I.J. Information Engineering and Electronic Business, 2016, 3, 31-40
Published Online May 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2016.03.04

Two Level Hybrid SECO Environment for Secure Cloud Environment

Manpreet kaur
Research Scholar, CGC, Landran Mohali, Punjab
E-mail: Cutemani.shergill@gmail.com

Hardeep Singh
Assistant Professor at CGC, Landran Mohali, Punjab
E-mail: Cgccoe.cse.hardeep@gmail.com

Abstract—As cloud computing becomes prevalent, sensitive information are being increasingly centralized into the cloud. Number of users used cloud to store their data. In general terms means encrypted form hackers can easily hack or modify the data because there is no security while uploading the data to cloud server. Due to this problem cloud server can easily deployed. As security is one of the major concerns in cloud environment for preventing data deployment during upload. The best solution for the protection of data privacy is done by encryption the sensitive data before being outsourced to cloud server, which makes effective data utilization a very challenging task. There are a number of security and privacy concerns associated with cloud computing but these issues fall into two broad categories: security and privacy concerns faced by cloud providers and security and privacy concerns faced by their customers. Different set of algorithms have been implemented on cloud environment for enhancing the security but still there are some major concerns like malicious attacks. In previous work on AES based encryption and a SECO based environment were introduced.. In SECO based environment root package generated key by using diffie-hellman algorithm and domain package generated key by using private key of root package. In AES algorithm and SECO based environment individually provided some sort of level encryption. In this both algorithms work on single level encryption approach which may be easily broken by malicious users. So, in proposed work both techniques that is AES and SECO based environment will be combined to provide two level security and also will double the encrypted environment which may not be easily broken by malicious users. Result will be more efficient and secure than the previous work.

Index Terms—Cloud computing, content security, AES algoritm, Diffie-hellman algorithm, Digital Signature, Window Azure.

I. Introduction

Cloud computing is growing fast with time. With the dramatic increase in storage of data over cloud. The term "Cloud Computing" is the computing services in Information Technology like infrastructure, platforms, or applications could be arranged and used through the internet. Infrastructure upon which cloud is built upon is a large scaled distributed infrastructure in which shared pool of resources are generally virtualized, and services which are offered are distributed to clients in terms of virtual machines, deployment environment, or software. Hence it can be easily concluded that according to the requirements and current workloads, the services of cloud could be scaled dynamically. As many resources are used, they are measured and then the payment is made on the basis of consumption of those resources.

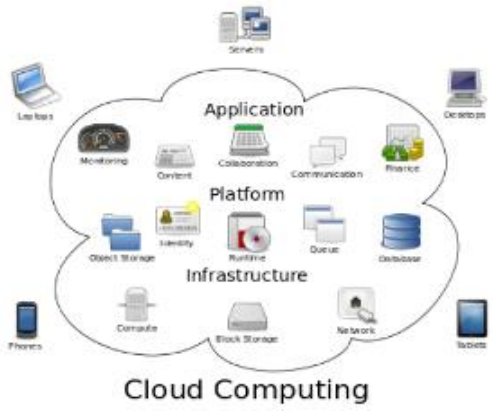

Fig.1. Structure of Cloud Computing

According to the definition of[8], cloud computing is "it is a significant distributed computing model that is directed by financial prudence of balance, in which stake of isolate, fundamental, loading, podium in which a facilities are supplied as per the request of exterior foreign clients through the internet". There are some examples of cloud services like webmail, online file and business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Firstly, cloud facilities are enormous extensible and the procurement and clemency of these benefits (services) could be done dynamically with minimum practical (operational) backing required. Secondly, the price is charged on a usage support and the

condition of cloud service, such as privacy and capability, and authorize basically on opportunity of web and how basic resources are achieved and disburse to customers. The major focus of cloud computing is that clients only use what they want and apart pay for what they actually used. Sources are accessible to be executable from the cloud at any time from any place via web. There is no demand to take tension about how different items are being used behind the scenes. In this client can easily buy the IT assistance as they want any other utility. The main reason is that cloud computing has also been known as utility computing. On internet there is the delivery of computing services in Cloud Computing. At remote locations every individual and businesses use hardware and software that are managed by third parties and are provided by cloud services. There are some examples of cloud services like webmail, online file and business applications. From anywhere if network connection is available only then cloud computing model allow access to information and computer resources. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

1.1 Cloud Deployment Model

Cloud computing has mainly three types that is public cloud, private and hybrid cloud.

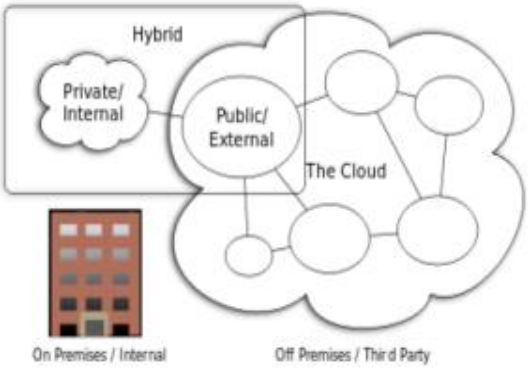

Fig.2. Cloud Deployment Model

Public cloud: public cloud describes the conventional meaning of cloud computing that is accessible, effective ways and means, which are accessible on internet from a minor party, which detached assets and charges its clients on the basis of utility. Cloud organization is possessed and accomplish by a supplier who suggest its retune to public domain. E.g. Google, Amazon, Microsoft offers cloud services via Internet. There are different benefits of public cloud model.

