A NOVEL APPROACH TO ENHANCE THE SECURITY OF CLOUD COMPUTING

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

RAJVEER KAUR

11406928

Supervisor

DR. ASHISH KUMAR

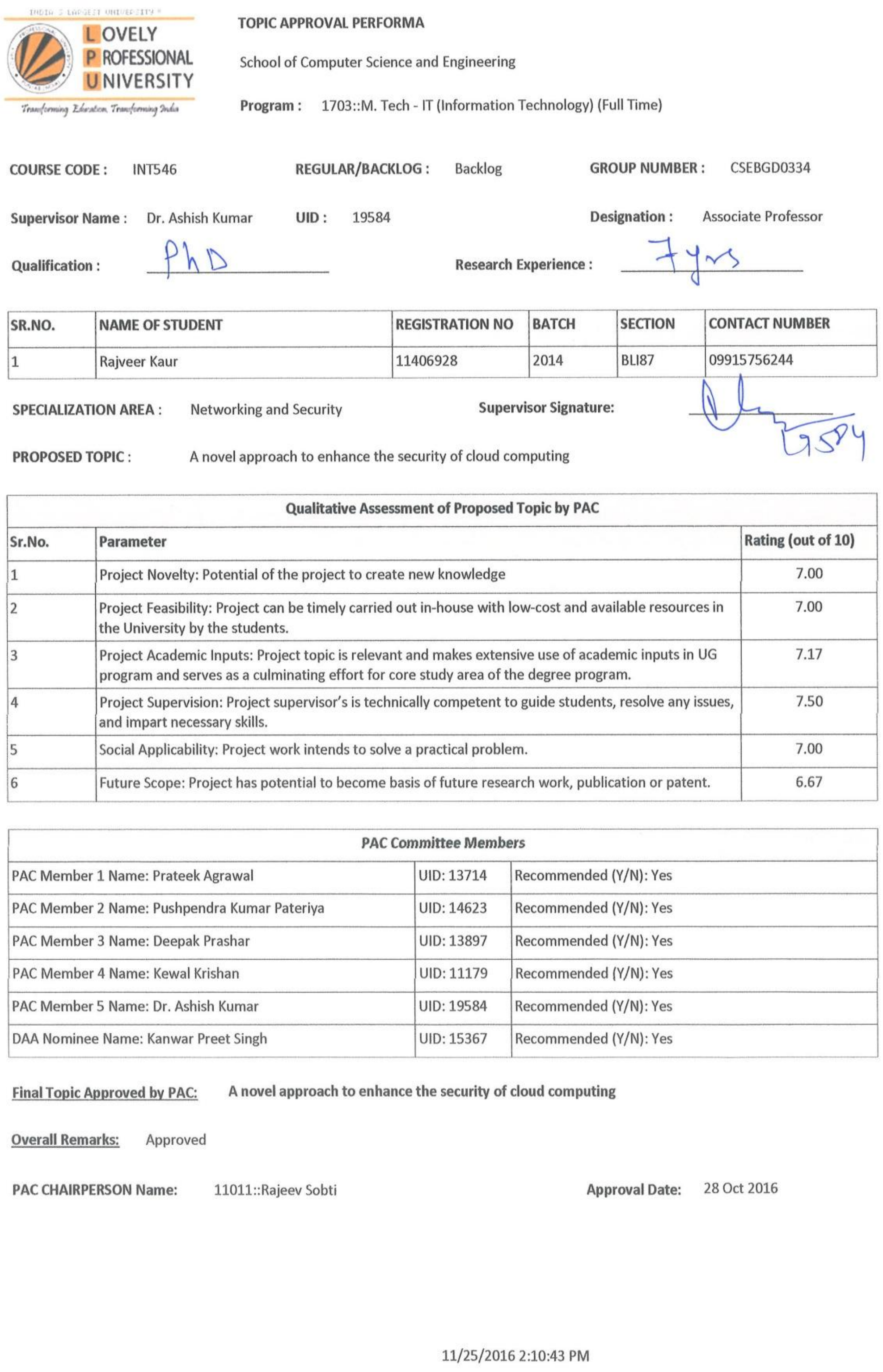
School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

December 2016

PAC FORM



TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : 1703::M. Tech - IT (Information Technology) (Full Time)

COURSE CODE : INT546 **REGULAR/BACKLOG :** Backlog **GROUP NUMBER :** CSEBGD0334

Supervisor Name : Dr. Ashish Kumar **UID :** 19584 **Designation :** Associate Professor

Qualification : PhD **Research Experience :** 7yrs

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Rajveer Kaur	11406928	2014	BLI87	09915756244

SPECIALIZATION AREA : Networking and Security **Supervisor Signature:** 19584

PROPOSED TOPIC : A novel approach to enhance the security of cloud computing

Qualitative Assessment of Proposed Topic by PAC

Sr.No.	Parameter	Rating (out of 10)
1	Project Novelty: Potential of the project to create new knowledge	7.00
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.00
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.17
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.50
5	Social Applicability: Project work intends to solve a practical problem.	7.00
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	6.67

PAC Committee Members

PAC Member 1 Name: Prateek Agrawal	UID: 13714	Recommended (Y/N): Yes
PAC Member 2 Name: Pushpendra Kumar Pateriya	UID: 14623	Recommended (Y/N): Yes
PAC Member 3 Name: Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member 4 Name: Kewal Krishan	UID: 11179	Recommended (Y/N): Yes
PAC Member 5 Name: Dr. Ashish Kumar	UID: 19584	Recommended (Y/N): Yes
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): Yes

Final Topic Approved by PAC: **A novel approach to enhance the security of cloud computing**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11011::Rajeev Sobti **Approval Date:** 28 Oct 2016

11/25/2016 2:10:43 PM

ABSTRACT

Cloud computing is widely used technology .The world is connected with internet .cloud computing is the facility provided by internet. The on demand services provided by cloud are database, network, web servers, email, virtual desktop, customer relationship management etc. There are some security issues with cloud environment .Many cryptographic techniques are designed to overcome these issues. The cloud storage is increasing day by day ,due to the reason time of encrypting and decrypting the data is increasing .To overcome these issues the hybrid technique is proposed by using elliptic curve cryptography, diffie-hellman, and quantum AES .The proposed technique will enhance the security and reduce the storage and time .

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation entitled **"A NOVEL APPROACH TO ENHANCE THE SECURITY OF CLOUD COMPUTING”** in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor **Dr. Ashish Kumar**. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University’s Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

Rajveer Kaur

11406928

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled **"A Novel Approach To Enhance The Security Of Cloud Computing"**, submitted by **Rajveer Kaur** at **Lovely Professional University, Phagwara, India** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

Dr. Ashish Kr. Luhach

Date: ______________

Counter Signed by:

1) **HoD's Signature: ________________**

   HoD Name: ___________________

   Date: ___________________

2) **Neutral Examiners:**

   (i) Examiner 1

   Signature: _______________

   Name: __________________

   Date: ___________________

   (ii) Examiner 2

   Signature: _______________

   Name: __________________

   Date: ___________________

ACKNOWLEDGEMENT

I would like to express my deepest gratitude towards my mentor **Dr. Ashish Kumar** for providing excellent guidance, advice, encouragement, supervision and inspiration throughout the development of this dissertation study. I would like to thank to the **Project Approval Committee members** for their valuable comments and discussions. I would also like to thank to **Lovely Professional University** for the support on academic studies and letting me involve in this study.

And last but not least, I find no words to acknowledge the moral support rendered by my parents and friends. All this has become reality because of their blessings and above all by the grace of **GOD.**

RAJVEER KAUR

(11406928)

TABLE OF CONTENTS

CONTENTS **PAGE NO.**

LIST OF FIGURES

FIGURE NO. FIGURE DESCRIPTION PAGE NO.

LIST OF TABLES

TABLE NO. TABLE DESCRIPTION PAGE NO.

CHAPTER 1
INTRODUCTION

1.1 CLOUD COMPUTING

Cloud computing [4][5][6] is blooming like no other technology in the market. Cloud hosts many of the services like email, search engines, social networks. Every organization wants to adopt cloud computing. Cloud has all features that allows client to avoid hardware and software, gain flexibility, complete use of resources and specially client access control. The services and applications that run on distributed network using virtual resources and can be accessed by common internet protocols and networking standards. The resources are unlimited and virtual that can be customized according to our demand. The physical systems which are actually operating the software abstracted from the user. Cloud computing contains deployment and service model Development model where the cloud is located and for what purpose. There are four types of clouds in the deployment model:

- **Private cloud**
- **Public cloud**
- **Community cloud**
- **Hybrid cloud**

Service model is a type of service that what kind of service is offered by the service provider. Service model contains- software as a service, platform as a service and infrastructure as a service. A cloud is based on abstraction and virtualization .abstraction is to abstract or hide the details of the cloud .The cloud is ubiquitous but applications inside the cloud are not specified and virtualization to complete use of available resources. Cloud computing is visualized by resource pooling, storage and system can be provisioned as needed from the centralized infrastructure. The resources are scalable with agility. The concept of multi-tenancy and the cost is also on metered basis.

Now we take an example of drop box to understand the concept of cloud computing. In drop box which is a cloud service users can use their cloud with free account or premium account (with extra privileges). There is one problem is exist in drop box, any user can access the data of any other user without the permission of other user. It is a big issue in cloud computing that how we prevent these types of problems. Many organizations and companies use firewall, IDS and antivirus to prevent them. As the defense against services like identify frauds and the malicious services almost all service provider organizations use the access control and user authentication mechanisms. The best feature of cloud computing is user can access the cloud from anywhere in the world.

In the cloud computing, there is no need to know about the configuration of the system and physical location of the service providers. Basic characteristics of clouds are homogeneity, virtualization, Massive scale, low cost software, advance security, services orientation and geographic distribution. By using cloud computing we access more effective computing with the help of centralizing storage, processing, bandwidth and memory. The Availability of cloud computing is required Software, hardware, application, platform, infrastructure and storage with an internet connection.

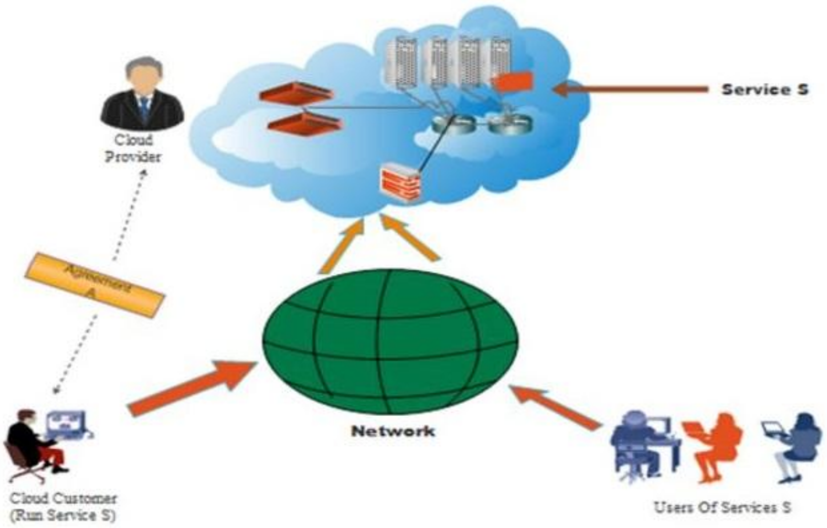


Figure 1.1- Cloud computing

1.2 CLOUD COMPONETS

Cloud system has three main components. Each component has definite purpose and play a specific role. Components are given below:

1.2.1 Client

There is an interaction between end users and client to manage information related to the cloud. There are three types of clients are present:

- **Mobile:** Smartphone, Windows smart phone e.g. Samsung, Blackberry.
- **Thin:** This is used only for displaying the information with the help of server. Thin client does not have internal memory and does not perform any computation work.
- **Thick:** Thick client use different browsers like IE, Google chrome in order to connect with internet cloud.

1.2.2 Datacenter

Datacenter is a collection of servers which are hosting different applications. End user is connected with datacenter to use different applications and it may present so far from the end user.

1.2.3 Distributed server

It is the part of cloud which is present throughout the internet hosting different applications. When the user uses the application from cloud, he feel like application is run from his own system.

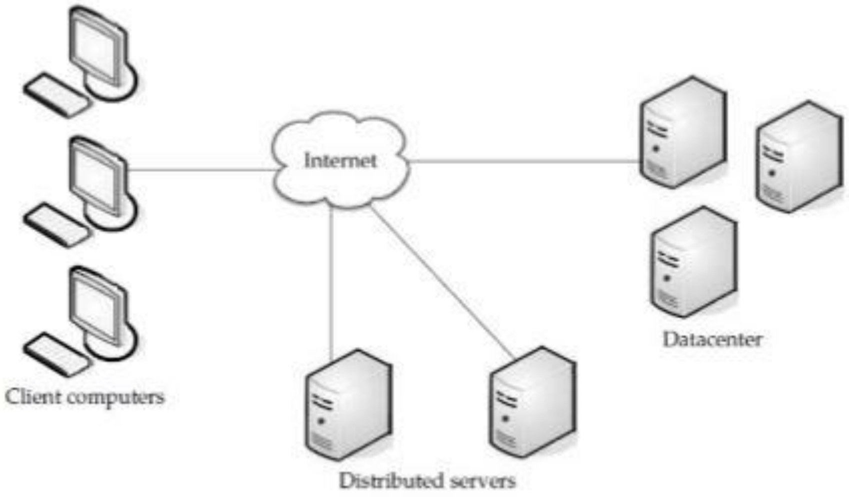


Figure 1.2- Cloud components

The main steps to achieve the concept of cloud are given below:

- **Grid computing:** Grid computing means solve the large scale problems on parallel computing.
- **Utility computing:** In utility computing, resources are available on the metered basis means user pays only that amount which he has used.
- **SAAS:** It provides the network based subscription and it is a part of service model of cloud computing.
- **Cloud computing:** The services which are provided by all the above techniques is cover in cloud computing.

1.3 FEATURES OF CLOUD COMPUTING

Cloud computing has various features [1]. Some of them are as follows:

- **On demand:** The cloud is available on demand, but there is no attraction to service provider.
- **Broad network access:** Cloud provides broad area usage because of platform independence. The applications can be run over many wide area networks.
- **Resource pooling:** Resource pooling is the best way of utilization of resources using multi-tenancy .the hardware as well software resources can be used at the same time .The application can access resource pool when there is requirement of hardware and software resources.
- **Measured service:** Cloud computing is a measured service .the cost is according to the uses has to pay according to the service and bandwidth provided.
- **Lower cost:** The cost is lower because it is worth to the efficiency and utilization of resources.
- **Ease of utilization:** The utilization of service is easy .there is no license required for particular service.
- **Low barrier to entry:** The expenditures are reduced according to user requirements. Anyone can be granted by service provider anytime.
- **Reliability:** The cloud balances the network load and reduces the failure.

1.4 DISADVANTAGE OF CLOUD COMPUTING

The major aspects in cloud which are considered as disadvantages are security and privacy[1][2], lack of control [2][3], downtime [1], attack vulnerability to cloud environment [2] and cost .These are some issues to be discussed in brief.

1.4.1 Security and Privacy

Security is major concern in today's world. All the service providers promote their ideas of having latest security techniques. But as it comes to internet computing that is using online applications and storage, the customers feel insecure to share personal and business data with the third party cloud providers. Many best service providers' offers great authentication techniques for customer trust.

1.4.2 Lack of Control

Cloud users have less or we can say limited control over the functions provided by service provider. They have also a limited control over data and services but not on the infrastructure at the backend.

