**Two Level Hybrid SECO Environment For Secure Cloud Environment**

Manpreet kaur,

Research Scholar, CGC, Landran

Mohali, Punjab

[*Cutemani.shergill@gmail.com*](mailto:Cutemani.shergill@gmail.com)

Hardeep Singh ,

Assistant Professor at CGC, Landran

Mohali, Punjab

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 term a mean 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 algorithm 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. Results will be more efficient and secure than the previous work.**

Keywords- Cloud computing, Content security, AES algorithm, Diffie-Hellmann algorithm, Digital signature, window Azure.

1. 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. 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.

1. **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. The following figure shows some of those benefits:

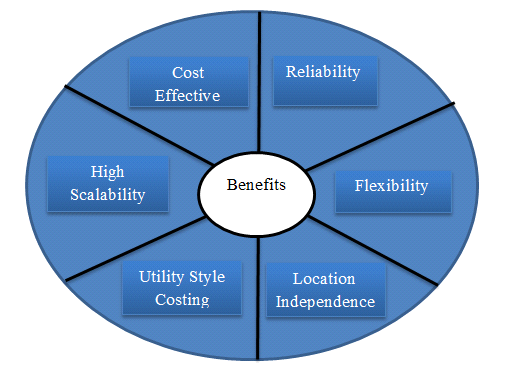


Figure5.1: Benefits of public cloud

**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 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. The diagram given below depicts a few of these advantages (benefits):

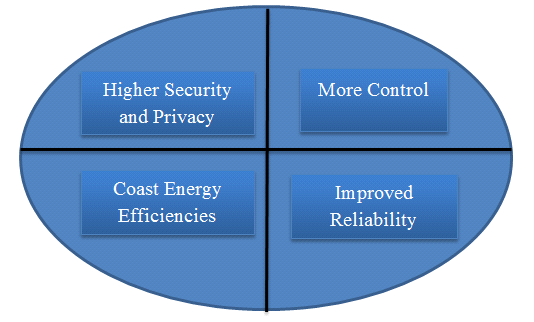


Figure5.2: Benefits of Private cloud

**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).The diagram given below reveals some of those advantages (benefits):

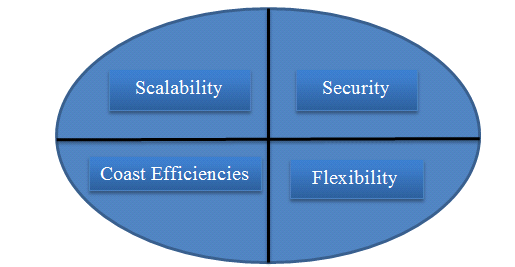


Figure5.3: Benefits of hybrid cloud

**b) Cloud Service Model**

**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. There are different issues in IaaS such as:

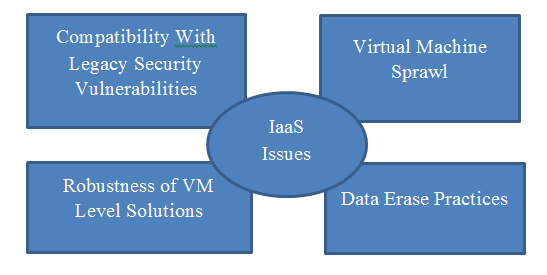


Figure: IaaS Issues

**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. There are different issues in PaaS such as:

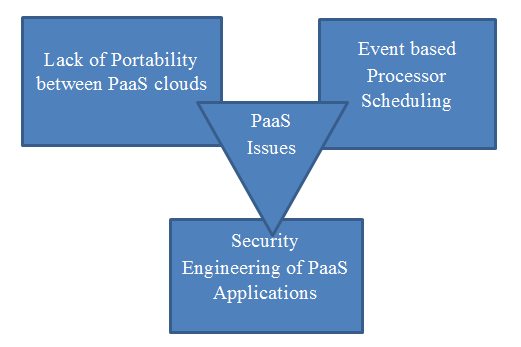


Figure: PaaS Issues

**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.

1. **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:

o Data Storage

o Legal and Regulatory Risks

o Privacy and Confidentiality

o Availability

o Integrity

o Computationally feasible

o Proper usage metering

o Internal and external attacks

o 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 behavior 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.