Private Cloud: Private cloud is a term used to donate a proprietary computing architecture provisioned services on corporate networks. Big enterprises usually used this type of cloud computing to permit their private network and information Centre administrators to effectively become in-house 'service providers' catering to

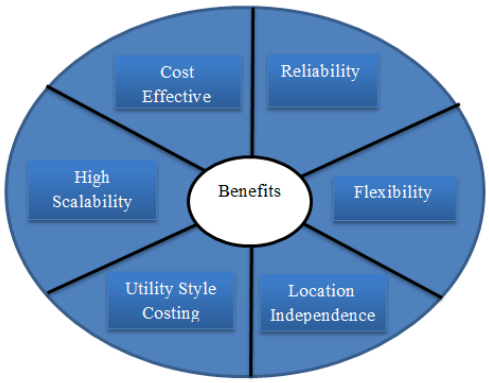

Fig.3. Benefits of Public Cloud

customers within the corporation. Cloud organization is establishing for a particular aggregation and managed by a third party under a service level agreement. Only single organization preferred to operate via corporate cloud. There are advantages (benefits) of internal cloud model.

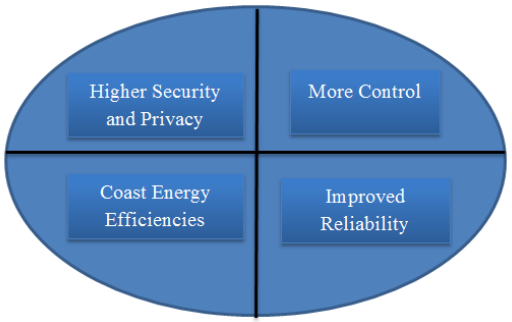

Fig.4. Benefits of Private Cloud

Hybrid Cloud: A hybrid cloud comprises assets from both corporate and public providers will definitely become the demanded choice for enterprises. The hybrid cloud is a combination of both corporate cloud and public cloud.. For example, for general computing enterprise could selects to make usage of external services, and its own data Centre's comprises it own data Centre's. Hybrid cloud model has number of advantages (benefits).

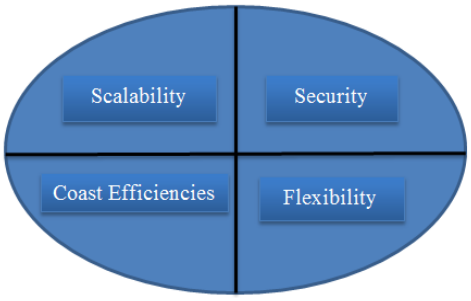

Fig.5. Benefits of Hybrid Cloud

1.2 Cloud Service Model

Cloud computing offers three fundamental service models that is [27] Infrastructure as a service, Platform as a service and Software as a service:

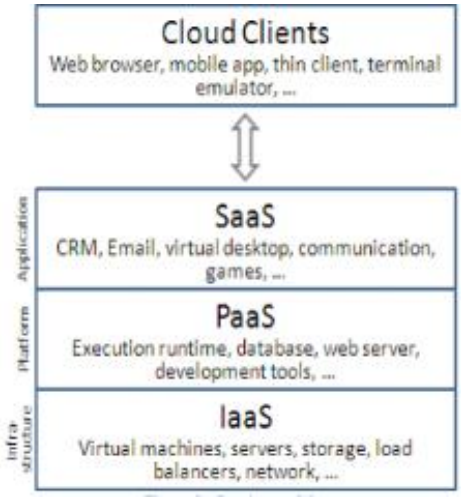

Fig.6. Service Models

Cloud Infrastructure as a service (IaaS): In this composition of implemented environment for their system a supplier must be supply a different computing resources which include loading, processing unit. Client has flexile to achieve and switches software mutilated to be implemented and vary between different applications like operating system etc.

Cloud Platform as a service (PaaS): This software supplies client with the ability to establish and extended applications that are mainly positioned on equipment and programming languages promoted by the suppliers. In this the client has no containment over the different organization but has containment over the extended applications. Examples of this class of services include Google App Engine, Windows Azure Platform and rack space.

Types of PaaS: There are different types of PaaS such as

- Application Delivers only Environments
- Standalone Developments Environments
- Open Platform & Open Service
- Add on Development Possibility

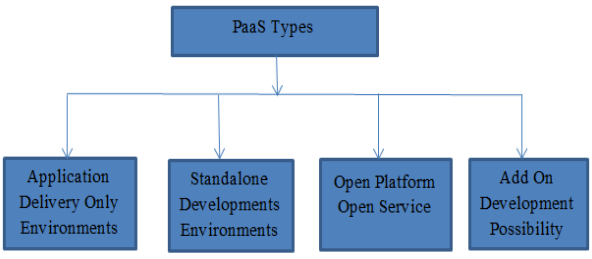

Fig.7. Types of PaaS

Cloud Software as a service (SaaS): This software supplies the ability to usage the appliances which implemented on cloud organization. With the usage of standard interfaces like web browser or online (e-mail) client, these appliances are obtainable. SaaS appliances are obtained from different devices like mobile, workstation from anywhere at any time.

