Katara, “A New Technique of Data Integrity for Analysis of the Cloud Computing Security,” 5th International Conference on Computational Intelligence and Communication Networks, pp. 469-473, 2013.
4. M. Sugumaran, BalaMurugan. B and D. Kamalraj, “An Architecture for Data Security in Cloud Computing,” World Congress on Computing and Communication Technologies, pp. 252-255, 2014.
5. Eman M.Mohamed and Hatem S. Abdelkader, “Enhanced Data Security Model for Cloud Computing,” 8th International Conference on Informatics and Systems, 2012.
6. K. Rubin and A. Silverberg, A report on Wiles’ Cambridge lectures, Bulletin of the American Mathematical Society, pp. 15-38, 1994.
7. Kou-Min Cheng, Ting-Yi Chang, and Jung-Wen Lo, “Cryptanalysis of Security Enhancement for a Modified Authenticated Key Agreement Protocol,” International Journal of Network Security, vol. 11, no.1, pp.55, 2010.

Author Profile

Preeti Ahuja received the B.Tech. degree in Computer Science and Engineering from University College of Engineering, Punjabi University, Patiala, Punjab, India in 2012. She is currently pursuing M.Tech from Punjabi University Regional Center of I.T. and Mgmt., Mohali, India.