1. **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 exchanssge 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 (mod n) from the known values of (mod n) and (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

Table1: Private Computations

|  |  |
| --- | --- |
| Master | Slave |
| Choose a secret number a.  Compute M=(mod n) | Choose a secret number b  Compute S=(mod n) |

* Master compute the number.
* Bob compute the number

Here Master and Slave have the same key that is K=(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\_\_\_\_, 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=mod 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].

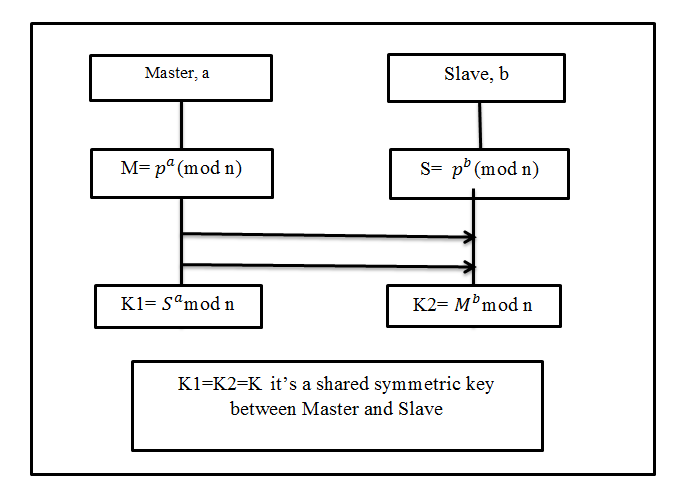


Figure: Diffie Hellman key exchange

**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(sum) 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 are 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 combined 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 each byte is replaced with another according to look up table.
* **Shift Rows:** A transposition step where each row of the state is shifted cyclicallya certain number of steps.
* **Mix Columns:** A mixing operation which operates on the columns of the state, combining the four bytes in each column.
* **Add Round key:** In this each byte of the state is combined 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 generates unique keys for users once they authenticate themselves with the server. The key is generated using instances of AES key generator class. This key is then transferred to the cloud client via the mail-server through a mail which receives and stores a copy for it for decrypting purpose.

1. **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.

* 1. **Proposed Model**

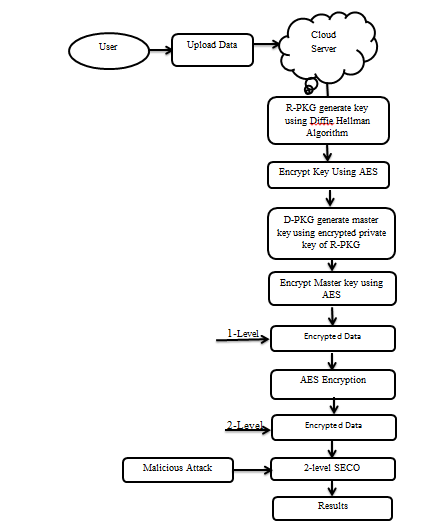
The proposed modal focuses on following five objectives which are helpful in increasing the security on content/data storage and are simulated by visual studio environment using Azure Cloud.

* 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.

* 1. **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.

Figure: Basic Block design of proposed work

This scheme is proposed to enhance the security in cloud data storage systems. The Block design of the proposed work is shown in Fig .