Cloud Network as a service (NaaS): NaaS provides the capability to use the network services and inter-cloud network connectivity services. Improvement of possession allocation services include in view of network and computing resources. These type of services involved extensible, enhanced virtual private network.

II. Major Risk of Cloud Computing Security

There are a lot of security issues in cloud computing service environments such as virtualization, distributed big data processing, serviceability, traffic-handling, application security, access control, authentication, cryptography and etc. Especially, data access using various resources needs user authentication and access control model for integrated management and control in cloud computing environments.

Cloud computing security is a hot topic for research, its freshness, interestingness and recognition created an appeal for researches to pursue this topic in specific. Many security concerns evolved while weighing the benefits of using cloud computing over local resources. Below are the major risks introduced by the cloud are:

- Data Storage
- Legal and Regulatory Risks
- Privacy and Confidentiality
- Availability
- Integrity
- Computationally feasible
- Proper usage metering
- Internal and external attacks
- Abusing cloud's resources

1. Data Issues

Whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data.

Data stealing is a one of serious issue [17] in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server.

Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire.

Solution: "Data protection in cloud computing is very important factor it could be complicated for the cloud customer to efficiently check the behaviour of the cloud supplier and as a result he is confident that data is handled. Also very efficient data integrity method [15] in cloud computing."

2. Privacy Issues

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

Solution: "Authentication [7] is a best solution for the privacy issue. Authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet."

3. Infected Application

Any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

Solution: "To prevent [9] cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server."

4. Security Issues

Cloud computing security must be done on two levels. One is on provider level and another is on user level. The user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action.

Solution: "Cloud computing service provider should make sure that the server is well secured [16] from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user. A cloud is good only when there is a good security provided by the service provider to the user."

5. Trust Issues

Trust is very necessary aspect in business. Still cloud is failed to make trust between customer and provider. So the vendor uses this marvelous application should make trust. Weak trust relationship and lack of customer trust cause many problems during deployment of cloud services.

III. Security In Cloud Computing

Diffie Hellman Algorithm: Diffie Hellman was the first key algorithm ever invented, in 1976. Diffie Hellman key agreement protocol is [3]:

Exponential key agreement
Allows two users to exchange a secret key
Requires no prior secrets
Real-time over an untrusted network

Definition of Diffie Hellman: Let n be a prime number and p be an integer. The Diffie Hellman Problem (DHP) is the problem of computing the value of p^{ab} (mod n) from the known values of p^a (mod n) and p^b (mod n). The setup of Diffie Hellman algorithm

- Suppose we have two parties Master and Slave, they want to communicate to each other.
- They do not want the eavesdropper to know their message.
- Alice and Bob agree upon and make public two numbers n and p, where n is a prime number and p is a primitive root mod n. Anyone has access to these numbers.
- Public exchange of values.
- Masters sends M to slave==M
- S= Slave sends S to Master

Table 1. Private Computations

Master	Slave
Choose a secret number a. Compute $M = p^a (mod\ n)$	Choose a secret number b. Compute $S = p^b (mod\ n)$

- Master compute the number= $s^a = (P)^b (mod\ n)$.
- Bob compute the number $K = M^b = (p^b)^a (mod\ n)$

Here Master and Slave have the same key that is K=p^{ab} (mod n).

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. 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 [3]. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

Figure 8, shows that Master and Slave wants to communicate with each other. To start communication both parties need to establish secure channel. To establish secure channel, two random prime numbers p and n are selected, both devices are agreed on these two numbers. Selected p and n are the public numbers. Both parties, say device 1 become master and device 2 become slave, both master and slave select their private numbers a' and 'b' respectively. Master and slave use their public and private number and calculated their private keys [22].

From M, slave computes:

$$K2=M^b \bmod n$$

If both master and slave calculate same values of K1 and K2, then secure channel is established between them. The combination of KI and K2 becomes the shared symmetric key between master and slave.

To encrypt the messages, they used the public key or shared key (k) of both parties. For decryption of messages private key of both parties which is randomly chosen by the users i.e. 'a' and 'b' are used [11].

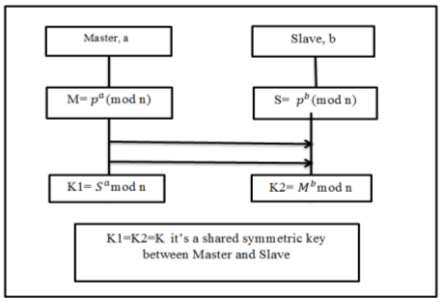

Fig.8. Diffie Hellman Key Exchange

Advanced Encryption Standard: Two Belgian cryptographers Joan Daemen and vincient Rijmen, developed AES algorithm in 1998. AES is a secret key encryption algorithm which operates on a fixed block size of 128 bits, but different key lengths that is 128, 192 and 256 bits. The sum of recurrence of conversions rounds that disciple the input called plain text into the final output called the cipher text. Number of repetitions (recurrence) of transformation (conversions) rounds that convert (disciple) the input called plain text into the final output called the cipher text.