1.4.3 Downtime

The downtime of a cloud service leads to a great affect over customer services for example reliability. The service provider have to handle huge rush every time. The access is completely dependent on the internet connection. So sometimes when your server is down, the access to the application goes down.

1.4.4 Vulnerability to Attack

As the information is provided over the internet, attacker can gain access to online applications by using appropriate methodologies. Even the best service providers can be hacked by the attackers.

1.4.5 Cost

The cost at some small scales the cost can be précised. But at business level the cost ends up more than expected. The costs are changing, so it should be checked on regular basis or smartly pay first if you know what amount of data you are going to use.

1.5 CLOUD MODELS

Cloud has deployment model [3][4]which contains different types of clouds.

1.5.1 Private Cloud

In the private cloud the existing infrastructure is only of use for an organization .This is supposed to be more secure among all providing greater efficiency and security. It involves secure and distinct environment. The infrastructure is owned and managed by an organization itself. The private cloud owned environment with which a specified client can operate. The private cloud costs more because it requires more bandwidth and because of single organization uses it the cost cannot be divided .The private cloud provides environment to operate applications which are specified within the organization for use. These type of clouds are more reliable and stop cloud bursting at some extent because sensitive information is biggest issue in today‘s world either it is for organizational or personal use. Moreover it has more control over resources due to single organization.

1.5.2 Public Cloud

Public cloud is shared among many organizations or can say it is for public use. Public cloud is believed to be unsecure because number of people are using public cloud and due to the open access to the data .The purpose can be common the type of cloud can be run and managed by organization dealing with cloud environment and constructed using public network like internet. The type of cloud is run over public channel like google app engine, IBM’s blue cloud, sun cloud etc. The cloud is location independent, scalable, reliable and cost effective.

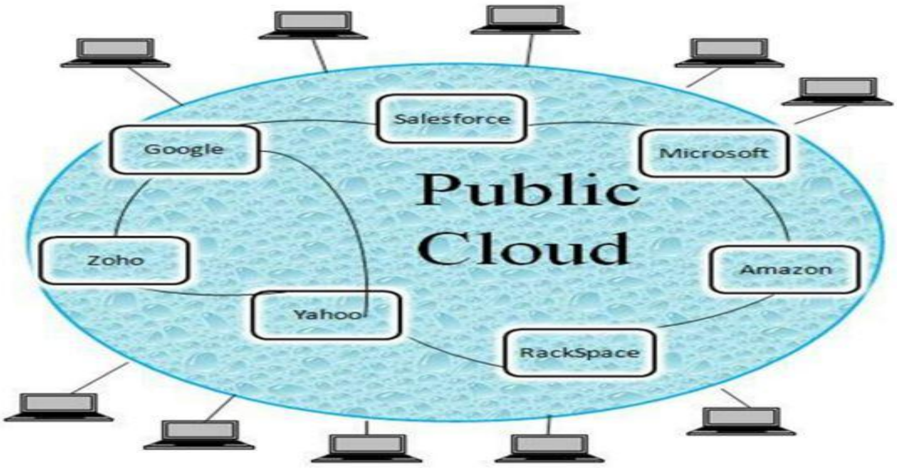


Figure 1.3- Public cloud

1.5.3 Hybrid Cloud

The hybrid cloud is made up from public and private clouds .the organizations combines both the clouds for their effective use .The functions and data which is meant to be kept hidden comes under private cloud and data which is of public use like commercial apps are comes under public cloud .The combination of both the clouds is said to be hybrid cloud. Some other clouds can be used together as hybrid technology for various purposes .The type of cloud can be much more effective among all the clouds and fulfill the requirements.

1.5.4 Community Cloud

The community cloud lies in between public and private cloud and can be accessed by more than one organization for common business purposes. It is less secure because it is used by many organizations. Community cloud takes less cost because cost is divided among participating organizations. The cloud is generally managed by third party. The major drawback is bandwidth is shared among the users and hence decreases the reliability.

1.6 CLOUD COMPUTING SERVICE

In today’s scenario, cloud computing systems are providing a huge variety of interfaces. It makes vendors to enable rent out their services on customer’s physical machines. The services provided by cloud may vary from virtual machines to the software host services. Cloud is an area in which companies can gain profit, for this reason many organizations like IBM, Google, EBay, Amazon have already invested in cloud technologies.

There are following services provided by cloud [1][2][4][5][6]:

- IAAS (Infrastructure as a Service)
- SAAS (Software as a Service)
- PAAS (Platform as a Service)

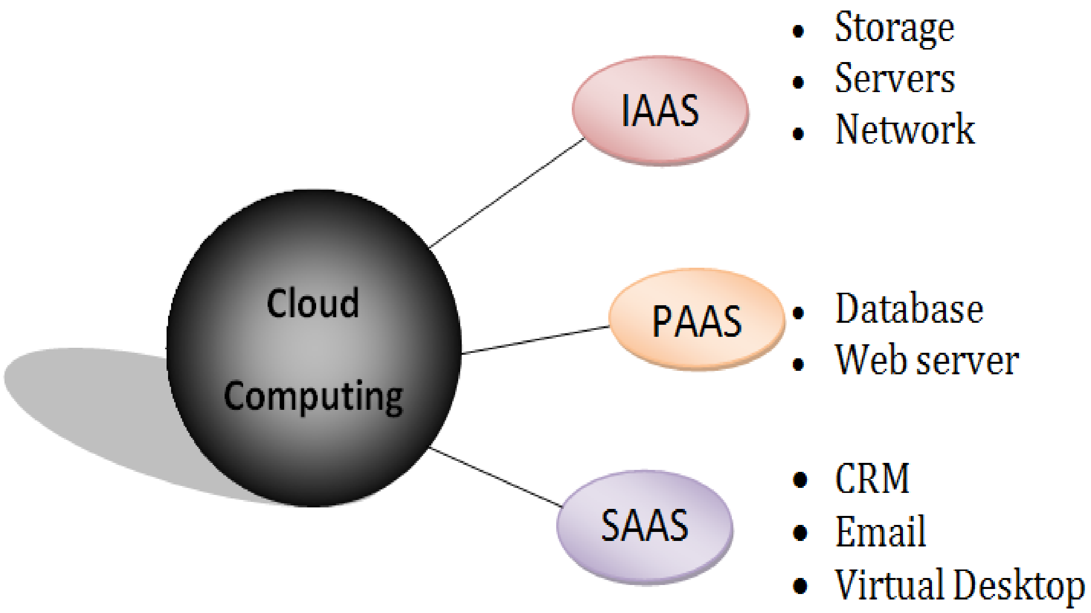


Figure 1.4- Service model of cloud computing

1.6.1 IAAS

IAAS (Infrastructure as a Service) manages the infrastructure service provider, but client is responsible for all other deployments like operating system etc. the most common infrastructure provided by cloud is google compute engine. It makes companies free from infrastructure. The virtual machines, virtual storage, virtual infrastructure and hardware assets are used as resource. The service providers for IAAS are Amazon elastic compute cloud, Go Grid, Terre mark, Linode, flexi scale.

- **Go-grid:** Go-grid is an infrastructure service provided by cloud, which is hosting Linux and windows virtual machines. It is basically a data pipe company .They also deals in hybrid cloud hosting. The service is being managed by multi-server control panel.
- **Linode:** Linode is privately owned a virtual private server provider company. It is an American company established in 2003 and providing virtual infrastructure and servers over 400,000 customers.

1.6.2 SAAS

SAAS (software as a service) is a service provided to the client through thin client interface. The customer is responsible for begins and ends with entering and managing data. For example, operating system with application environment and user interface. The service providers are GoogleApps, Oracle on Demand, SQLAzure and salesForce.com.

- **SQLAzure:** SQLAzure is run and managed by Microsoft Azure, Which provides cloud database as a service, storage files and high availability and offering online data storage
- **SalesForce.com:** It works on cloud customer relationship management. It also capitalizes on commercial applications through the social websites.

1.6.3 PAAS

PAAS (platform as a service) provides platform to run applications more than one. It virtualizes the computer system over the cloud infrastructure supported by Paas service provides for cloud infrastructure and manages operating systems. Client is responsible for installing the application. For example operating system, application services, development service etc. Service providers are Force.com, GoogleAppEngine and WindowsAzurePlatform. Cloud also offers network as a service, under Naas it provides virtual private networks and bandwidth on demand. There are many other services provided by cloud computing.

- **GoogleAppEngine:** It provides platform as a service for developing and hosting the web applications. The resource consumption is free up to certain level and after a limit it is chargeable. As per demand it automatically allocates the resources for the web applications.

- **WindowsAzurePlatform:** it is a platform and infrastructure developed by Microsoft, which supports many programming languages. It manages applications through a global network of data centers.

Figure 1.5- Service providers of cloud computing

1.7 CLOUD ATTACKS AND SECURITY

The term security refers to provide security to the data available on cloud. This to maintins the authenticity, integrity and availability of data. There are some attacks possible on cloud environment [2] [3][4][5][6].

1.7.1 DENIAL OF SERVICE ATTACK

When the requests to the server exceeds the limit of server then server goes down, it can be performed by attacker to reject the user's access or resources from the server The denial of service attack can be more damaging. As per cloud needs, there are numbers of users of cloud. An attack distributed denial of service attack can be there in cloud environment.

1.7.2 CLOUD MALWARE INJECTION ATTACK

The attempt is to inject malicious service or any virtual machine in cloud. The particular serve a purpose for attacker for which it is introduced to the cloud. The purpose may be any like data theft, eavesdropping, data modification. This requires the implementation of malicious service and virtual machine i.e. Saas, Pass and Iaas respectively. The malicious service is added to cloud.

1.7.3 AUTHENTICATION ATTACK

The authentication is provided in many ways in cloud environment; basically it is about crypto graphical algorithms and revolves around what facts user knows. There is a list of authentication attack and mechanisms .the mechanisms providing authentication to the systems can be attacked if the unauthorized person have advance knowledge of their implementation.

1.7.4 MAN-IN-MIDDLE ATTACK

The attack is performed by attacker by placing himself within two parties. The aim can be spoofing the information that is being shared among both the parties. The attack can be passive or active attack .Passive attack will be spoofing the information. On the other side active attack is about modifying or intercepting the information.

1.8 DIFFIE-HELLMAN KEY EXCHANGE

Diffie-Hellman is the first public key cryptography or symmetric key agreement ever intended, in 1976. Diffie-Hellman allows the sharing of secret key between two users and it is an exponential key agreement. It requires no prior secrets.

In diffie-hellman when two users want to share secret key, At first, both the parties need to choose two numbers n and p. Let p is an integer and n is a prime number. The setup for the diffie-hellman algorithm:

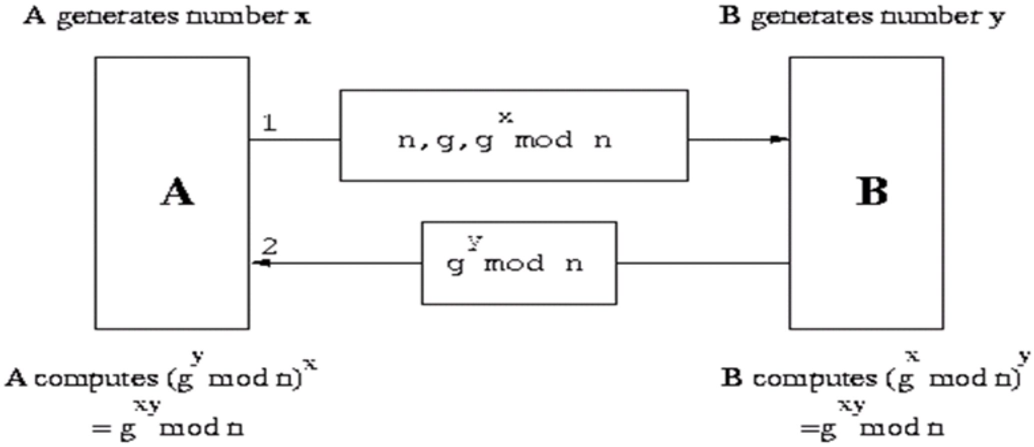


Figure 1.6- Diffie-hellman process

- Suppose that we have two parties M (Master) and S (Slave), they want to communicate with each other.
- Both the parties do not want the eavesdropping to know their communication.
- M and S agree upon and select two numbers n and p, p is primitive root mod n and n is a prime number. Anyone can see these two numbers.

Table 1.1- Private computations

M	S
Choose a secret number a.	Choose a secret number b.
Compute X = P^a (mod n)	Compute Y = P^b (mod n)

- Public values are exchanged.
- M sends X to S == X.
- Y = S sends Y to M.
- M calculates the number K = Y^a = P^{ab} (mod n).
- S calculates the number K = X^b = P^{ba} (mod n).

Now M and S have same key K.

In diffie-hellman when two parties want to exchange the data they need to agree upon the same key means symmetric key. Symmetric key is used for both encryption and decryption of the messages. Diffie-hellman algorithm is used only for exchanging the keys between two parties not for encryption and decryption process.

1.9 AES

AES (Advanced Encryption Standard) [21][14][5][6] is an open algorithm and modern symmetric-key block algorithm for encrypting the electronic data. AES is an encryption algorithm which replaces the DES. It uses the encryption key and encryption rounds. A block cipher is an encryption algorithm which works on single block of the data. AES uses the single key encryption mechanism; it may be 128 bit, 192 bit and 256 bit long. 128 bit key means, it is encryption key length. In AES encryption and decryption is performed by same key, so it is called symmetric encryption algorithm.

Modes of operations of AES:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Counter (CTR)
- Cipher Feedback (CFB)
- Output Feedback (OFB)

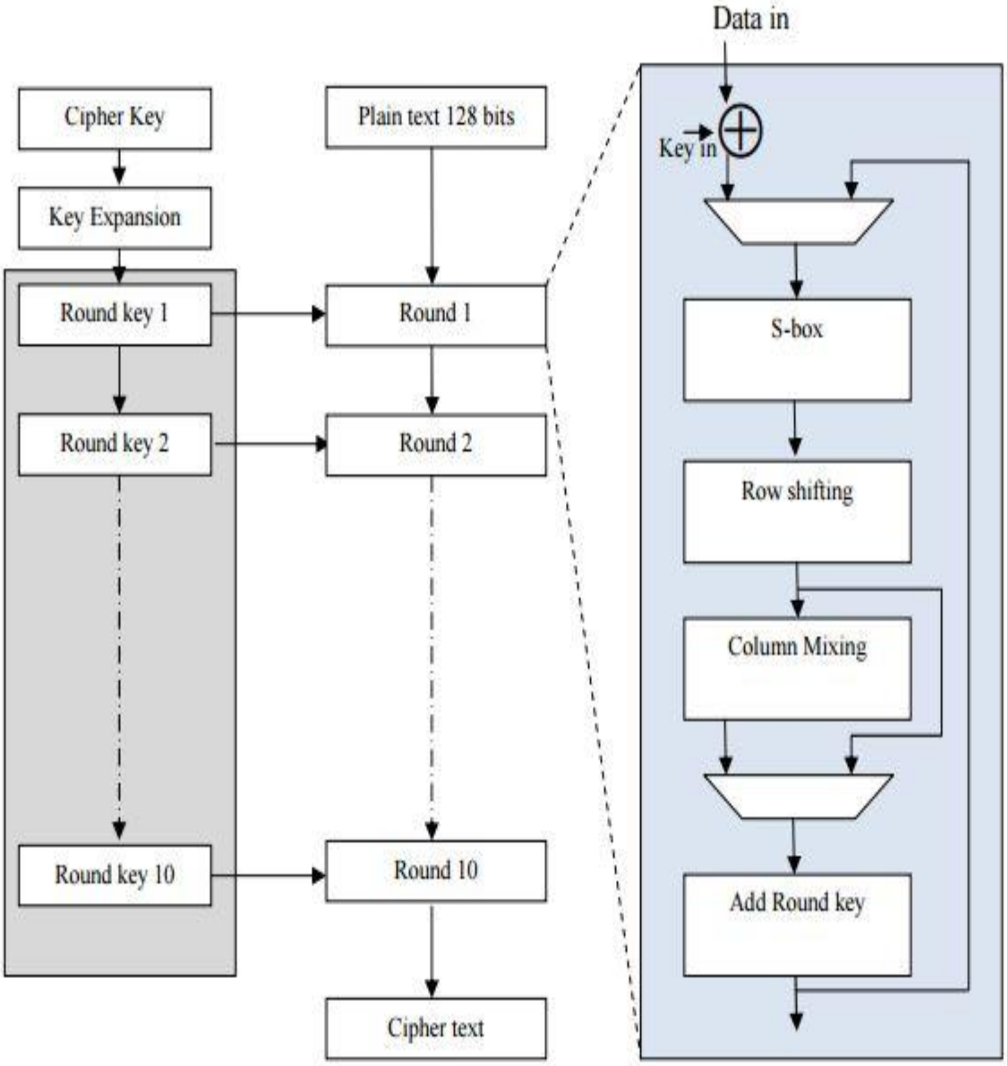


Figure 1.7- AES flow chart

1.9.1 Initial version of AES:

There are three versions of AES.

