# A 5-Level Security Approach for Data Storage in Cloud

Bina Kotiyal, Priti Saxena, R. H. Goudar, Rashmi M. Jogdand
Department of Computer Science and Engineering, Graphic Era University
Dehradun (Uttarakhand), India

## ABSTRACT

Everyone in the IT world is bustling with the cloud computing concept. Conversing about the catchphrase cloud, the terms like virtualization, resources, elasticity, security, pay per use basis hit the mind. A key stumbling block of motivating the IT sector towards cloud ethnicity is the lack of conviction on security. The cloud provider, in turn, also needs to insist on authoritarian of the security policies, making trust on the clients. To improve the mutual trust between costumer and cloud provider, a well-understood trust foundation needs to be in place. Keeping in mind this paper presents a new approach to provide five level securities to the data stored and accessed by the cloud user. In cloud, the data of the individual or an organization is stored tenuously and the client does not have any control over it, hence the security becomes a major dilemma. Keeping in mind of the security required, this paper introduces a strong authentication, confidentiality and integrity mechanisms for storing the data of client at the data center. The modernization of this method is to place identity and information separately on different level thus providing five - level security which have no direct communication between them, all working at different places.

## General Terms

Security Challenges, Vulnerabilities, Proposed Idea

## Keywords

Hashed Password; Double Authentication; Data Storage Security; IP Notification; E-mail Encryption;

## 1. INTRODUCTION

Cloud computing is an exemplar swing of computing paradigm to cloud paradigm passing through distributed computing world.

The paper introduces the 5 – levels of security as:

- Use of IP tunneling technique by securing the IP address over the network and notify user in case of any change in IP address
- Securing and authenticating the identity of the user by means of authentication technique performed at the cloud user and provider using the codes
- Generation of hashed password at the data centre hence, securing password from the hackers at the cloud provider and data centre as it will never be known to anyone except the user
- Sending encrypted email to the cloud user containing password
- Lastly after getting authenticated, transferring data using cryptographic MD5 digest technique.

A cloud is a pool of resources which includes hardware and software which are accessed virtually by their clients. The cloud user should be concerned only about the resource available as a service. The service and data reside in the data centers and can be accessed by means of internet service on pay-per-use basis. Thus, the market research company IDC for example defines cloud computing [1] very general as "*an emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet*" (Gens 2008).

Grid computing and distributed systems forms the base of cloud environment, thus security has become an imperative concerned. To improve the performance, the data is placed at various data centers throughout the globe and is accessed through virtualized servers. As the data of the organization as well as of an individual is perceptible to one and all as a concluder cloud computing requires a lot of trust among the members working under this area.

Security necessitates in ensuring the authorized access of the resources. Secure computing not only embrace security and confidentiality, but also availability, integrity, reliability and safety.

## 2. SECURITY CHALLLENGES

### 2.1 Authentication

The authentication is the mechanism whereby system may securely identify its users. Authentication systems provide answers to the questions

Who is the user?

Is the user really who/he/she claims himself to be?

Authentication is a process which requires the users to identify himself using some unique information like password, mobile number etc. if presented correctly then the user is considered *authenticated.* By contrast, authorization provides different level of access like r, w, e, to the user in order to have a secure access to the resources. Both of these are somewhat tightly coupled mechanism – authorization specifies who the user is. An authentication specifies the security level of the user, specifying read, write and execute operation. Some common authentication methods are:

2.1.1 *The Traditional Authentication Method – in this model user name and password information for each user is stored locally on the server system. If the provided values are found to be matched, the user will become an authenticated user.*

The Weaknesses Are: in many cases user's password is stored in plain text form on the server machine. Anyone who can gain access to the server's database has access to enough information to impersonate any authentic user.

In case where the passwords are stored in an encrypted form on the server machine, plaintext passwords are still sent across a possibly insecure network from client to the server. Anyone with access to the intervening network may be able to snoops pair out of conversation and replay them to forge authentication to the system. There is no attempt made within the model to cross authenticate the server and the client.