The sum of revolution of recurrence is as follows:

10 cycles of repetition for 128 bits.
12 cycles of repetition for 192 bits.
14 cycles of repetition for 256 bits.

Each round consists of several processing steps. In this total number of reversible rounds are applied to conversion cipher text into the plain text with the usage of encryption key. The basic steps of AES algorithm are stated as:

Key Expansions
Initial Rounds
Rounds
Final Round
Key Generation

Key Expansions: In this round keys are derived from cipher keys. AES requires a separate 128 bits keys plus one more key.

Initial Round: In this add round key is used which is explained further:

Add Round key: In this each byte of the state is connected with block of the round key using bit wise XOR.

Rounds: In this three different steps are used that is sub-bytes, shift rows and mix columns.

- **Sub-bytes:** A non-linear substitutions steps where individual eight bits is change with another on the basis of look up table.
- **Shift Rows:** A transposition step where each row of the state is shifted cyclically a certain number of steps.
- **Mix Columns:** A mixing application which applicants on the columns of the state, connected the four bytes in individual column.
- **Add Round key:** In this individual eight bit of the state is connected with block of the round key using bit wise XOR.

Final Round: In this all steps are same as round except mix columns.

Key Generation: This module handles key generation by the cryptographic module at client side. The server developed unique keys for clients once they authenticate themselves with the server. The key is developed using instances of AES key generator class. This key is then changed to the cloud client via the mail-server through a mail which receives and saves a duplicate copy for it for decrypting purpose.

IV. Related Work

Dong et al.[9] described the one major issue is that how to authorize a private information association assistance along with information access and update in cloud computing. In the proposed work, a private and adequate information association scheme is SECO. In this, they apply a two level hierarchical identity based encryption (HIBE) to guarantee information privacy against unauthorized cloud. Song et al. [28] proposed that practical techniques for searches on encrypted data. In this to minimize the privacy and security risk data is store in encrypted form on data storage server such as mail server and file servers. This technique had number of crucial advantages. They were almost private and they granted almost privacy for encryption, means that the unauthorized client could not know about the plain text, when they only provided the cipher text. In this they given query isolation for researches, in the sense that unauthorized client could not know a little bit more information about the plain text then they research conclusion, as they given composed researching, so that the unauthorized client could not research for an arbitrary word without the user authorization, they also supported hidden queries so that the user may asked the unauthorized client to research for a private word without depicting the word to the server. Neha Jain et al.[19] presented a data security system in cloud computing using DES algorithm. This Cipher Block Chaining system is to be secure for clients and server. The conclusion is that in the order to be private the structure the conversation between modules is encrypted with the usage of symmetric key. Cong Wang et al.[6] described that the major focus on the privacy of cloud data storage. Additionally, it is a major aspect of quality of assistance to assure the exactness of clients information in the cloud. In proposed work, new technique supports private and feasible dynamic operations on information blocks which includes information update, delete and append. Huge privacy and result analysis depicts that the new technique is much feasible and strong against byzantine failure, unauthorized information modification attack. Bala Chandra et al. [1] described that to provide some vendor assertion in SLA to satisfy the user on privacy issues. Service level agreements (SLA) reveals various stages of

privacy and their problems based on the services to make the client learn the privacy policies that are being done. Moreover, it can be beneficial for some organization to look forward in usage of the cloud services. Meiko Jensen et al.[22] describes several problems of Cloud Computing and tries to solve them. Section one introduces the history of Cloud Computing and outlines the concept of Cloud Computing. Section two and three describe three kinds of main Cloud Security problems and propose several methods to solve them. A summary of the whole paper is presented in section four. Cheng et al[5] described cryptanalytic of privacy enlargement for a customize verified key agreement protocol. This paper demonstrates the previous distribute password to agreement a same session key via insecure network. It also shows that technique is also deteriorate from the rearward reaction assault on the off-line password guessing attack. Bellare et al. [2] presented as-strong-as-possible definitions for security and construction achieving them for public key encryption techniques. It is happened only where encryption algorithm is acceptance. One construct is called RSA-DOAEP. It has the combined characteristic of being length maintaining. This is the reason that it is first example of public key cipher. This work focussed on obtaining efficiently-searchable encryption which permits more flexible security to research time trade-offs via scheme is called bucketization. Ritu pahal et al.[27] described the quick advancement of digital information conversion in electronic method. In this data privacy is enhancing more important in information storage and transmission. Two types of cryptographic techniques are being used: symmetric and asymmetric. This paper used symmetric cryptographic technique advance encryption standard (AES) which having 200 bit blocks same as key size. Rohini et al. [20] discussed Communication is the medium for sending and receiving the data between two parties i.e. Sender and receiver but communication needs the security from unauthorized people. Security covers a variety of computer networks that are used in every day. For more security, we use Diffie – Hellman algorithm. Our proposed work provides better security and implemented in any network. We have enhanced the hardness of security by DH algorithm. The DH algorithm is improved by adding codes to the algorithm. Rameshwari Malik et al.[21] discussed the Security is often cited as one of the most contentious issues in Cloud computing. The future of cloud, specifically in advancement the number of appliances, which add much deeper degree of security and authorization. In proposed work, information saved model where information is encrypted with the usage of AES and verified by Diffie Hellman algorithm before it is dispatch in the cloud. Thus assuring information privacy and confidentiality