- Advanced Encryption Standard (128-bit)
- Advanced Encryption Standard (192-bit)
- Advanced Encryption Standard (256-bit)

128, 192 and 256 bit are the key length for encryption process. In AES-128 bit, key is represented in an array 4*4 and it has 10 rounds. In AES-192 bit, key is represented in an array 4*6 and it has 12 rounds. In AES-256 bit, key is represented in an array 4*8 and it has 14 rounds. Each round has four states except the last round. The last round in all the version of AES has all the states except mix-column transformation.

- Substitution transformation
- Shift-row transformation
- Mix-column transformation
- Add round key transformation

Substitution transformation replaces each element of an array with S-box values. For example, if element in an array is a8 then the value corresponding to a row and 8th column of the S-box is used to replace the a8 value.

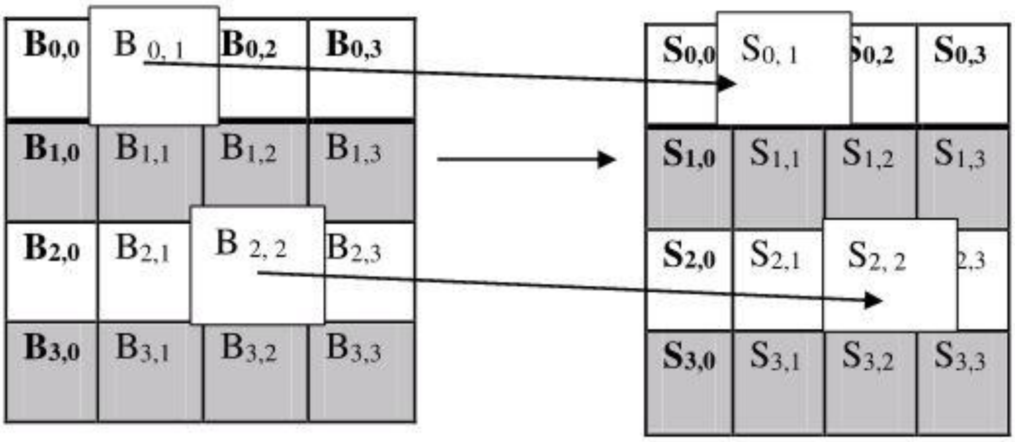
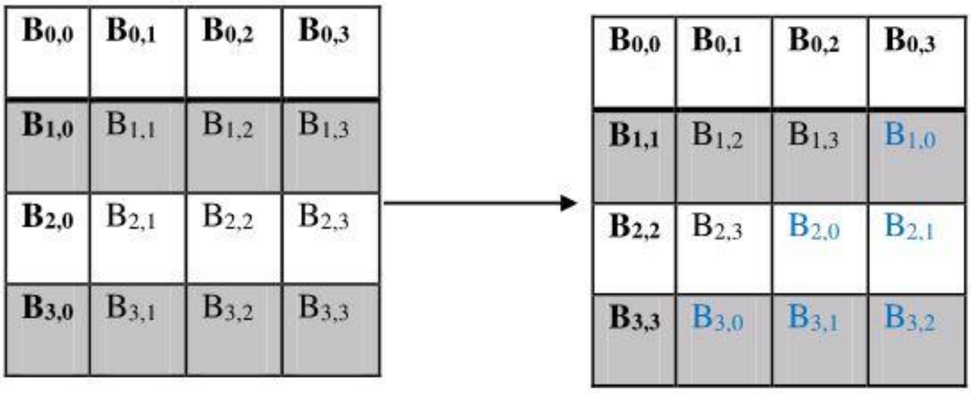


Figure 1.8- Sub-byte transformation

Shift-row transformation involves the action on the rows of an array. In this first row not shifted at all, 2nd row is shifted towards left by 1 step, 3rd row is shifted towards left by 2 steps and 4th row is moved towards left by 3 steps.

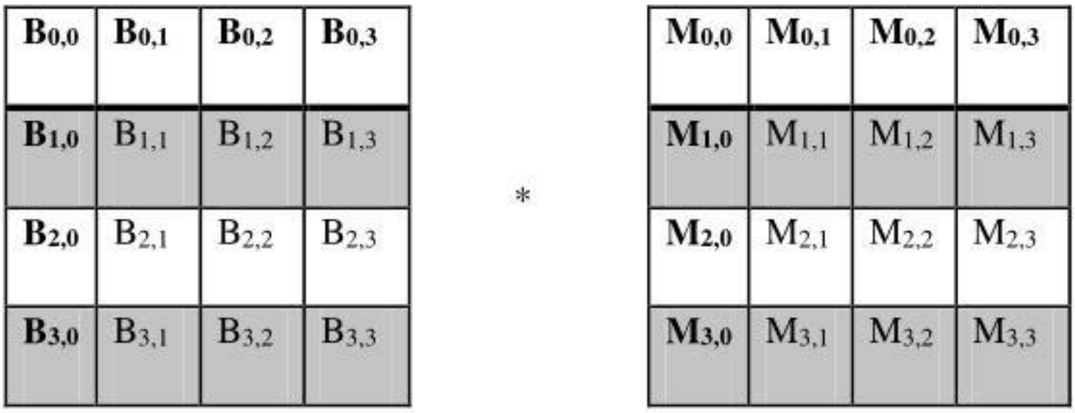


$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$B_{0,3}$
$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$B_{1,3}$
$B_{2,0}$	$B_{2,1}$	$B_{2,2}$	$B_{2,3}$
$B_{3,0}$	$B_{3,1}$	$B_{3,2}$	$B_{3,3}$

$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$B_{0,3}$
$B_{1,1}$	$B_{1,2}$	$B_{1,3}$	$B_{1,0}$
$B_{2,2}$	$B_{2,3}$	$B_{2,0}$	$B_{2,1}$
$B_{3,3}$	$B_{3,0}$	$B_{3,1}$	$B_{3,2}$

Figure 1.9- Shift-row transformation

Mix-column transposition is involves each column of state array multiplied by fixed 4*4 array.



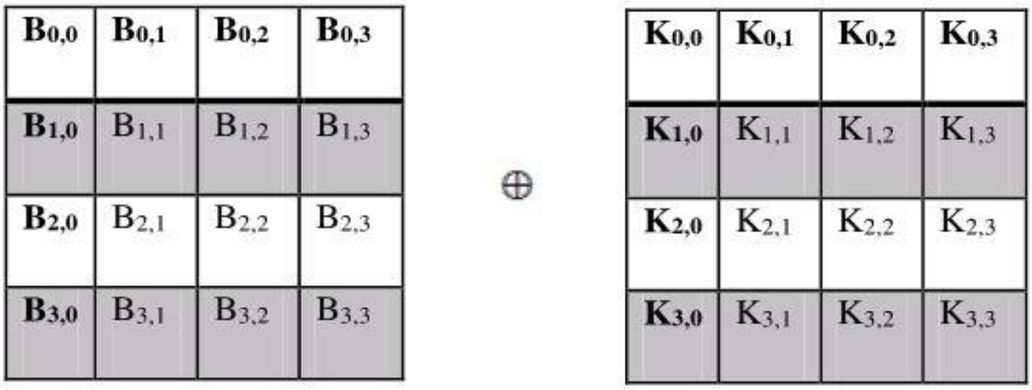
$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$B_{0,3}$
$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$B_{1,3}$
$B_{2,0}$	$B_{2,1}$	$B_{2,2}$	$B_{2,3}$
$B_{3,0}$	$B_{3,1}$	$B_{3,2}$	$B_{3,3}$

*

$M_{0,0}$	$M_{0,1}$	$M_{0,2}$	$M_{0,3}$
$M_{1,0}$	$M_{1,1}$	$M_{1,2}$	$M_{1,3}$
$M_{2,0}$	$M_{2,1}$	$M_{2,2}$	$M_{2,3}$
$M_{3,0}$	$M_{3,1}$	$M_{3,2}$	$M_{3,3}$

Figure 1.10- Mix-columns transposition

Add round key involves the process of XOR which means each element of an array perform the function of XOR with each of the key.



$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$B_{0,3}$
$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$B_{1,3}$
$B_{2,0}$	$B_{2,1}$	$B_{2,2}$	$B_{2,3}$
$B_{3,0}$	$B_{3,1}$	$B_{3,2}$	$B_{3,3}$

⊕

$K_{0,0}$	$K_{0,1}$	$K_{0,2}$	$K_{0,3}$
$K_{1,0}$	$K_{1,1}$	$K_{1,2}$	$K_{1,3}$
$K_{2,0}$	$K_{2,1}$	$K_{2,2}$	$K_{2,3}$
$K_{3,0}$	$K_{3,1}$	$K_{3,2}$	$K_{3,3}$

Figure 1.11- Add-round key

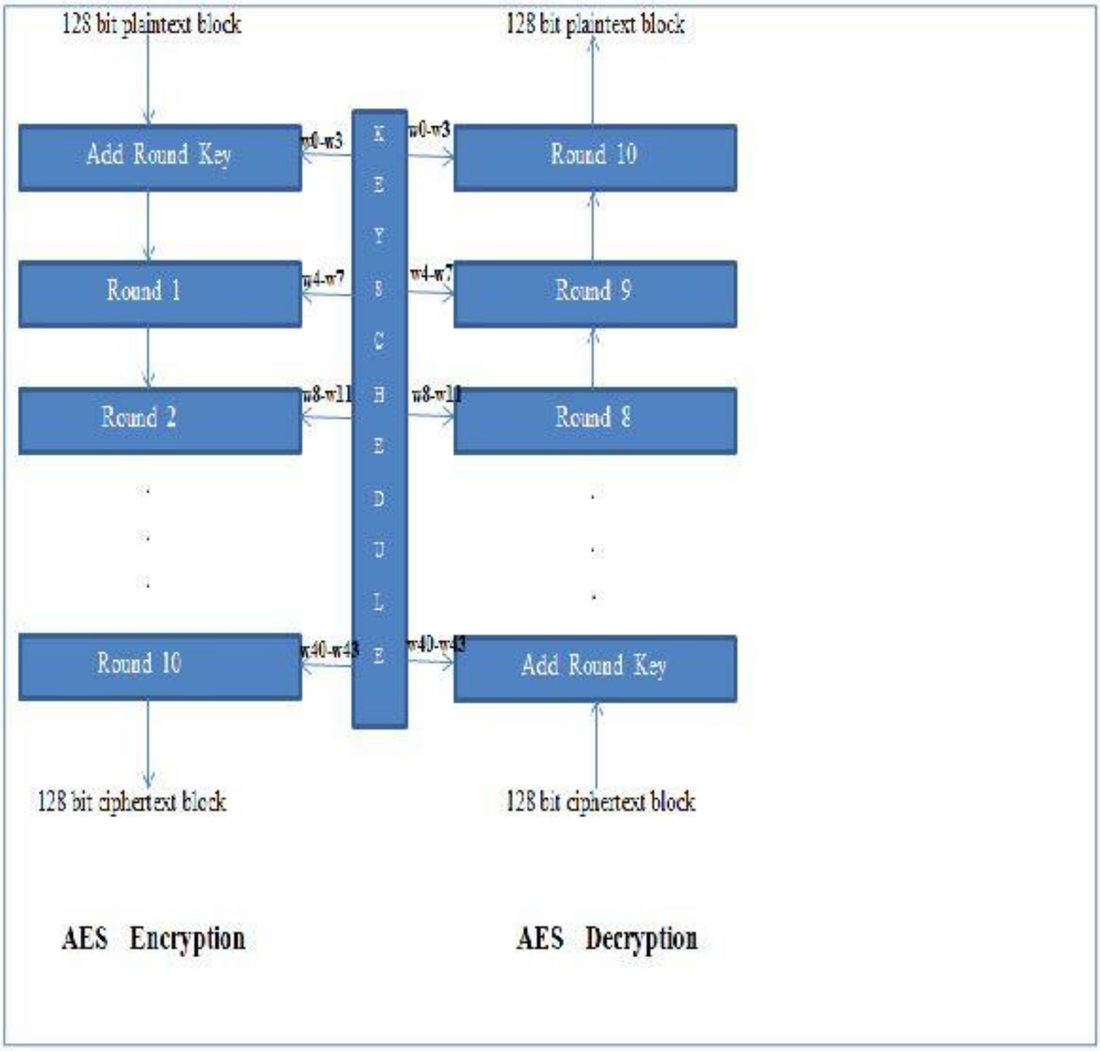


Figure 1.12- Encryption and decryption process of AES

CHAPTER 2
REVIEW OF LITERATURE

Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi, Shirin Dabbaghi Varnosfaderani [8] proposed a new scalable and efficient user authentication scheme for the environment of cloud computing. In this paper, a client based user authentication agent was user for proving the identity of user at the client side and also use the two different servers for the cryptography resources and storing authentication to decrease the encryption time form main server. Firstly a client sends the request for registration with mac ID, com ID, user ID and access type and server check that request id server confirms after that client sends the optional password and server performs some functions like DL (Download-link generation) and EACG (Encrypting ACG, PW) and sends to the client. In the next step client open a browser and type login id and password for access the cloud service and send to the MDHA (Modified Diffie-Hellman Agent) for the confirmation of the same. The agent uses the modified diffie-hellman algorithm and RSA algorithm for the confirmation of the login status. In this paper, cloud environment is protected form man in the middle attack, brute force and timing attack. The reliability and rate of trust in cloud environment was increased by the use of this scheme.

C. Tien-Ho, Y. Hsiu-lien and S. Wei-Kuan [9] proposed an Elliptic Curve Cryptosystem (ECC) based on dynamic ID-Based remote mutual authentication. In this paper, cloud Cognitive Authenticator (CCA) which is integrated authentication model uses the concepts of Advance Encryption Standard (AES) and one round Zero Knowledge Proof (ZKP) and to enhance the security in private, public and hybrid clouds. In this paper, the authors provide four procedures with two levels of authentication and technique of encrypting the user identifiers. The main specification of CCA in comparison with other models is the coverage of the two levels of authentication together with strength of the encryption algorithm. In AES compatibility and interoperability are the major weaknesses of CCA.