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

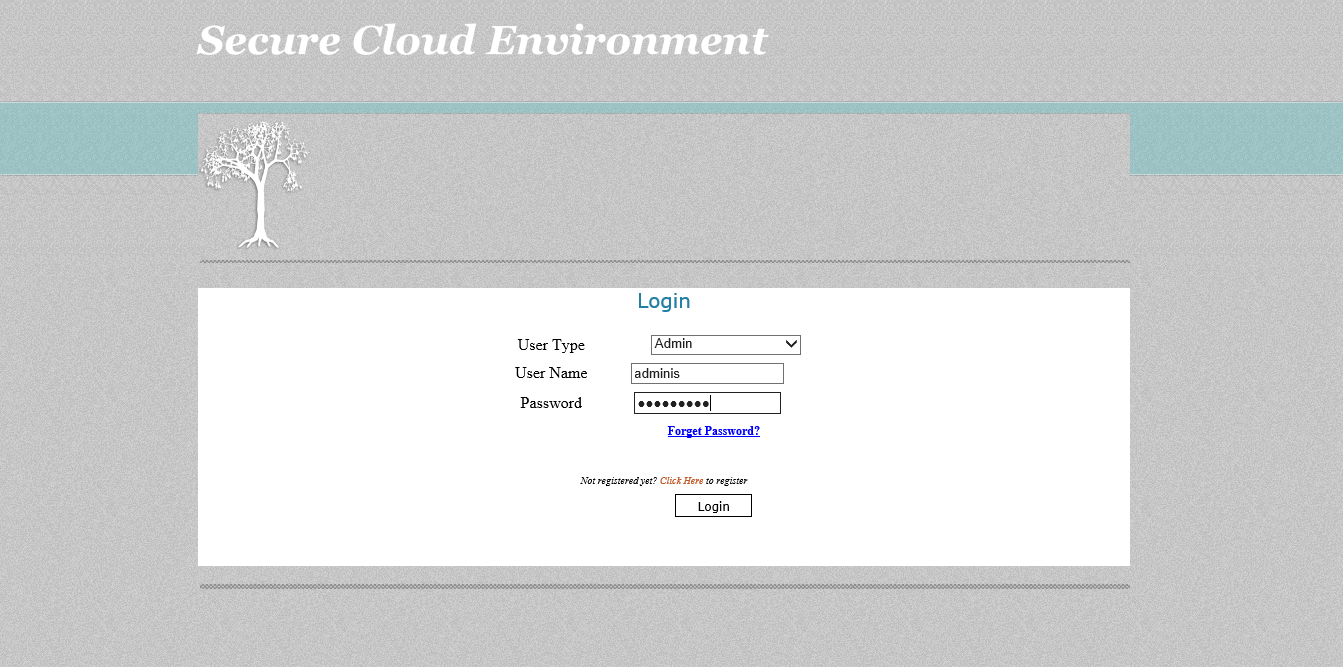


Figure: Admin page

***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.

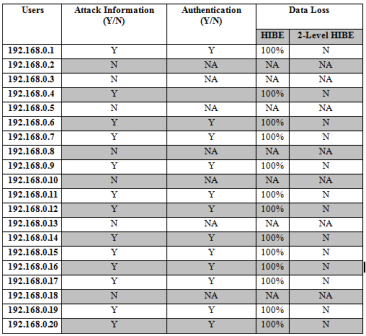
**8 Results & Discussions**

**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.



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.

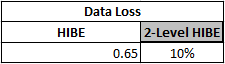
In the above analysis 65% attack is on the cloud environment out of 100%.