V. Proposed Scheme to enhance Security in Cloud Computing

Data storage in Cloud Computing reached to very high level. So security is the need of the Cloud Environment. This enhanced scheme is used AES and SECO algorithm to encrypt the data. Firstly, both algorithms are individually used to encrypt the data, but this type of security can be easily hacked by unauthenticated users.This scheme is proposed to enhance the security in cloud data storage systems. Security can be easily hacked by hackers when both the algorithms individually provide some form of encryption. So, in proposed work both techniques that is AES and SECO based environment will be combined to provide two level security and also will double the encrypted environment which may not be easily broken by malicious users.

The simulation tool which is used in this work is visual studio 2010. The whole web based work is done in visual studio. To create the cloud environment Microsoft window azure is used.

This paper focus on the following parameters:

- Data Loss
- Attack Acceptance & Rejection
- Security Enhancement

SECO environment used in this to achieve the following objectives:

- To generate Secure cloud environment.
- To implement AES architecture on cloud.
- To implement SECO architecture on cloud.
- To implement double encrypted environment on SECO environment using AES.
- To enhance the security level and evaluate on the basis of efficiency in security.

In this proposed work, admin has a single duty that is to make restrictions over number of transactions per user as per his role. After login, the user can upload the text or image data only if they have any transaction left. When user upload any type of data then it is saved at window azure cloud in encrypted form locked with digital .signature.

a. Basic Block Design

Data Storage in Cloud Computing reached to very high level so; security is the need of the Cloud Environment. This proposed enhanced scheme use AES & SECO Encoding schemes and add signatures to lock the data for more security.

The basic design of the system is shown in the figure 4. In this data is uploaded on the cloud server. By using diffie hellman algorithm root package generate a key and the encryption occur on that key with the help of AES algorithm. On that key, both the algorithms occur step by step that is why it is known as a SECO environment by using hierarchal identification based encryption (HIBE). After that, domain package generate master key by using encrypted private key of root package. On that master key again AES algorithm encryption occurs that encrypted data is known as one level encryption. Moreover, on encrypted data again AES encryption occur then that encrypted data is known as a two level encryption and

created 2- Level SECO environment. If malicious user attack on this two level environment then more secure and efficient results occur.

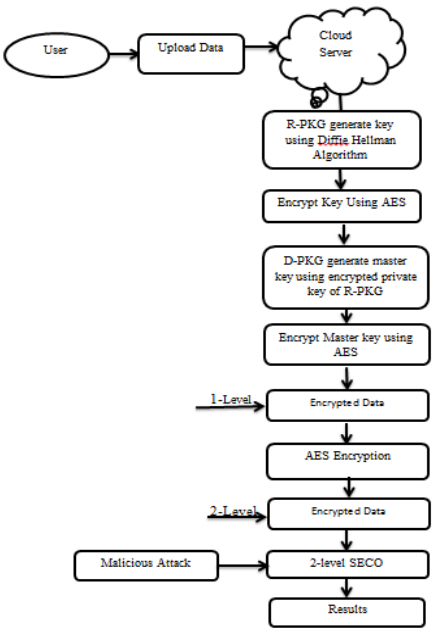

Fig.9. Basic Block Design of Proposed Work

Two Level Hybrid SECO Environment

Step 1: Initialization
Step 2: Upload the data on cloud server.
Step 3: By using diffie hellman algorithm root package generate key.
Step 4: Encryption occur on root package key by using AES algorithm
Step 5: Domain package generated key by using private key of root package
Step 6: One level encryption done by encrypting master key with usage of AES algorithm.
Step 7: Two level encryption done by encrypting the one level data with the usage of AES algorithm.
Step 8: Two level SECO environment.

SECO environment use the advantage of both Diffie hellman and AES algorithm. Both the algorithms are applied simultaneously. It is very easy to break the security of one algorithm but these two algorithms are overcome the each disadvantage. By using these two algorithms, results are more effective and efficient.

Admin: In an organization, admin create roles for users & also specify the number of transactions per user as per their role.

User: A user can upload/ download file when uploading file AES & SECO. Encoding schemes are used to encrypt data & digital signature is included to lock that data and when downloading file inverse AES & SECO are used to decrypt data & digital signature is used to unlock the file.

Window Azure: Window Azure Cloud is used to store data in the encrypted form.

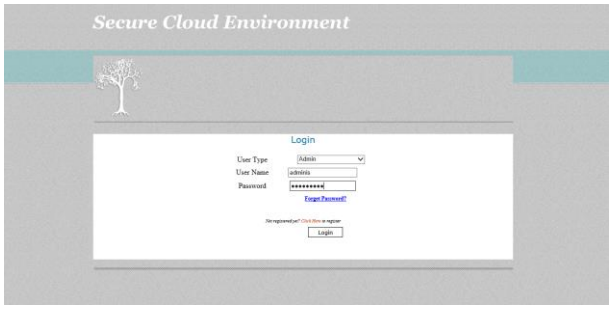

Fig.10. Admin Page

Results & Discussions

Case Study 1 (Data Loss): Let us consider, Total no. Of users in cloud= 20 named as user1, user 2, so on upto user20 respectively.