Jen-Ho Yang and Pei-Yu Lin [10] proposed the id based user authentication in the cloud computing. The proposed method had higher security level and lower computation costs. The authors used the various parameters like ID of the user and server, XOR operation, random number, hash function and. The proposed method had user, id provider and the server and method has been divided into two phases: Registration phase and mutual authentication phase. In the first phase, the user send the id of his own and server to the id provider and then the id provider reply back after performed the hash functions. In the second phase, the users choose random number and create one value for send to the server. Server check the timestamp, if it's not valid then server denies the user. If timestamp was valid then the server compute one value using XOR operation on the id's and allowed for login to user. Servers choose a random number to create some value and send to the user. User checks for the timestamp, if its valid then user assumed that server is legal otherwise not. The proposed algorithm has provided the security against the insider attack, outsider attack, and impersonating. The computation cost was less as compared to the previous methods.

Dr.V.Venkatesa Kumar and A.Murugavel [11] described about the authentication of file content which had stored on cloud server, so that it can only be accessed by authenticated persons. A protocol had been introduced to existing methodology. It was cryptographic protocol named DFA (deterministic finite automata) authentication. It was performed between client and service provider along with key generation. The public and private keys were generated for secure communication between both the parties. The protocol ensured the data integrity.

Subhash Chandra Patel, Ravi Shankar Singh and Sumit Jaiswal [12] described the method to achieve fine grained security with approach of the PGP and the Kerberos. The method has provided the authentication, confidentiality, integrity and privacy features to the cloud service providers and users. We had used PGP with Kerberos because Kerberos does not support repudiation. In this user register his identity to Kerberos and get a ticket. KDC also send ticket to cloud service provider and then user encrypted his data before sending. PGP user requested to service provider for data and Cloud service provider send the data to user. It has provided authentication and integrity by creating message digest then encrypts it with his private key. He added this with original message and send to the CSP, and then CSP calculate message digest and compare.

Wei-Tsung Su, Wo-Chen Liu, Chao-Lieh Chen, Tsung-Pao Chen [13] described about access control in multilayer cloud network. They introduced CAC (Cloud access control) to provide access control on data. The security as a service had provided through CAC. The access policy implemented within service provider and responder. The language they used control expression language, such as ORDL and XACML but CACEL (Cloud control expression language was more suitable for cloud access control.

Cristian PERRA [14] defined a framework for providing user control over online media sharing. There was need of privacy and security and the sharing should be under user control, the content sent through network had received by generating 160 bit key for user and 128 bit symmetric key by AES module. The input data generates manifest file with metadata information and media data information and encrypted signature. This can be downloaded by subscriber, but he/she must have necessary keys and authorization to the file. The trusted key management handles all the process.

Sandeep Sahu, Aditi Bhadoria [15] described about their proposed method where data has been encrypted using image and algorithm used for multilevel security. For establishing a method for securing data over the cloud, they had survey from available information about security of data, like Kerberos and pretty good privacy. In this paper, it was assumed that data over the cloud can be stolen during the transmission before it reaches to the cloud. Kerberos and PKI were implemented together for data security. User registered to Kerberos, which gives user a ticket as well as CSP (Cloud service provider) to communicate with each other. PKI is used to authenticate user and send information to service provider and PGP send user encrypted data to the cloud.

Dinesha H A CORI, Agrawal V K CORI [16] described authentication at different levels of cloud computing. As for an application used in an organization, at first level to provide password generated, it was for ensuring the access from the vendor. At second level, a team level password had generated for authentication the team for cloud service. At more levels, authentication can be done but at last level user was authenticated with password. It had described user permissions. The organization for which process was done actually a service provider, who provides multilevel authentication to the client. An algorithm was necessary to provide security to restrict the use of service.

Shigeaki Tanimoto, Toshihiko Moriya, Hiroyuki Sato and Atsushi Kanai [17] described the secure usage and safe achieving of ICT environment at the universities by the construction of PKI (Public Key Infrastructure). PKI had not widely constructed due to cost, in this paper firstly they re-examining the multi-policy of conventional and then add the dynamic evaluation was based on real operations performed. They use the three layer architecture of UPKI (University Public Key Infrastructure), in this open domain PKI, campus PKI, grid PKI are the three layers, by using this technique the cost reduced up to 30 percent.

Allen Oommen Joseph, Jaspher W. Kathrine and Rohit Vijayan [18] described the various security mechanisms which are provided in the enterprise. Cloud computing is open area, so many security issues arises time to time, they use some security mechanism and show the protection of database. Four types of clouds are present public, private, hybrid and community cloud. First mechanism was authentication, by using this mechanism we ensure that data had stored on cloud only by the right person i.e authenticated person. They used RSA, single sign-on for reduce the cost and improve the security like secure against honey pot attack and against dictionary attack. Second mechanism was authorization, in this user submit its user identity for login into particular web service. There were multiple vendors like ORACLE, OASIS CLOUD and VMware use the oracle database vault, cloudAuthz and two factor hard and soft tokens. Third mechanism was encryption, in this user encrypted its data and stored on the cloud by using full disk encryption and hardware/software based encryption. Fourth mechanism was access control, means data was provided only to the authorized persons. MCCAFEE and FUJITSU were the vendors of access control.

Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem [19] described the new security architecture for cloud computing for ensuring the secure communication system and hiding the information from others. They used

AES for encryption and asynchronous key system for exchanging the information and MD5, they also used one time password for user authentication process. In this paper they had security on one end means between user and the system not between system and storage. RSA had been used for encrypting process and it use the public key of the system for encryption process.MD5 had been used for hashing purpose means hiding the information, in this paper user login with the help of username and it use the RSA then system sends the otp to the user.

Gaurav Raj, Ram Charan Kesireddi and Shruti Gupta [20] has been described the model based on AES (Advanced Encryption Standard) for encrypting the user data based on the requirement of user. In AES 128-bit, 192-bit and 256-bit key length is used for encrypting and decrypting process. In the proposed model user can encrypts the data based on his requirement. In the first step, user divides the data into three ways; small for 128-bit, medium for 192-bit and large for 256-bit. Now user select the data of encryption or decryption then choose the key length means method for encryption like 128-bit, 192-bit or 256-bit and upload the data on the cloud.

Shui.Han and J.X [21] proposed a model for ensuring the data storage by using third party auditor scheme in cloud computing. In the proposed model, a new trusted third party is introduced in which user can store and operate their confidential data on the cloud. In cloud computing the security of stored data is big challenge for the researchers. For more security to the stored data on the cloud a new scheme is proposed; a noval third party auditor. In the proposed model a trusted third party auditor is used so it reduces the complexity of the system. The third party auditor provides techniques like: Bilinear diffie-hellman and RSA. By using RSA data is encrypted from sender to receiver and by using bilinear keys are exchanged within sender and receiver. With exchanging the keys, data is always sent to valid and authorized user.

Nivedita Shimbre and Prof. Priya Deshpande [22] proposed a model to enhance the distributed cloud data security with the help of AES and TPA algorithms. When the file is distributed then the data which is stored in a file is also segmented, so we need high level of security for the data. In the proposed model SHA-1 (Secure hash Algorithm) is used. Every block of data has its own hash code; with the help of hash code user authentication process is also enhanced. The data is encrypted with AES because we need to store confidential data on the cloud. The third party auditor has been used for public auditing. Proposed model is very efficient and secured as compare to others.

S.IShaik Hussain and V.Yuvaraj [23] proposed a method which is used for secure data access using AES (Advanced Encryption Standard) over the cloud storage. In this paper P2P (Peer to Peer) computing has been described with the help of AES and double encryption namely ABE and PRE. These encryption techniques are based on user attributes. Firstly owner of the data simply encrypts the plaintext into cipher text with the help of symmetric encryption, ACP, Attributes of the user, environment and cloud. In the second phase PRE is implemented on encrypted data for increase the security level of data. The decryption process is almost same as encryption. In the first step of proposed algorithm, the system has been setup after that encrypts the data and uploads to P2P storage. In the next step, add the new user into existing system and gave the rights to access by the admin. In the last step, user decrypts the data from P2P cloud storage. The proposed model provides secure, efficient and fine-grained data access control for the P2P cloud storage. It provides the integrity to data and reduces the encryption-decryption time as compared to other models.

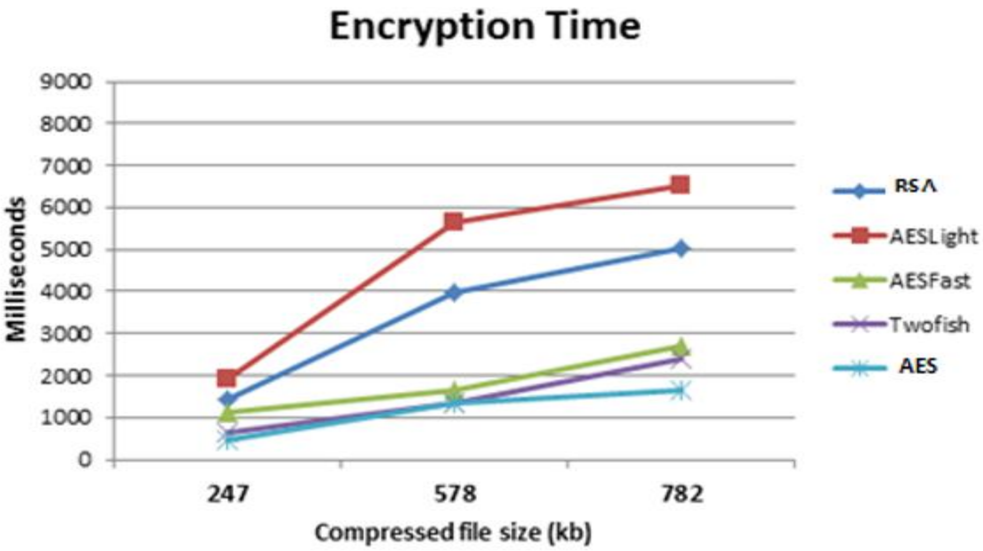


Figure 2.1- Comparison between encryption times

Dhaval Patel, M.B.Chaudhari [24] described the usage of three step mechanism like digital signature, diffie Hellman and AES for cloud security. Security had been considered as important aspect because data can be stored on any location which is not in user control. There were number of attacks on cloud like Tampering, repudiation, information disclosure etc. In this paper, they had been used two processes one is uploading and second is downloading the file. In the file uploading process firstly user generated message digest using of SHA and signed it using private key of RSA algorithm, then AES had been used for data encryption and then computer verifies the signature and stored the file on the server. In the file downloading process, computer firstly retrieved the data from storage then apply decryption algorithm and extract the signature and then verified. By using the mechanisms, the user had been checked for authorization.

Shobha Rajak, Ashok Verma [25] described the way of securing the data which had been stored on the cloud. They used the CFX_MF algorithm with digital signature. Attacks on the user name and password has been prevented by use of digital signature, the technique improved the authentication and non-repudiation of the message. The purposed algorithm had been divided into two parts- server and client. Sever worked on the user authentication and identify the program in the server. Authentication has been performed at client side. The Process had started with server by the username and password, server generated the key and sent to the user, on the client side key had been checked and gave the access control.

Aditya Harbola, DeeptiNegi, Deepak Harbola [26] described about the services which are provided by Internet Service Provider (ISP). There was an authentication subscriber check for access authorization. This process was for cost recovery, resource planning service and billing. In this paper the authors proposed a new authentication protocol named AAA Kerberos protocol. This protocol had been used for distributed system but the traditional protocol cannot work with distributed systems. Authorization, accounting of service usage are the components of distributed system. AAA stands for authentication, authorization and accounting. It had provided framework for managing the challenges for multiple network platforms. It consisted of a user profile’s data and data of configuration which can communicate with AAA clients. There, AAA server had a centralized server for comparing the authentication applied by user with the authentication which has been stored in database. There are number of attacks in Kerberos like password guessing attack, application system security, timestamp problem and secure storage for session key. A new protocol had based on Kerberos, in this they divides the entire process into two phases. First phase was service which means user was authenticated first and then he will use the service. Second phase was accounting means measure the usage of service which can be verified using database.

YaserFuad, Al Dubai and Dr. Khamitkar [27] described about access control security, issues and attacks. Kerberos had acted as authentication protocol model for cloud based systems. Kerberos had provided single sign-on and prevent against DDOS attack in access control systems. This model helped to provide filtering against unauthorized access to reduce the burden and memory usage of cloud for authentication checks for each client. It had acted as third party between client and server to allow the secure access to cloud services. In the single sign based systems, client acted as single initial sign-on to an identity provider. The existing system was role based model which uses the combined cryptographic techniques to use the access control provider and cipher text can only be to decrypted by the users who satisfied the specification of RBAC(role based accessing control). It was difficult for single administrator to handle the larger systems. RBAC was unable to provide the fine-grained access .So the existing system does not meet the security requirements as they were expected. After examining the existing work, a new system had been designed KARBAC (Kerberos authentication role based access control). KARBAC had worked with cloud client authentication protocols, gateway, cloud application, authorization server. Authorization server decided about the authorization with the help of RBAC data base engine. Gateway identified cloud client and service components and manages session and connection manages .the unauthorized access can be overcome by using this model. It was difficult to decrypt, because password was not stored anywhere and cryptographic algorithms were used to do encryption. The future work of Purposed system wills its complex structure.

Aeri Lee [28] proposed the authentication scheme for smart learning system in cloud computing environment. Smart learning had features like portability, mobility, motivation, efficiency and so on. Various authentication techniques had used id password, public key certificate, and multi-factor authentication. Single sign on, mobile trusted module. The various attacks like mobile trusted module, replay attack and password attack. The proposed scheme allowed the user to access the smart learning system through user authentication service by two factor methods, the mixture of USIM_id and login information of ID and password .USIM_ID was provided by user to server for authorization and server encryption and sent against the user. The user encrypted the key. User had two keys, compared to values useful for running applications. The user had requested to access and registration was done, the server performed XOR operation with USIM_ID and random number RND. The authentication server generates user's key with existed secret key. Verified the timestamp which had been created by authentication server, if it was valid the server generates new key and verified the USIM_ID and value of time stamp. If values were equal, the user has been authenticated by smart learning system. This method of authentication provided the mutual authentication, integrity.

Sowmiy Murthy [29] proposed a secure cloud storage model that addressed security and removed the storage issue from cloud computing environment. The various security related improvements had done in this model, the model implemented centralized architecture with mutual KDC structure and implemented a role based access control .the digital signature had been used for anonymous authentication .storage related improvements ,implemented a strong encryption and decryption technique by using homomorphism encryption and automatic data retrieval had implemented. The proposed model had multiple numbers of KDC for key distribution and for management. The first level of authentication has been achieved by registration process. User was identified as legitimate user and authentication process was done by trusted third party. The trustee system generated token for the user and it was passed to KDC for generating the keys .the secure file storage purpose had accomplished with homographic technique. It was implemented as encrypted key by using server .The files which were encrypted by using the keys generated by KDC .There was an access control policy for other users who wants to read or write a file, base 64 encoding algorithm was used for uploading the files on cloud. File replication and file replacement with string matching algorithm was implemented for data recovery. The proposed system was fast and secure in terms of recovery and file encryption.