Total number of users=20

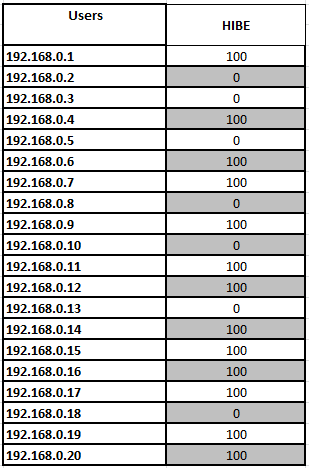
Attack on users=13

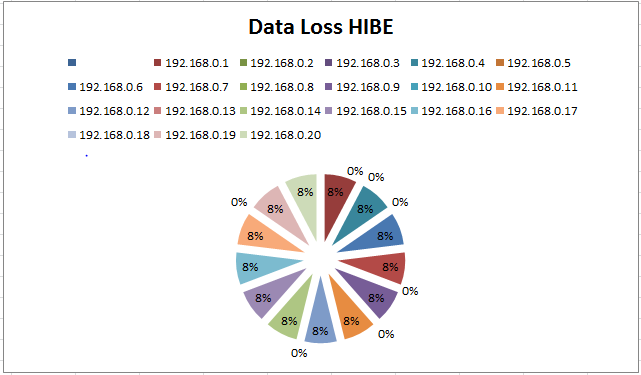
%age attack= (13/20)\*100=65%

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



Individually Data Loss in HIBE for 20 users



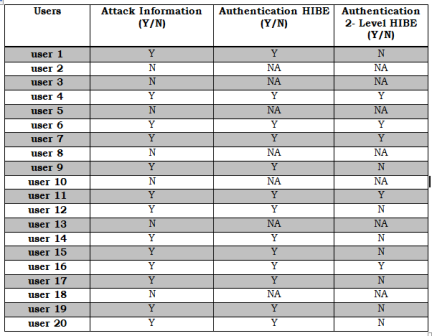


**Case Study 2 (Attacks Acceptance/Rejection Rate):**

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.



**Acceptance Rate:**

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

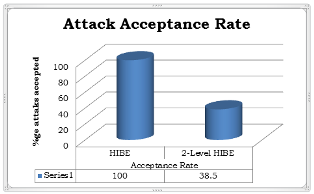
Total number of users=20

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%



**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

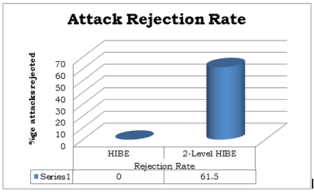
Attacks

k on users=13

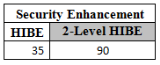
%age attack= (13/20)\*100=65%

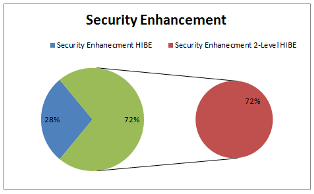
%age attacks rejected in HIBE= (0/13)\*100 = 0%

%age attacks rejected in 2-level HIBE= (8/13)\*100= 61.5%



**Case Study 3 ( Security Enhancement):**





1. **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 analyse this architecture on real cloud environment, So that the real performance factors will be analysed.

1. **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) C. Dourolis, P. Ramanathan and D. Moore, “ what do packet dispersion techniques measures/”, In Proc. IEEE INFOCOM, Anchorage, AK pp. 905-914[2001]

3) Cheng, K.M., chang,T.Y., and Lo J.W.,2010.” Cryptanalysis of security enhancement for a Modified Authenticated Key Agreement Protocol “ international Journal of network security, vol.11,No.1, pp.55-57.

4) 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.

5) 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]

6) 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.

[7] Er. Rimmy Chuchra,Lovely Professional University,Phagwara, India, *“Data Security in Cloud Computing”*, International Journal Nov.,2012.

8) Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360-Degree Compared CoRR. *abs/0901.0131*.

9) 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.

10) 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

11) http:// [www.google.com/sens.org/rr/encryption algorithm.php](http://www.google.com/sens.org/rr/encryption%20algorithm.php), Diffie Hellman algorithm Rilly Lochridge Algorithm, 2003

12) J. Brodkin. Gartner: *“Seven cloud-computing security risks”,* Infoworld, 2008.

13) 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.

14) Jintao Liu,School of Electronics and Computer Science University of Southampton, *“Cloud Computing Security”* ,2009.

15) 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.

16) Meiko Jensen, JlorgSchwenk, Nils Gruschka and Luigi Lo Iacono, *“On Technical Security Issues In Cloud Computing”,*IEEE International Conference on Cloud Computing,2009.

17) 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.

18) 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.

19) Neela,K.,” A survey on security Issues and vulnerabilities on cloud computing”, vol.2, No.7, pp.855-860

20) Nils Gruschka and Meiko Jensen ,”Attack surface : A taxonomy for attacks on cloud services” in 2010 IEEE 3rd international conference on cloud computing.

21) Vamsee Krishna and Sriram Ramanujam,*”**Data Security in Cloud Computing”,* Journal of Computer and Mathematical Sciences,vol. 2, Issue 1, 28 February, 2011.

s22) will Gorner, “ Diffie Hellman Key Exchange” ppts.

23) 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.

**Biography of Authors**

**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 llies 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.

s