All the users saved their information to cloud using both HIBE & 2-level HIBE architecture.

Out of 20 users, accounts of 13 users have been hacked by malicious users that mean 13 attacks are there under consideration. The following analysis has been done to measure the performance of secure environment.

Table 2. Data Loss per User

Users	Attack Information (Y/N)	Authentication (Y/N)	Data Loss	
			HIBE	2-Level HIBE
192.168.0.1	Y	Y	100%	N
192.168.0.2	N	NA	NA	NA
192.168.0.3	N	NA	NA	NA
192.168.0.4	Y		100%	N
192.168.0.5	N	NA	NA	NA
192.168.0.6	Y	Y	100%	N
192.168.0.7	Y	Y	100%	N
192.168.0.8	N	NA	NA	NA
192.168.0.9	Y	Y	100%	N
192.168.0.10	N	NA	NA	NA
192.168.0.11	Y	Y	100%	N
192.168.0.12	Y	Y	100%	N
192.168.0.13	N	NA	NA	NA
192.168.0.14	Y	Y	100%	N
192.168.0.15	Y	Y	100%	N
192.168.0.16	Y	Y	100%	N
192.168.0.17	Y	Y	100%	N
192.168.0.18	N	NA	NA	NA
192.168.0.19	Y	Y	100%	N
192.168.0.20	Y	Y	100%	N

Acc. To above analysis:

It is clear that when malicious users gets ID & password information then there is 100% chances for loss of information in HIBE but there is no chance in Two level HIBE because data will be accessed only when user have their master key information which sent on the registered mail account while upload data.

In the above analysis 65% attack is on the cloud environment out of 100%.

Total number of users=20
Attack on users=13
%age attack= (13/20)*100=65%

So information/Data Loss in HIBE environment is 65% & in Two level HIBE only 10% chances are there only when registered mail account hacked.

Table 3. Data Loss by HIBE

Data Loss	
HIBE	2-Level HIBE
0.65	10%

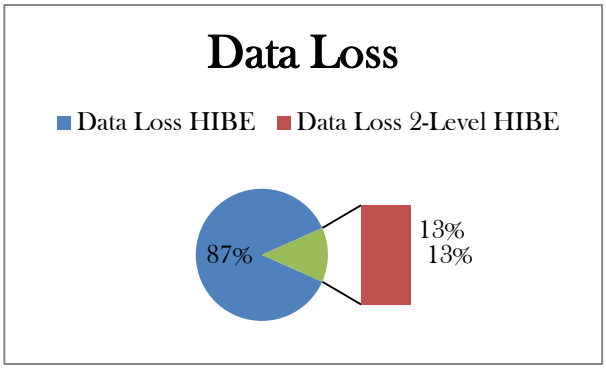

Fig.11. Total Data Loss

Individually Data Loss in HIBE for 20 users

Table 4. Individual Data Loss in HIBE

Users	HIBE
192.168.0.1	100
192.168.0.2	0
192.168.0.3	0
192.168.0.4	100
192.168.0.5	0
192.168.0.6	100
192.168.0.7	100
192.168.0.8	0
192.168.0.9	100
192.168.0.10	0
192.168.0.11	100
192.168.0.12	100
192.168.0.13	0
192.168.0.14	100
192.168.0.15	100
192.168.0.16	100
192.168.0.17	100
192.168.0.18	0
192.168.0.19	100
192.168.0.20	100

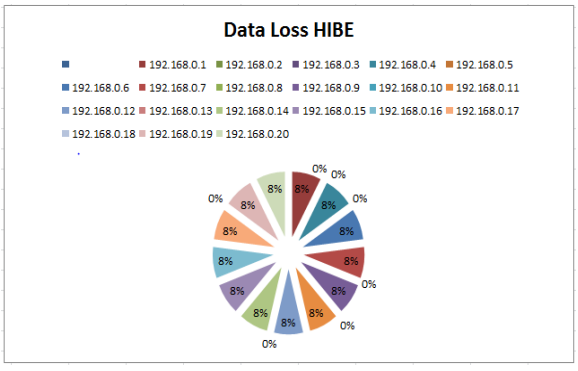

Fig.12. Individual Data loss in HIBE

Case Study 2 (Attacks Acceptance/Rejection Rate):

Let us consider, Total no. Of users in cloud= 20 named as user1, user2, so on upto user20 respectively.

All the users saved their information to cloud using both HIBE & 2-level HIBE architecture.

Out of 20 users, accounts of 13 users have been hacked by malicious users that mean 13 attacks are there under consideration. The following analysis has been done to measure the performance of secure environment.

Table 5. Attack Acceptance Rate per User

Users	Attack Information (Y/N)	Authentication HIBE (Y/N)	Authentication 2- Level HIBE (Y/N)
user 1	Y	Y	N
user 2	N	NA	NA
user 3	N	NA	NA
user 4	Y	Y	Y
user 5	N	NA	NA
user 6	Y	Y	Y
user 7	Y	Y	Y
user 8	N	NA	NA
user 9	Y	Y	N
user 10	N	NA	NA
user 11	Y	Y	Y
user 12	Y	Y	N
user 13	N	NA	NA
user 14	Y	Y	N
user 15	Y	Y	N
user 16	Y	Y	Y
user 17	Y	Y	N
user 18	N	NA	NA
user 19	Y	Y	N
user 20	Y	Y	N

Acceptance Rate:

The above table analyze that out of 13 attacks HIBE architecture accepts 13 attacks but 2-level HIBE accepts only 5 attacks.