Ms. Jasmin Bhambure, Ms. DhanashriChavan, Ms. Pallavi Band, Mrs.Lakshmi Madhuri [30] described about an authentication protocol. Kerberos was a network authentication protocol which has been designed to provide a strong authentication using secret key cryptography. The aim of the paper has to enhance the security of Kerberos by preventing it from replay attack. This paper presents improved method which protects replay attack by using steganography. A replay attack has been described when intruder steal data packet from the network and forward the packet to the service. The authentication server had created that was used to derive the steganography image from the user‘s password. Steganography and visual cryptography has been used to provide the security to the Kerberos. In this paper, they purposed a Kerberos system over an existing Kerberos system using the concept of steganography image key which encrypted the information in the form of stegano image.

CHAPTER 3
PRESENT WORK

3.1 Problem Formulation

The problem arises within the base paper techniques (AES) is high power consumption and high memory. It also consumes a lot of encryption/decryption time and upload/download time. Various attacks such as brute force, DoS (Denial of Services) are prevented but there are certain attacks such as XSL (eXtended Sparse Linearization) that breaks the algorithm.

Proposed work

To achieve the encryption /decryption process in QAES-128 must be follow the following steps:

- The quantum secret key is generated over the Quantum channel using BB84 protocol.
- The sender and the receiver parties check the online compatibility for the generated secret key.
- The system used diffie-hellman key exchanger method between client and cloud.
- Cloud simulates by Cloud sim and creates VM and broker environment.
- Cloud stores the encrypted data.
- The sender and the receiver choose the appropriate key length (128, 192, 256 bits) through the classical channels in order to perform the encryption/decryption process.
- The two parts deploy the selected final secret key to the symmetric encryption algorithm
 (AES).
- Encrypt the first block input file (P1-128bits) by the AES stages.
- The decryption process starts with the end of the Encryption process (inverse methodology).
- After completion of process, analysis of storage and time on the cloud side.

3.2 OBJECTIVE OF STUDY

Objective 1: To reduce the encryption and decryption time in the cloud environment.

Objective 2: To reduce the storage on the cloud.

3.3 RESEARCH METHODOLOGY

SENDER'S SYSTEM ARCHITECTURE

Step1. Register and login with correct login information.

Here, we will register with particular details and will use that detail to login into the panel.

Step2. Select a file you want to upload.

We will select a file which we want to store on the cloud.

Step3. Select or choose a key for encryption.

DH will generate two keys and we will choose the key that we want to use for encryption.

Step4. Apply QAES on selected file will generate an encrypted file.

We will apply hybrid encryption techniques to encrypt the file.

Step5. Apply elliptic curve cryptography on the selected file.

Step6. Now, Store encrypted file along with encrypted key in cloud.

Here, we will store the file on cloud

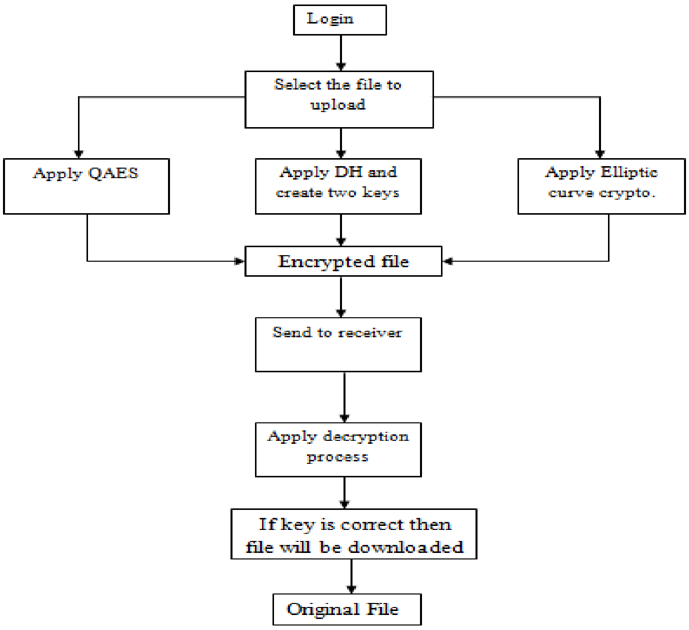

Login
Select the file to upload
Apply QAES
Apply DH and create two keys
Apply Elliptic curve crypto.
Encrypted file
Send to receiver
Apply decryption process
If key is correct then file will be downloaded
Original File

Figure 3.1- Flow chart of ECDHQAES

RECEIVER'S SYSTEM ARCHITECTURE

Step1. Login with correct information.

Login with personal details with which we have registered.

Step2. Select a file which you want to download from the cloud.

We will select a file which we want to download from the cloud.

Step4. Enter correct key to download file.

- If key is correct then allow access to download otherwise denied access to download.

Step5. Apply correct AES key on encrypted file.

- If key is correct then decrypt and allow access to the file otherwise denied accessibility.

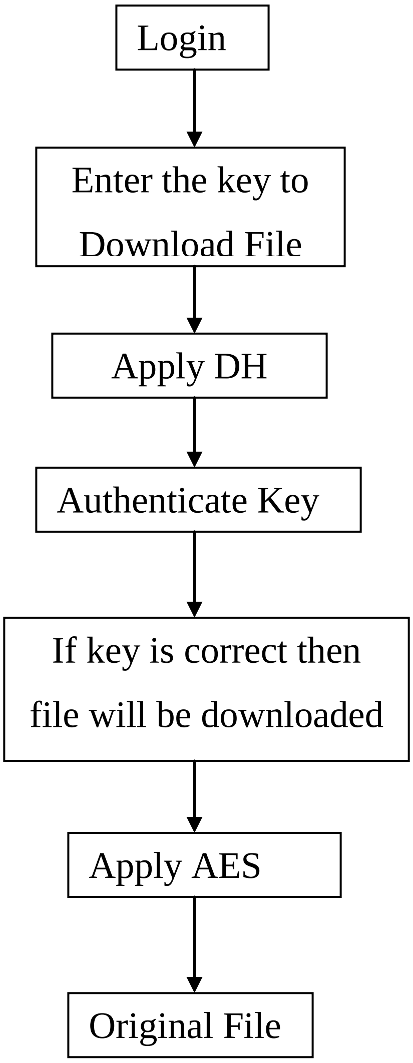

Login
Enter the key to Download File
Apply DH
Authenticate Key
If key is correct then file will be downloaded
Apply AES
Original File

Figure 3.2- Flow chart of decryption

CHAPTER 4
RESULT AND DISCUSSION

4.1 SIMULATOR: Cloudsim

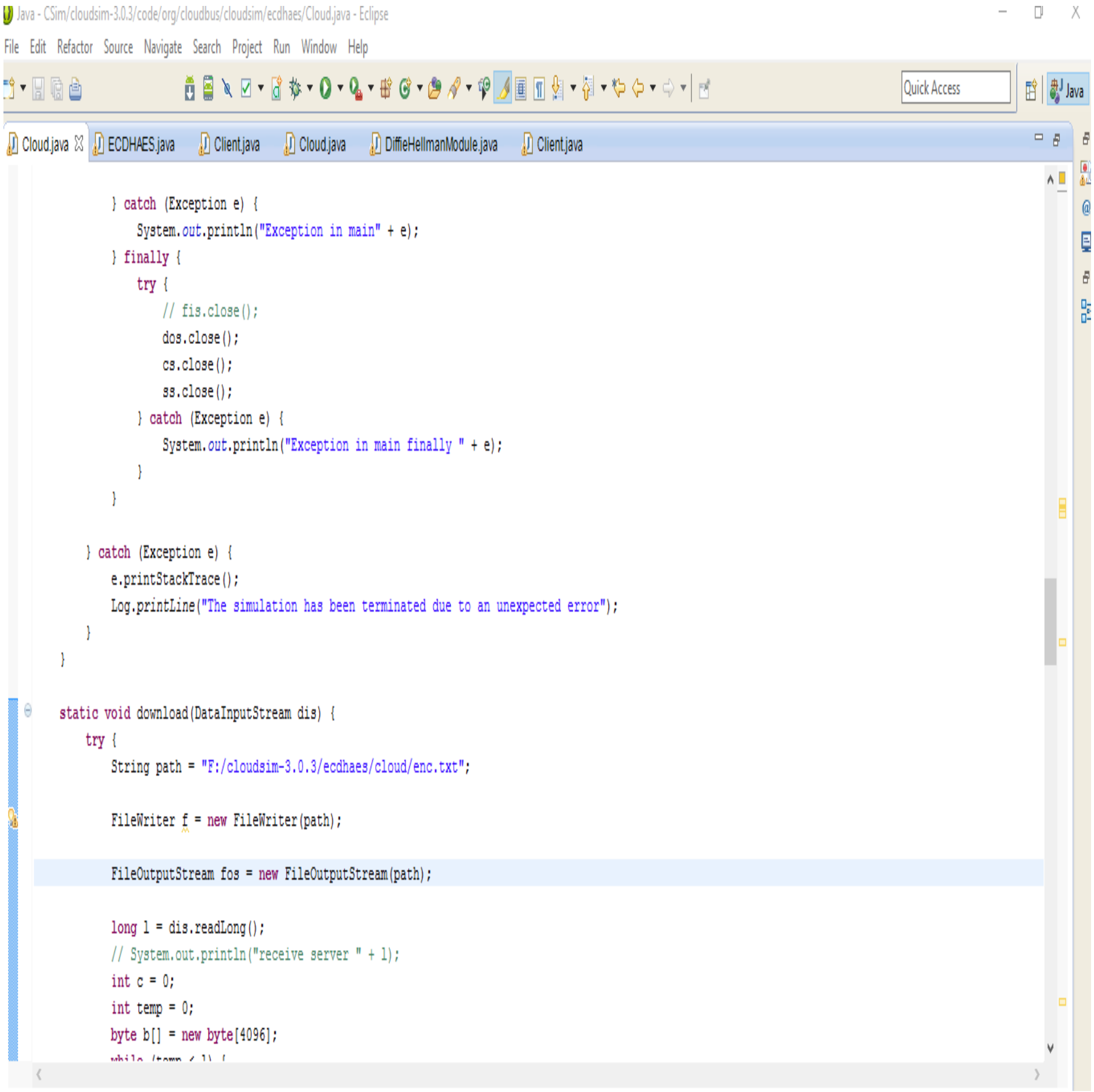
Cloudsim, which is a toolkit for the modeling and simulation of Cloud computing environments, comes to the rescue. It provides system and behavioral modeling of the Cloud computing components. Simulation of cloud environments and applications to evaluate performance can provide useful insights to explore such dynamic, massively distributed, and scalable environments.

The principal advantages of simulation are:

- Flexibility of defining configurations
- Ease of use and customization
- Cost benefits: First designing, developing, testing, and then redesigning, rebuilding, and retesting any application on the cloud can be expensive. Simulations take the building and rebuilding phase out of the loop by using the model already created in the design phase.
- Cloudsim is a toolkit for modeling and simulating cloud environments and to assess resource provisioning algorithms

Steps:

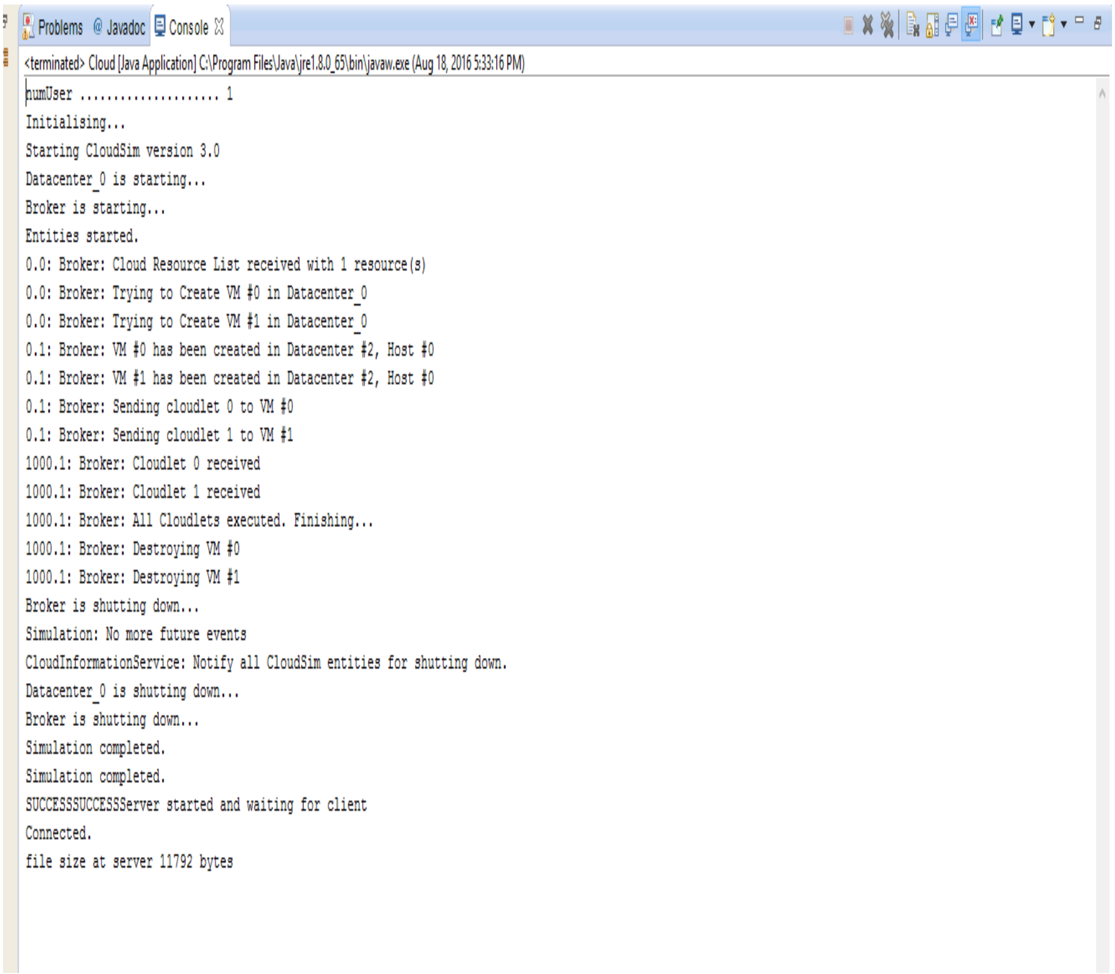
- Firstly we run the cloud.java file of any algorithm which is on simulator and it waiting for the client.
- In the second step, when cloud is running successfully then run the client of that particular algorithm.
- In the next step, check the value in the console mode.


Java - CSim/cloudsim-3.0.3/code/org/cloudbus/cloudsim/ecdhaes/Cloud.java - Eclipse
File Edit Refactor Source Navigate Search Project Run Window Help
Quick Access
Java
Cloud.java
ECDHAES.java
Client.java
Cloud.java
DiffieHellmanModule.java
Client.java

```java
            } catch (Exception e) {
                System.out.println("Exception in main" + e);
            } finally {
                try {
                    // fis.close();
                    dos.close();
                    cs.close();
                    ss.close();
                } catch (Exception e) {
                    System.out.println("Exception in main finally " + e);
                }
            }

        } catch (Exception e) {
            e.printStackTrace();
            Log.printLine("The simulation has been terminated due to an unexpected error");
        }
    }

    static void download(DataInputStream dis) {
        try {
            String path = "F:/cloudsim-3.0.3/ecdhaes/cloud/enc.txt";

            FileWriter f = new FileWriter(path);

            FileOutputStream fos = new FileOutputStream(path);

            long l = dis.readLong();
            // System.out.println("receive server " + l);
            int c = 0;
            int temp = 0;
            byte b[] = new byte[4096];
            while (temp < l) {
```

Figure 4.1- Simulation environment

In Fig. 4.1, shows the Cloudsim simulator, in which cloud.java, client.java files for the both algorithms means DHAES (previous one) and ECDHQAES (Proposed one).