### 2.1.2 *Double Authentication – In an order to protect the password from the illegal user the concept of double authentication is used which is a two step process. The first step engrosses the conventional process and the second step entails the generation of dynamic token in the database.*

Issues with Double Authentication - Though double authentication provides advanced security in identifying a user, the major drawback would be the time that it takes to generate a dynamic token and again matching it with its database. It is a tedious process and needs additional application software to support it. Moreover every time it follows the same process for every user and for every login[3].

### 2.1.3 *Kerberos Third Party Authentication Model – It's a significantly better authentication model which was developed and shepherded through the IETF standards processed by the staff at MIT a number of years ago. Kerberos addresses each of the major problems identified with the traditional authentication model, albeit at the expense of being significantly more complex than the traditional model.*

Weaknesses: The Kerberos model has certain weaknesses since the trust-ability of Kerberos system relies on the solidity of the encryption technology used which requires a security check on Kerberos IV. It is designed for use with the single user client systems. The restrictive factor of Kerberos authentication is the security of the multi-user.

This paper provides a new approach to the authentication process at various levels of cloud environment by replacing the concept of plain password storage with the hash password storage.

## 2.2 **Vulnerabilities**

According to the open groups risk taxonomy "vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an objects ability to resist that force. It is important to understand the levels at which there can be security vulnerabilities. The following areas can be identified as an unsecured and requires special concern.

*VM Security – Related to the virtual infrastructure vulnerabilities.*

*Data Security – Related to the data storage vulnerabilities.*

*Software Security – Application vulnerabilities* [4].

## 2.3 **Types of Vulnerabilities**

Vulnerability is a prominent factor of risk. ISO 27005 defines risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization," measuring [2] it in terms of both the likelihood of an event and its consequence.

Vulnerabilities exists in the cloud at different areas like storage, VM infrastructure, network etc, which needs to be recognized and at the same time the user should be made aware of these vulnerabilities.

Examples are:

### 2.3.1 *Hypervisor Holes*

These types of holes exist in the data centre as well as in the deployment software. These include the interruption of services, insertion of unwanted or objectionable code in the virtual machine.

### 2.3.2 *VM – Placement Attack*

In this type of attack, a VM is placed in the neighborhood of the target VM in order to increase the cross VM side channel attacks with an intent of extracting information.

### 2.3.3 *XML Signature*

XML protocols like – SOAP (Simple Object Access Protocol) is used in cloud. It contains the message details, if the content is modified by a malicious user with the guarantee that it contains the signature of the legal user. False messages can be sent.

### 2.3.4 *Malware Injection Attack*

In this type of attack a malicious user creates its own service modules and tries to use the cloud system to treat the services as the valid instance for the service. If it is successful the cloud system redirect the users request to this service and the malicious code is executed.

## 3. PROPOSED IDEA

In cloud computing security, IP address range and time becomes a great hurdle. In this paper we have proposed a triple security authentication scheme, with hashed password storage. The IP address is sent with encrypted identity code to the CSP, the code is decoded, and checked at the CSP, stored and passed on to the data centre ,where code is checked ,password is generated and hashed form is stored in the system, using hash function.

The data confidentiality and integrity is provided through MD5 cryptosystem hash technique. In case of change in IP address encountered a notification is sent to the user for the confirmation in change, if assured then the message is preceded to the data center.

## 3.1 Proposed Security Model

We proposed a five level security model for cloud computing that provides us Authentication, Integrity and Confidentiality in Figure 2.

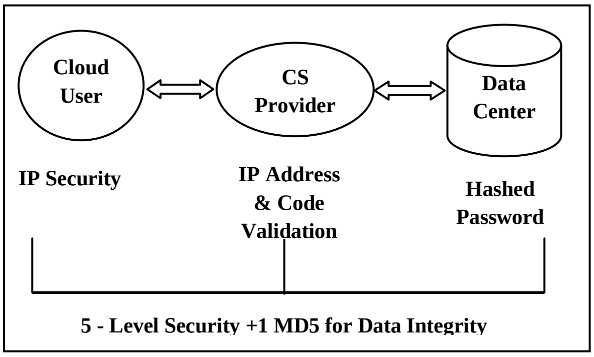
Cloud User
CS Provider
Data Center
IP Security
IP Address & Code Validation
Hashed Password
5 - Level Security +1 MD5 for Data Integrity