Total number of users=20
Attack on users=13
%age attack= (13/20)*100=65%
%age attacks accepted in HIBE= (13/13)*100 = 100%
%age attacks accepted in 2-level HIBE= (5/13)*100= 38.5%

Fig.13. Overall Attack Acceptance Rate

Rejection Rate:

The above table analyze that out of 13 attacks HIBE architecture accepts 13 attacks but 2-level HIBE accepts only 5 attacks.

Total number of users=20
Attacks
k on users=13
%age attack= (13/20)*100=65%
%age attacks rejected in HIBE= (0/13)*100 = 0%
%age attacks rejected in 2-level HIBE= (8/13)*100= 61.5%

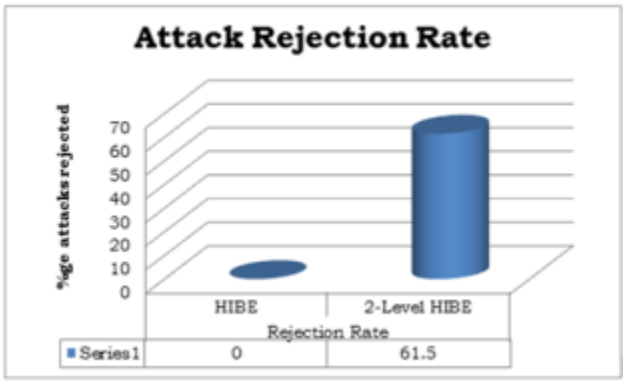

Fig.14. Attack Rejection Rate

Case Study 3 (Security enhancement):

In this individual security enhanced is only 35% but in two level 90% security enhanced. On the basis of it, security is higher than individual ones.

Table 6. Security Enhancement

Security Enhancement	
HIBE	2-Level HIBE
35	90

On the basis of following graph overall security enhanced is 72%

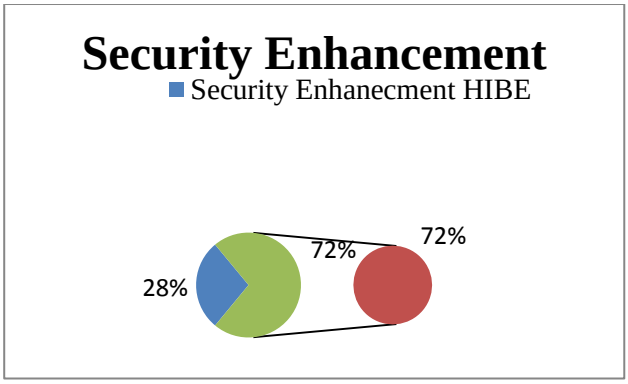

Fig.15. Overall Security Enhancement

Case Study 4 (performance analysis on the basis of time):

Table.7. Performance Time in Milliseconds

Input File Size	HIBE	2- Level HIBE
	Time in milliseconds	
9 KB	265.20	253.60
15 KB	288.33	291.83
30 KB	317.16	321.06
41 KB	380.60	414.96
54 KB	494.77	492.41
89 KB	593.73	597.01
106 KB	771.85	752.51
213 KB	926.22	948.70
289 KB	1204.08	1140.60
500 KB	1685.72	1699.39

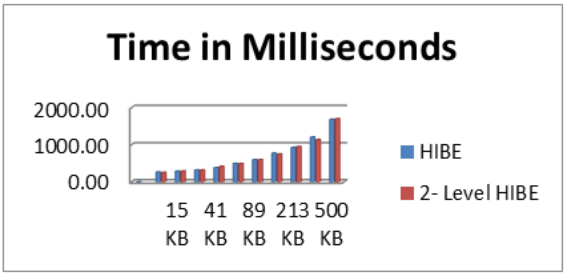

Fig.16. Overall Time in Milliseconds

VI. Conclusion & Future Scope

Security is a major concern in cloud computing. This work introduce a new enhanced server architecture method named as 2-level HIBE architecture for cloud computing. This architecture has been proposed to enhance the security of data stored on the cloud. In this work, data gets double encryption and it is difficult for malicious user to get easily access to cloud user's data until signatures are not matched. So, this architecture is more secure. Result analysis also show that there is less data loss in the 20level HIBE that is in case of HIBE data loss is 87% whereas in new enhanced architecture there is only 13% data loss. The above analysis also shows that the attack acceptance rate of HIBE is 100% whereas 2-level HIBE is only 38.5%. So, it proves that 2-level HIBE architecture can effectively improve the security of user's data on the cloud.

Future work could go in the direction to test and analyze this architecture on real cloud environment, So that the real performance factors will be analyzed.