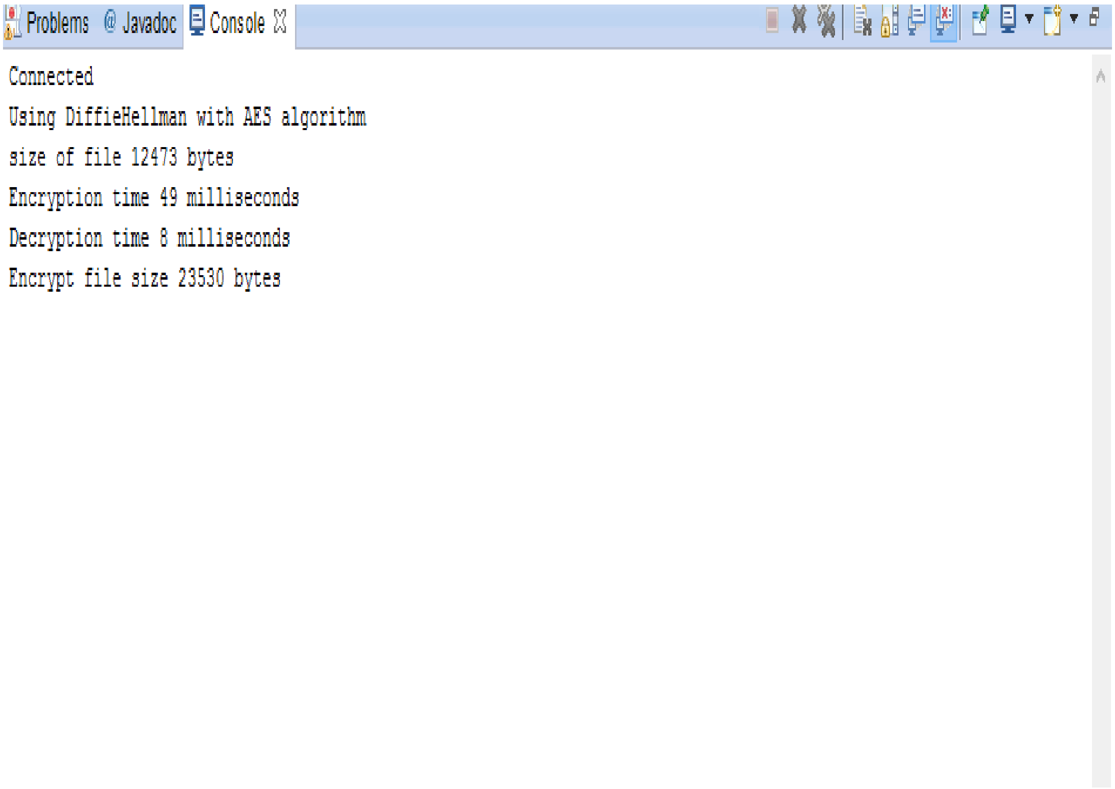
```
<terminated> Cloud [Java Application] C:\Program Files\Java\jre1.8.0_65\bin\javaw.exe (Aug 18, 2016 5:33:16 PM)
numUser .................... 1
Initialising...
Starting CloudSim version 3.0
Datacenter_0 is starting...
Broker is starting...
Entities started.
0.0: Broker: Cloud Resource List received with 1 resource(s)
0.0: Broker: Trying to Create VM #0 in Datacenter_0
0.0: Broker: Trying to Create VM #1 in Datacenter_0
0.1: Broker: VM #0 has been created in Datacenter #2, Host #0
0.1: Broker: VM #1 has been created in Datacenter #2, Host #0
0.1: Broker: Sending cloudlet 0 to VM #0
0.1: Broker: Sending cloudlet 1 to VM #1
1000.1: Broker: Cloudlet 0 received
1000.1: Broker: Cloudlet 1 received
1000.1: Broker: All Cloudlets executed. Finishing...
1000.1: Broker: Destroying VM #0
1000.1: Broker: Destroying VM #1
Broker is shutting down...
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for shutting down.
Datacenter_0 is shutting down...
Broker is shutting down...
Simulation completed.
Simulation completed.
SUCCESSSUCCESSServer started and waiting for client
Connected.
file size at server 11792 bytes
```

Figure 4.2- Running cloud

In Fig. 4.2, shows the running cloud on the simulator. When we run the cloud.java file from simulation environment then it waiting for the client and before that broker is start and then cloud is successfully running.

File name- File 1

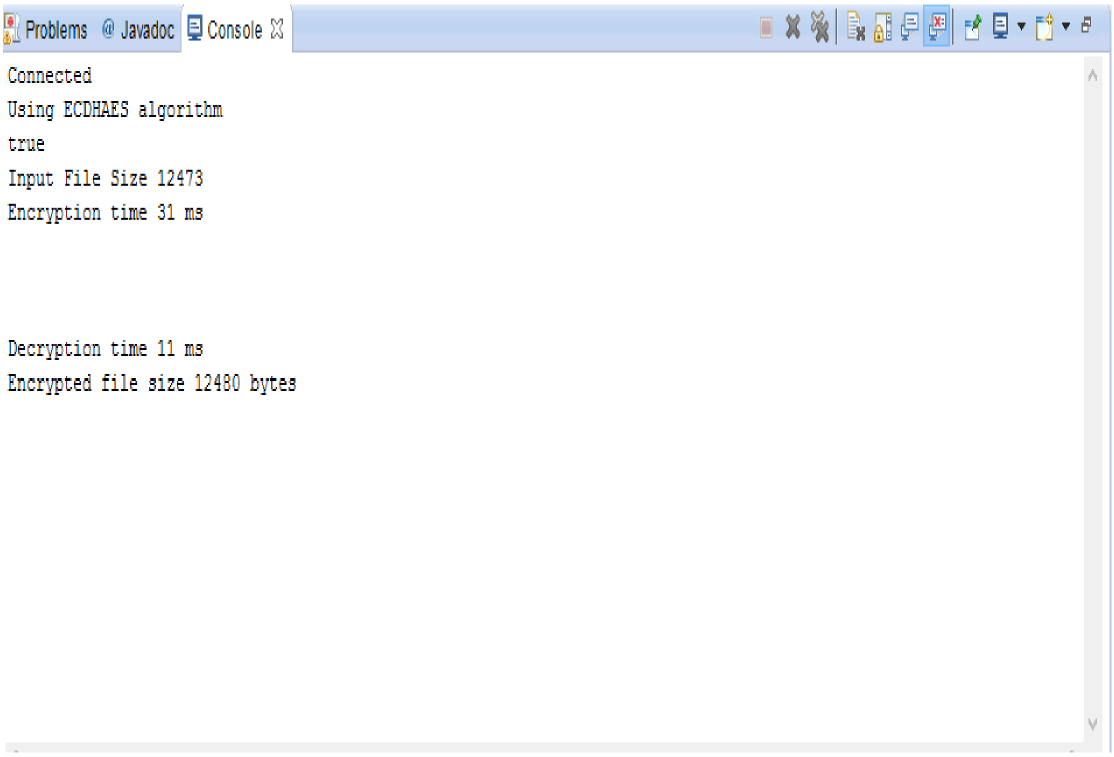
File size- 12473 bytes



```
Connected
Using DiffieHellman with AES algorithm
size of file 12473 bytes
Encryption time 49 milliseconds
Decryption time 8 milliseconds
Encrypt file size 23530 bytes
```

Figure 4.3- Result using DHAES (File 1)

In Fig. 4.3, shows the result of File 1 using DHAES algorithm. It encrypts the file and then decrypts the same file within 57 ms. File size after encryption is 23530 bytes.



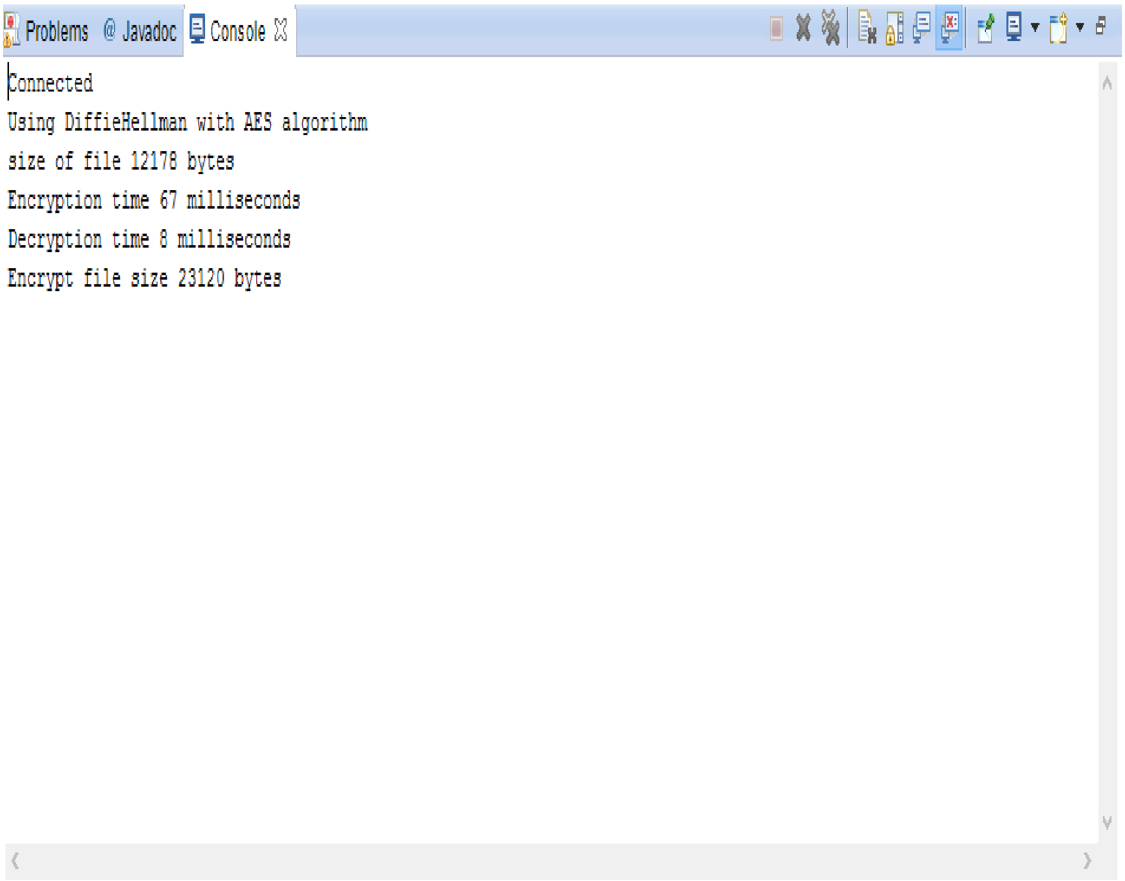
```
Connected
Using ECDHAES algorithm
true
Input File Size 12473
Encryption time 31 ms



Decryption time 11 ms
Encrypted file size 12480 bytes
```

Figure 4.4- Result using ECDHQAES (File 1)

In Fig. 4.4, shows the encryption, decryption time and encrypted file size which is calculated by using ECDHQAES (proposed algorithm).

File name- File 2

File size- 12178 bytes

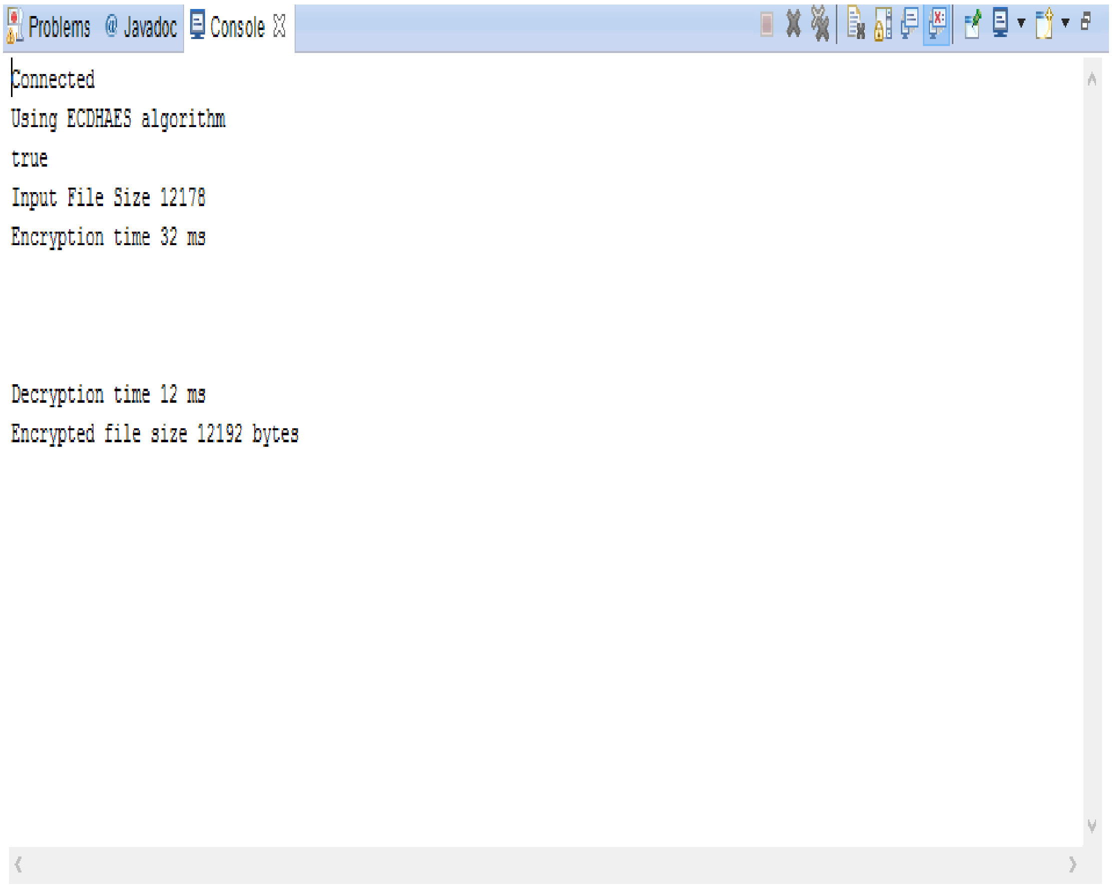


```
Connected
Using DiffieHellman with AES algorithm
size of file 12178 bytes
Encryption time 67 milliseconds
Decryption time 8 milliseconds
Encrypt file size 23120 bytes
```

Figure 4.5- Result using DHAES (File 2)

In Fig. 4.5, shows the result of File 2 using DHAES algorithm. It encrypts the file and then decrypts the same file within 75 ms. File size after encryption is 23120 bytes.

In Fig. 4.6, shows the result of File 2 using ECDHQAES algorithm. It encrypts the file and then decrypts the same file within 44 ms. File size after encryption is 12192 bytes.