**Fig 1: Basic architecture for cloud**

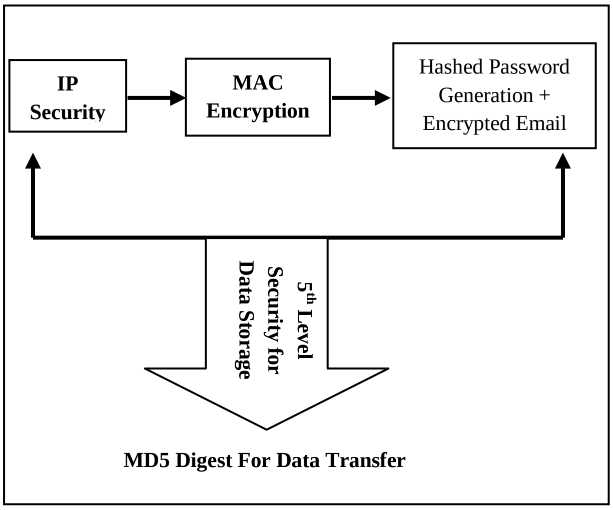
IP Security
MAC Encryption
Hashed Password Generation + Encrypted Email
5th Level Security for Data Storage
MD5 Digest For Data Transfer

**Fig 2: Five Level Securities in Cloud**

## 3.2 Overall Architecture Model

### 3.2.1 *Connection Establishment*

It occurs between the cloud users and cloud provider for first time when the user accesses the cloud. Then the cloud user and the data centre interaction occur for further process.

### 3.2.2 *User login process*

After the connection establishment, when the user is logged in, the password is checked at the data centre, there is no involvement of CSP. The password is first converted into a hash form and is matched with the stored hash password; if it is matched then the permission is granted. The main benefit of this scheme is except the cloud user no one can extract the password as it is stored in a hashed form in the data center.

### 3.2.3 *Data Storage, Retrieval & Other Operations*

After the login process gets completed. The user can send the data using MD5 digest cryptographic function making the data secured.

## 3.3 The Main Components Are

### 3.3.1 *Main Functionalities of Cloud Users*

*3.3.1.1 Creation of secured IP address*

*3.3.1.2 Encryption of code using MAC function*

*3.3.1.3 Sending MD5 encrypted code*

### 3.3.2 *Main Functionalities of Service Provider*

*3.3.2.1 Check the validity of IP address.*

*3.3.2.2 Verify the user in case of change of IP address.*

*3.3.2.3 Decode the code and forward to the data centre.*

*3.3.2.4 Store the E-mail, IP address and code of the user or organization.*

### 3.3.3 *Main Functionalities of Data Center Administrators*

*3.3.3.1 The password generation the first time the user approaches.*

*3.3.3.2 Storing the hashed password*

*3.3.3.3 Sending the generated password with a query question using Utimaco safeguard e-mail application*

*3.3.3.4 Validating the password every time the user logins*

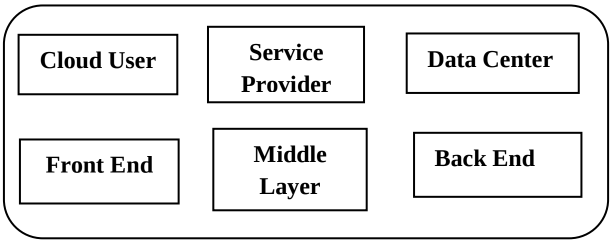

**Fig 3: Components of cloud**

# 4. IMPLEMENTATION

*Steps to be followed*

## 4.1 Step 1

The cloud user provides a secured IP address to the CSP and requests for the connection establishment. The process is shown diagrammatically in Fig 4.

## 4.2 Step 2

The user encrypts the code using MAC encryption method. The CSP decrypts the code and validates the code. The diagrammatic representation is as follows in Fig 5.