References

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

[2] Bellare, Mihir, Alexandra Boldyreva, and Adam O'Neill. "Deterministic and efficiently searchable encryption." *Advances in Cryptology-CRYPTO 2007*. Springer Berlin Heidelberg, 2007. 535-552.
[3] Chuah, M., and W. Hu. "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data." *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on*. IEEE, 2011.
[4] C. Dourolis, P. Ramanathan and D. Moore, "what do packet dispersion techniques measures/", In Proc. IEEE INFOCOM, Anchorage, AK pp. 905-914[2001].
[5] Cheng, K.M., chang. T.Y., and Lo J.W., 2010."Cryptanalysis of security enhancement for a Msodified Authenticated Key Agreement Protocol "international Journal of network security, vol. 11, No.1, pp. 55-57.
[6] 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.
[7] D. Brewer and M.Nash "The chinese wall security policy", In proc. Of the symp.on security and privacy, Dakland, CA pp. 215-228. IEEE Press, [1989]
[8] Dr.R.Manicka Chezian and C.bagyalakshmi "a survey on cloud data security Using encryption technique" in International journal of advanced research in computer engineering & technology , Volume 1, Issue 5, July 2012.
[9] Dong Xin, et al. "achieving secure and efficient data collaboration in cloud computing." Quality of service, 2013 IEEE/ACM 21st International symposium on.IEEE, 2013.
[10] Er. Rimmy Chuchra, Lovely Professional University, Phagwara, India, *"Data Security in Cloud Computing"*, International Journal Nov., 2012.
[11] Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360-Degree Compared CoRR. *abs/0901.0131*.
[12] Hassan Takabi, James B. D. Joshi and Gail-JoonAhn**,** *"Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments"* Proceedings of the 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops, p.393-398, July 19-23, 2010.
[13] Hamlen, K. Kantarcioglu, M., Khan, L., and Thuraisingham, B., " Security issues for cloud computing, "International journal of information security & privacy (IJISP), Vol.4, No.2 pp.36-48
[14] http://www.google.com/sens.org/rr/encryption algorithm. php, Diffie Hellman algorithm Rilly Lochridge Algorithm, 2003
[15] J. Brodkin. Gartner: *"Seven cloud-computing security risks",* Infoworld, 2008.
[16] Jianyong Chen, Yang Wang, and Xiaomin Wang, "On demand security Architecture for cloud computing", 0018- 9162/12, published by the IEEE Computer society in 2012.
[17] Jintao Liu, School of Electronics and Computer Science University of Southampton, "Cloud Computing Security", 2009.
[18] John Harauz, Lori M. Kaufman and Bruce Potter, "Data security in the world of cloud computing" published by the IEEE computer and reliability societies in July/August 2009.
[19] Jain, Neha, and Gurpreet Kaur. "Implementing DES Algorithm in cloud for data security." VSRD International Journal of Computer Science & Information Technology 2.4 (2012): 316-321.
[20] JainA, Palak, et al. "An Approach for a Password Encryption Using Dual Server."
[21] Malik, Rameshwari, and Pramod Kumar. "Cloud Computing Security Improvement using Diffie Hellman and AES." International Journal of Computer Applications 118.1 (2015).
[22] Meiko Jensen, JlorgSchwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues In Cloud Computing", IEEE International Conference on Cloud Computing, 2009.
[23] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the Clouds : A Berkeley View of Cloud Computing, 2009.
[24] Nabendu Chaki, "A Survey on Security issue in Cloud Computing" in 6th International conference on Electrical Engineering/Electronics, Computer, Telecommunication and Information Technology, May 2009.
[25] Neela, K., "A survey on security Issues and vulnerabilities on cloud computing", vol.2, No.7, pp.855-860
[26] Nils Gruschka and Meiko Jensen, "Attack surface: A taxonomy for attacks on cloud services" in 2010 IEEE 3rd international conference on cloud computing.
[27] Pahal, Ritu, and Vikas Kumar. "Efficient Implementation of AES." International Journal of Advanced Research in Computer Science and Software Engineering Volume 3 (2013).
[28] Song DX., Wagner D., Perrig A. (2000), "Practical techniques for searches on encrypted data" , Proceedings of IEEE Symposium on Security and Privacy, IEEE, Berkeley, California, pp 44–55.
[29] Vamsee Krishna and Sriram Ramanujam," Data Security in Cloud Computing", Journal of Computer and Mathematical Sciences, vol. 2, Issue 1, 28 February, 2011.
[30] Will Gorner, "Diffie Hellman Key Exchange" ppts.
[31] Xia Z., Zhu Y., Sun X. and Chen L. (2014), "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking "Journal of Cloud Computing", Springer 3.1, pp. 1-11.

Authors' Profiles

Manpreet kaur is pursuing her Masters in computer science and engineering from Chandigarh Group of college (CGC-COE) Landran, Mohali,(Punjab). She received the bachelor of technology degree from BGIET, Sangrur. Her research interests are lies in the field of Cloud Computing. Her current research work is based on the security issues in cloud computing.

Hardeep Singh works as assistant professor in CGC-COE landran Mohali, Punjab. He gives the guidance in this paper. He has completed his masters in computer science & engineering from Baba Banda Singh Bahadur college, Fatehgarh sahib. His research interest are in the fields of software engineering, cloud computing, cyber administration.