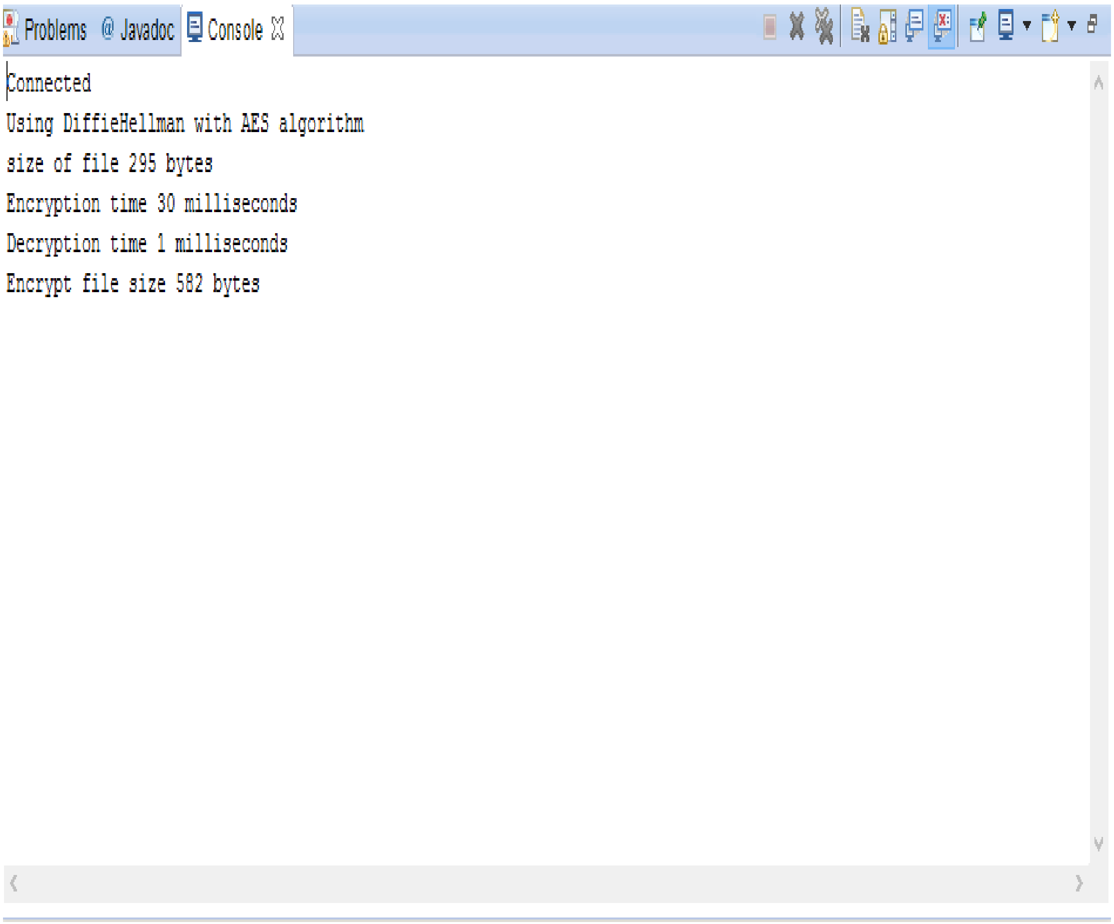


```
Connected
Using ECDHAES algorithm
true
Input File Size 12178
Encryption time 32 ms



Decryption time 12 ms
Encrypted file size 12192 bytes
```

Figure 4.6- Result using ECDHQAES (File 2)

File name- File 3

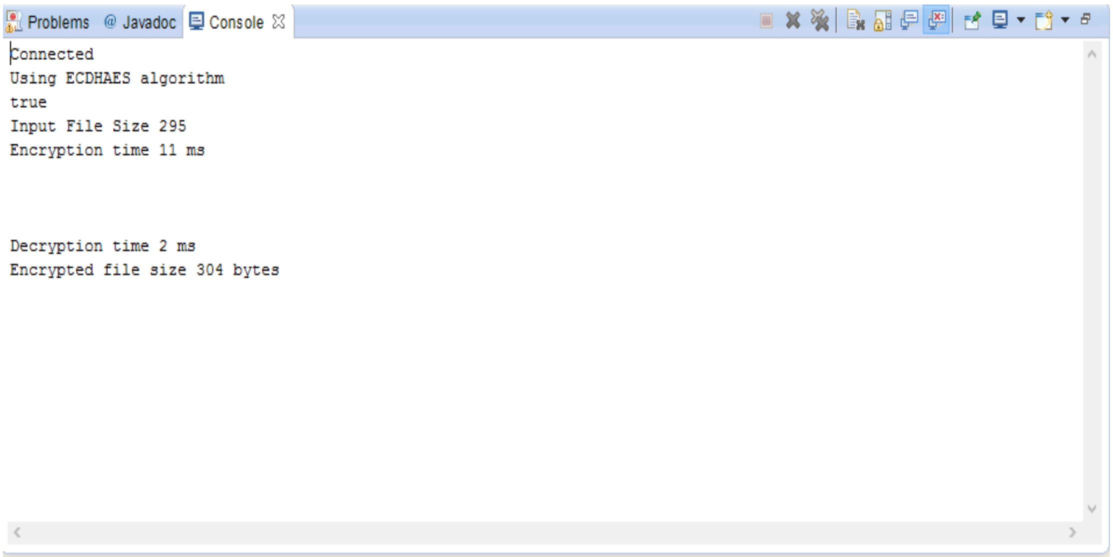
File size- 295 bytes



```
Connected
Using DiffieHellman with AES algorithm
size of file 295 bytes
Encryption time 30 milliseconds
Decryption time 1 milliseconds
Encrypt file size 582 bytes
```

Figure 4.7- Result using DHAES (File 3)

In Fig. 4.7, shows the result of File 3 using DHAES algorithm. It encrypts the file and then decrypts the same file within 31 ms. File size after encryption is 582 bytes.



```
Connected
Using ECDHAES algorithm
true
Input File Size 295
Encryption time 11 ms



Decryption time 2 ms
Encrypted file size 304 bytes
```

Figure 4.8- Result using ECDHQAES (File 3)

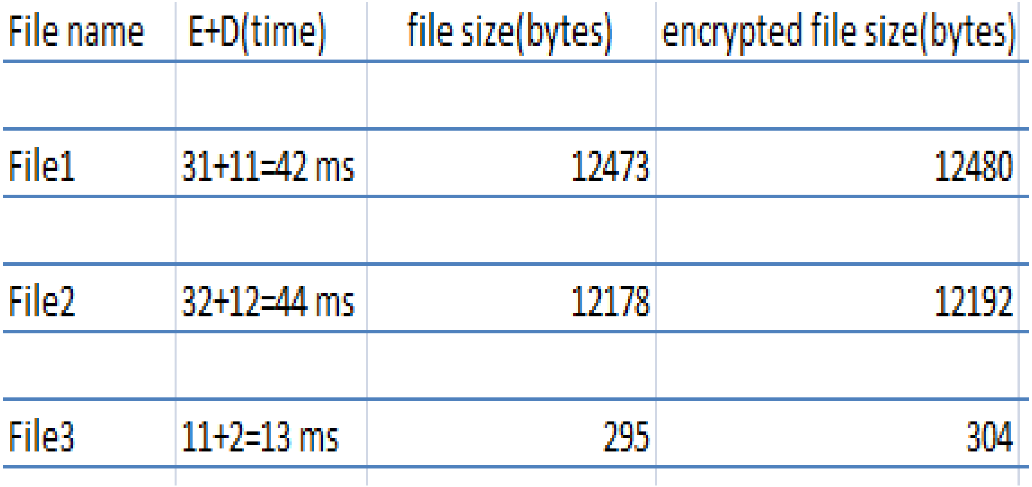
In Fig. 4.8, shows the result of File 3 using ECDHQAES algorithm. It encrypts the file and then decrypts the same file within 13 ms. File size after encryption is 304 bytes.

It shows that, when we use the ECDHQAES which is proposed algorithm the encryption and decryption time is less as compared to previous one DHAES. The proposed algorithm also reduce the storage on the cloud

4.2 Experimental Result

In this table, we show the file name, encryption and decryption time, file size and encrypted file size which are less than DHAES.

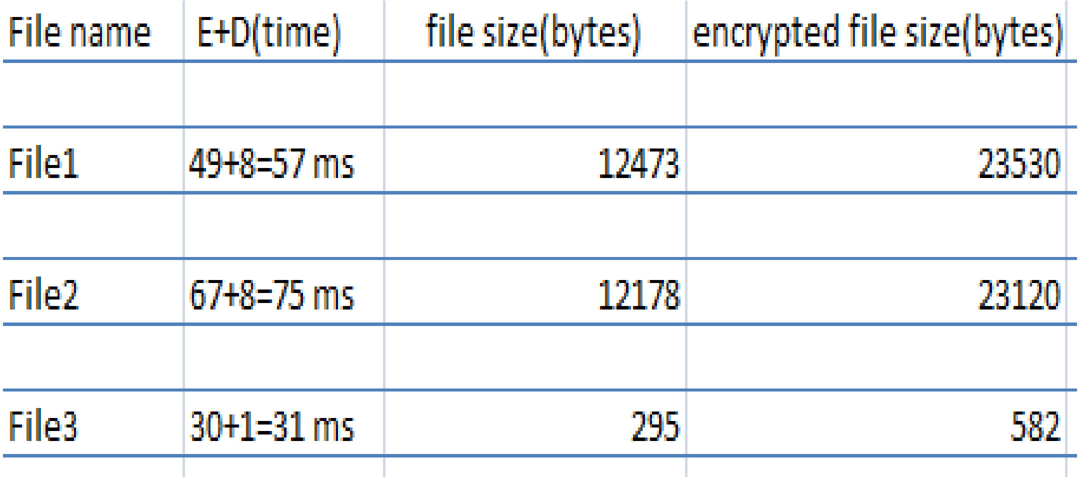
Table 4.1- Result of ECDHQAES (Proposed work)



File name	E+D(time)	file size(bytes)	encrypted file size(bytes)
File1	31+11=42 ms	12473	12480
File2	32+12=44 ms	12178	12192
File3	11+2=13 ms	295	304

In this table, we show the file name, encryption and decryption time, file size and encrypted file size which are more than ECDHQAES.

Table 4.2- Result of DHAES



File name	E+D(time)	file size(bytes)	encrypted file size(bytes)
File1	49+8=57 ms	12473	23530
File2	67+8=75 ms	12178	23120
File3	30+1=31 ms	295	582

Graphs

Graph shows the two parameters for both (DHAES and CDHQAES) algorithms:

1. Encryption + Decryption time.

2. Encrypted file size.

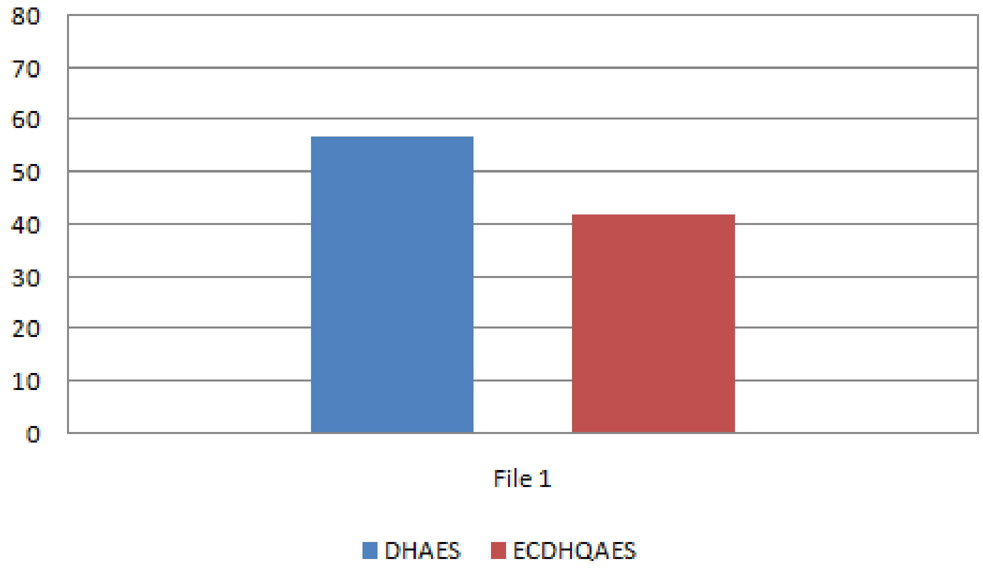


Figure 4.9- Comparison between E+D time (File 1)

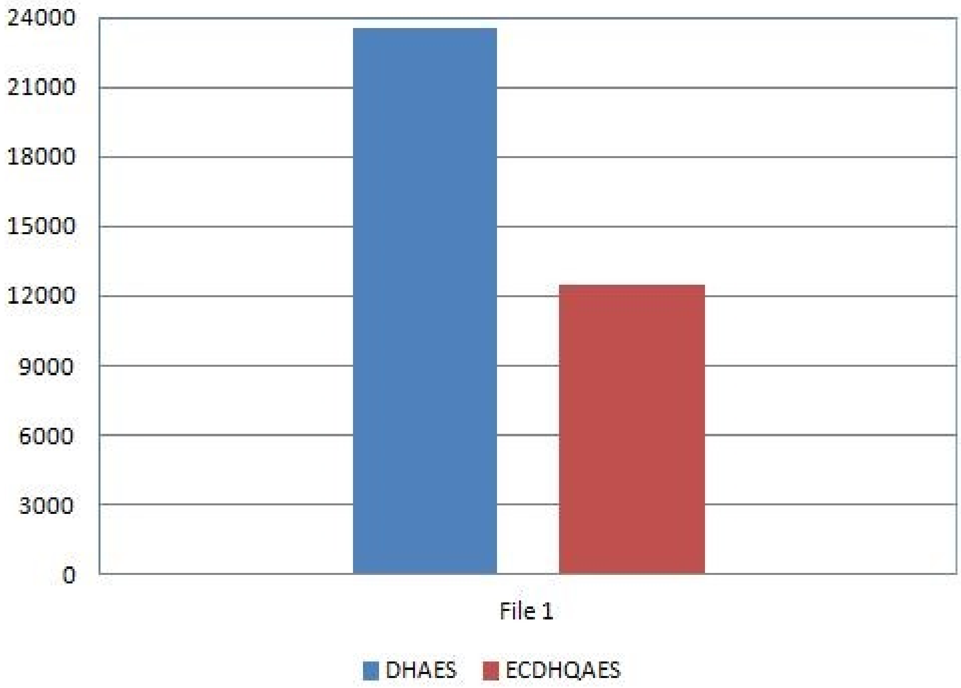


Figure 4.10- Comparison between encrypted file size (File 1)

In Fig. 4.9 and 4.10 shows the encryption + Decryption time and encrypted file size of file (File 1). The E + D time is shown in fig. 4.9, Blue graph shows the DHAES and red shows the ECDHQAES. It shows the variance in both the algorithms, proposed algorithm take less time for encryption and decryption as compared to DHAES and same in the case of encrypted file size.

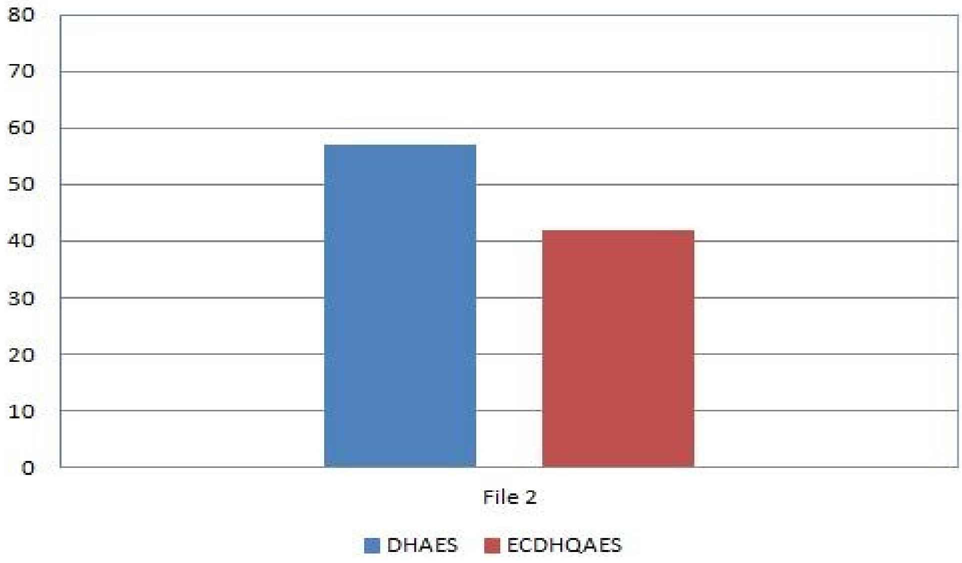


Figure 4.11- Comparison between E+D time (File 2)

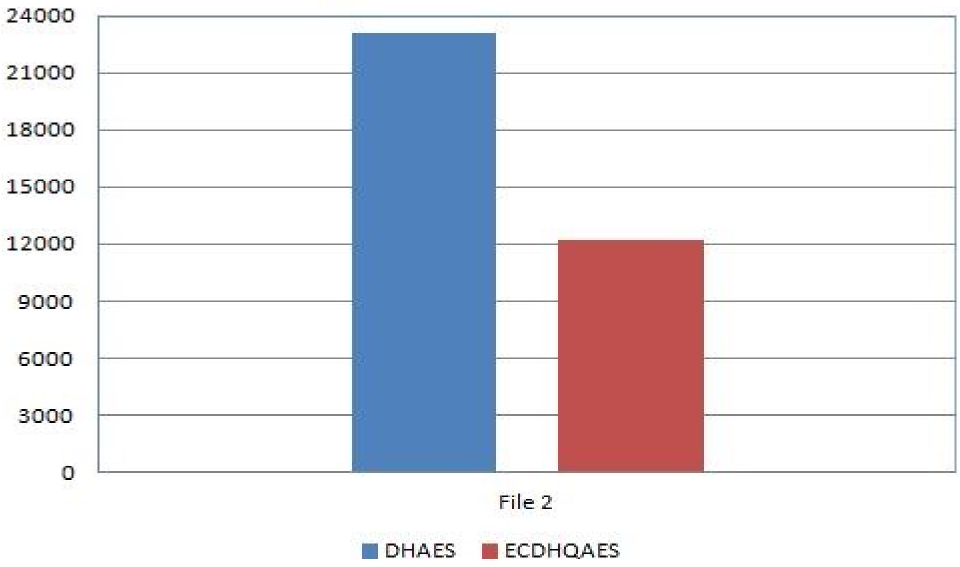


Figure 4.12- Comparison between encrypted file size (File 2)

In Fig. 4.11 and 4.12 shows the encryption + Decryption time and encrypted file size of file (File 1). The E + D time is shown in fig. 4.11, Blue graph shows the DHAES and red shows the ECDHQAES and encrypted file size is shown in the fig. 4.12. It shows the variance in both the algorithms, proposed algorithm take less time for encryption and decryption as compared to DHAES and same in the case of encrypted file size.

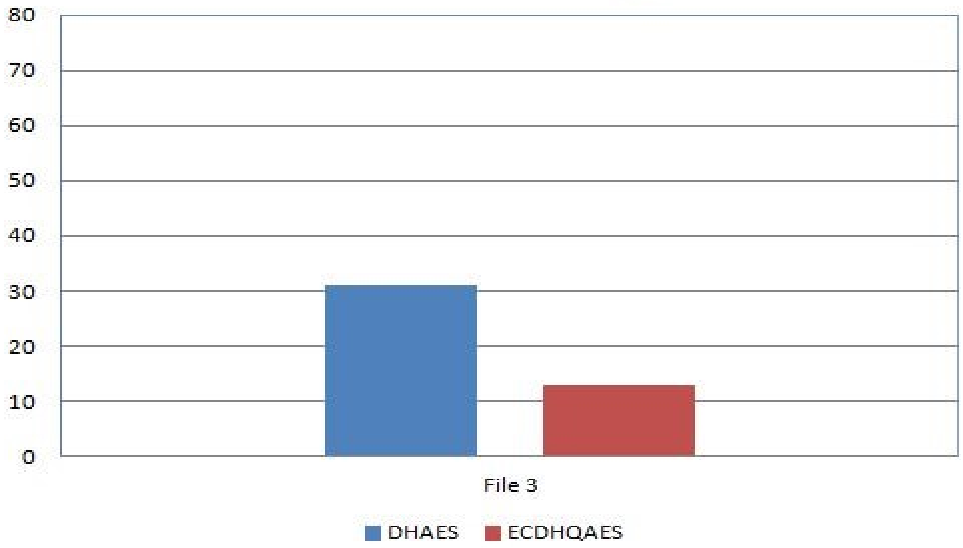


Figure 4.13- Comparison between E+D time (File 3)

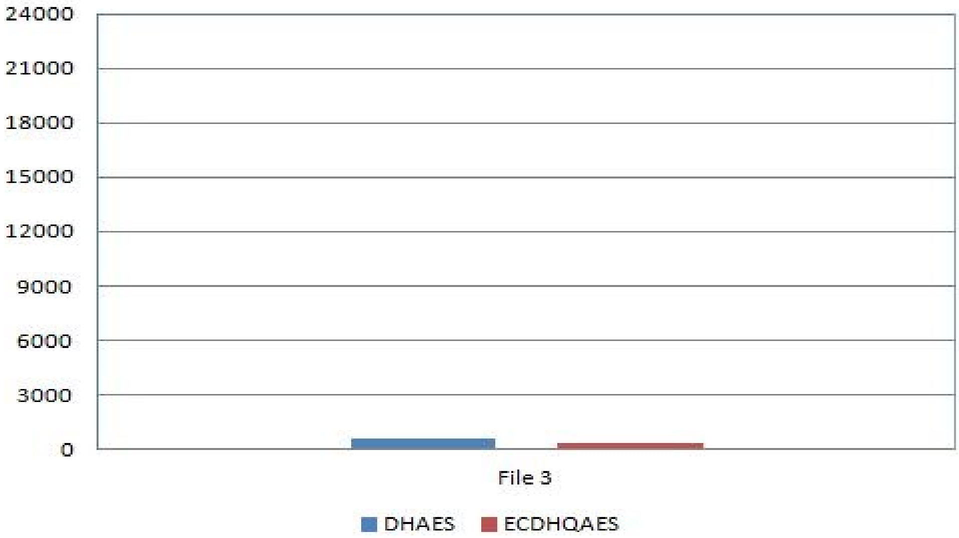


Figure 4.14- Comparison between encrypted file size (File 3)

In Fig. 4.13 and 4.14 shows the encryption + Decryption time and encrypted file size of file (File 1). The E + D time is shown in fig. 4.13, Blue graph shows the

DHAES and red shows the ECDHQAES. It shows the variance in both the algorithms, proposed algorithm take less time for encryption and decryption as compared to DHAES and same in the case of encrypted file size.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION

This report provides literature review to the cloud computing with its authentication techniques. In this report, various methods and techniques for implementing various levels of security using various cloud authentication and authorization schemes. There are many attacks in cloud environment and identity and access management holds the key to it. This report shows how I will work to maintain and enhance the security of cloud system by making secure access system.

Cloud computing is becoming a great approach for the business world and private use. As the cloud is widely used security is an important constraint .The proposed algorithm is based upon encryption and decryption using different keys, storage and the time taken by encryption and decryption process. This algorithm can reduce the encryption and decryption time of the selected file .Along with the time there is one another parameter that is storage. The size of the file is reduced which directly affect the storage area in bytes. The major concern was security .The cryptographic algorithms diffie-hellman, quantum -AES and elliptic curve cryptography is used to achieve the authentication and authorization. Diffie-hellman work as key exchanger between both the parties. Quantum-AES is advance encryption standard used to treat data as a block for encryption and decryption .Elliptic curve cryptography is used for public keys to compare the keys. Public cloud is unsecure to access, store and manage the data. The algorithm will work for public cloud as well as non – cloud environment.

5.2 FUTURE SCOPE:

The future scope of the algorithm is ,the enhancement in the proposed algorithm can handle the certain security attacks in cloud environment and it will work better for other parameters like automatic resource allocation ,data leak prevention, data access governance and many security audits.

REFERENCES

[1] Gehana Booth, Andrew Soknacki, and Anil Somayaji, "Cloud Security: Attacks and Current Defenses", 8th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'13), JUNE 4-5, 2013, ALBANY, NY.

[2] Ajey Singh, Dr. Maneesh Shrivastava," Overview of Attacks on Cloud Computing", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[3] Shikha Singh, Binay Kumar Pandey, Ratnesh Srivastava, Neha rawat,Poonam rawat, Awantika, "Cloud Computing Attacks: A DiscussionWith Solutions**",** OPEN JOURNAL OF MOBILE COMPUTING AND CLOUD COMPUTING, Volume 1, Number 1, August 2014.

[4] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", Recommendations of the National Institute of Standards and Technology, September 2011, Special Publication 800-145.

[5] Cloud Computing Bible. (2011)*Wiley Publishing, Inc*., Indianapolis, Indiana, p25.

[6] http://www.ibm.com/developerworks/cloud/library/cl-cloudserviesliaas.

[7] J. S. Wang, C. H. Liu, G. T. R. Lin, "How to Manage Information Security in Cloud Computing", IEEE, 2011, pp. 1405-1410.

[8] Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi, Shirin Dabbaghi Varnosfaderani, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", 978-1-4799-2027-3/14/$31.00 ©2014 IEEE.

[9] C. Tien-Ho, Y. Hsiu-lien and S. Wei-Kuan, "Elliptic Curve Cryptosystem (ECC) based on dynamic ID-Based remote mutual authentication", IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICJJECS)2015, © 2015 IEEE.

[10] Jen-Ho Yang, Pei-Yu Lin, “An ID-Based User Authentication Scheme for Cloud Computing”, 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, © 2014 IEEE.

[11] Dr.V.Venkatesa Kumar and A.Murugavel, “ENSURING CONSISTENCY FILE AUTHENTICATION OVER ENCRYPTED FILES IN THE CLOUD”, 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICIIECS) 2015, 978-1-4799-6818-3/15/© 2015 IEEE.

[12] Subhash Chandra Patel, Ravi Shankar Singh, Sumit Jaiswal, “Secure and Privacy Enhanced Authentication Framework for Cloud Computing”, SECOND INTERNATIONAL CONFERENCE ON ELECTRONICS AND COMMUNICATION SYSTEMS (ICECS ‘2015), 978-1- 4788-7225 - 8/15/©2015 IEEE.

[13] Wei-Tsung Su, Wo-Chen Liu, Chao-Lieh Chen, Tsung-Pao Chen, “Cloud Access Control in Multi-layer Cloud Networks”, International Conference on Consumer Electronics-Taiwan (ICCE-TW)-2015, 978-1-4799-8745-0/15/©2015 IEEE.

[14] Cristian PERRA, “A Framework for User Control Over Media Data Based on a Trusted Point”, IEEE International Conference on Consumer Electronics (ICCE)-2015, 978-1-4799-7543-3/15/©2015 IEEE.

[15] Sandeep Sahu, Aditi Bhadoria, “Data Privacy over the Cloud Using Differential Evolution Algorithm”, International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 4, Special Issue September 2015.

[16] Dinesha H A CORI, Agrawal V K CORI, “Multi-level Authentication Technique for Accessing Cloud Services”, ICCCA, 2012 International Conference on, vol., no., pp.1-4, 22-24 Feb. 2012

[17] Shigeaki Tanimoto, Toshihiko Moriya, Hiroyuki Sato and Atsushi Kanai, “Improvement of Multiple CP/CPS based on Level of Assurance for Campus PKI Deployment”, IEEE SNPD 2015, June 1-3 2015, Takamatsu, Japan.

[18] Allen Oommen Joseph, Jaspher W. Kathrine and Rohit Vijayan, "Cloud Security Mechanisms for Data Protection: A Survey", International Journal of Multimedia and Ubiquitous Engineering Vol.9, No.9 (2014).

[19] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem, "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.

[20] Gaurav Raj, Ram Charan Kesireddi and Shruti Gupta, "Enhancement of Security Mechanism for Confidential Data using AES-128, 192 and 256bit Encryption in Cloud", 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015, ©2015 IEEE.

[21] Shui.Han, J.X, "Ensuring data storage through a noval third party auditor scheme in cloud computing", IEEE computer science and technology, pp-264-268.

[22] Nivedita Shimbre and Prof. Priya Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm", International Conference on Computing Communication Control and Automation, © 2015 IEEE DOI-10.1109/ICCUBEA.2015.16.

[23] S.IShaik Hussain and V.Yuvaraj, "A SECURE DATA ACCESS CONTROL METHOD USING AES FOR P2P STORAGE CLOUD", IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICJJECS)2015, © 2015 IEEE.

[24] Dhaval Patel, M.B.Chaudhari, "DATA SECURITY IN CLOUD COMPUTING USING DIGITAL SIGNATURE", International Journal For Technological Research In Engineering Volume 1, Issue 10, June-2014, ISSN (Online): 2347 – 4718.

[25] Shobha Rajak, Ashok Verma, "Secure Data Storage in the Cloud using Digital Signature Mechanism", International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012, ISSN: 2278 – 1323.

[26] Aditya Harbola, Deepti Negi, Deepak Harbola, “A NEW A3 KERBEROS MODEL”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, March 2012, pp.- 290-293.

[27] YaserFuad Al-Dubai & Dr. Khamitkar S. D, “Kerberos: Secure Single Sign-on Authentication Protocol Framework for Cloud Access Control”, Global Journal of Computer Science and Technology: B Cloud and Distributed Volume 14 Issue 1 Version 1.0 Year 2014.

[28] Aeri Lee, “Authentication scheme for smart learning system in the cloud computing environment”, J Comput Virol Hack Tech (2015), © Springer-Verlag France 2015.

[29] Sowmiya Murthy, “CRYPTOGRAPHIC SECURE CLOUD STORAGE MODEL WITH ANONYMOUS AUTHENTICATION AND AUTOMATIC FILE RECOVERY”, ICTACT JOURNAL ON SOFT COMPUTING, vol. 05, oct.-2014.

[30] Ms. Jasmin Bhambure, Ms. Dhanashri Chavan, Ms. Pallavi Band, Mrs.Lakshmi Madhuri,” Secure Authentication Protocol in Client – Server Application using Visual Cryptography”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014, pp.- 556-560.

APPENDIX

IAAS	Infrastructure as a service
PAAS	Platform as a service
SAAS	Software as a service
KDC	Key distribution center
RBAC	Role based access control
KARBAC	Kerberos authentication role based access control
SHA	Secure hash algorithm
AES	Advance encryption standard
PKI	Public key infrastructure
CSP	Cloud service provider
DHAES	Diffie-Hellman Advance Encryption Standard
ECDHQAES	Elliptic Curve Diffie-Hellman Quantum Advance Encryption Standard