### 4.2.1 *Working of MAC*

M= Code of the Company

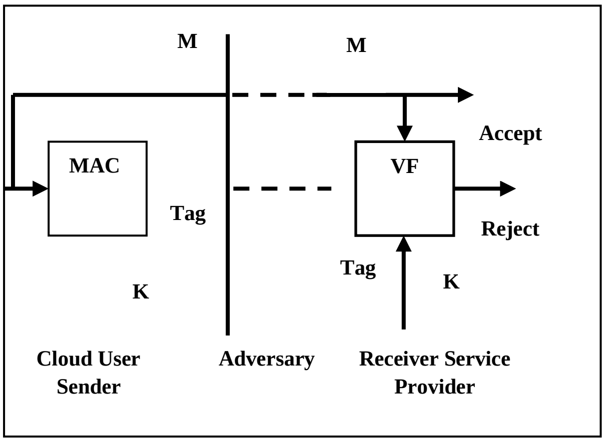

**Fig 5: Working of MAC**

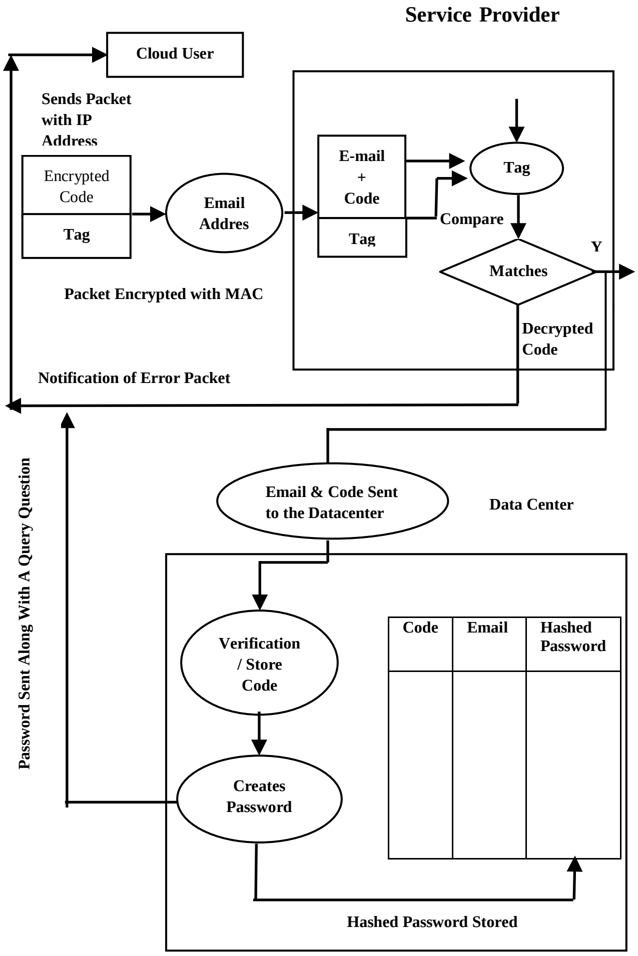
Service Provider
Cloud User
Sends Packet with IP Address
Encrypted Code
Tag
Email Addres
E-mail + Code
Tag
Tag
Compare
Matches
Y
Decrypted Code
Packet Encrypted with MAC
Notification of Error Packet
Password Sent Along With A Query Question
Email & Code Sent to the Datacenter
Data Center
Verification / Store Code
Creates Password
Code
Email
Hashed Password
Hashed Password Stored

**Fig 4: Connection establishment**

## 4.3 Step 3

Once the code is verified the CSP sends the details along with the code to the data centre. The data centre on receiving/validating the code generates the password and stores it in the message digest form. It uses Utimaco application to send the encrypted email to the cloud user. The e-mail carries the password along with the query question.

In the process of sending the password to the cloud user, the data centre uses a secured e-mail encryption technique.

### *Sending the Secure E-Mail*

Authenticity is one of the major issues in the e-mails usage. Serious losses may occur in the user-misleading e-mails. Classic e-mail services do not provide a secure solution for the verification of the e-mail origin. Moreover, they only provide cryptic information which can only be understood by experienced system administrators. Digital signature provides a secure and user-friendly solution to verify the origin (sender's signature) or the route of transport (route confirmation).

### *E-Mail Encryption*

Confidentiality is an essential facet of modern e-mail communication. The comfort of modern e-mail services makes it invisible for the user whether e-mail continues to stay within the secured area of his company or is led through insecure public networks. The encryption of e-mails is an important mechanism enabling companies to take advantage of the e-mail facilities without taking security risks. The diagrammatic representation is shown figure 6.

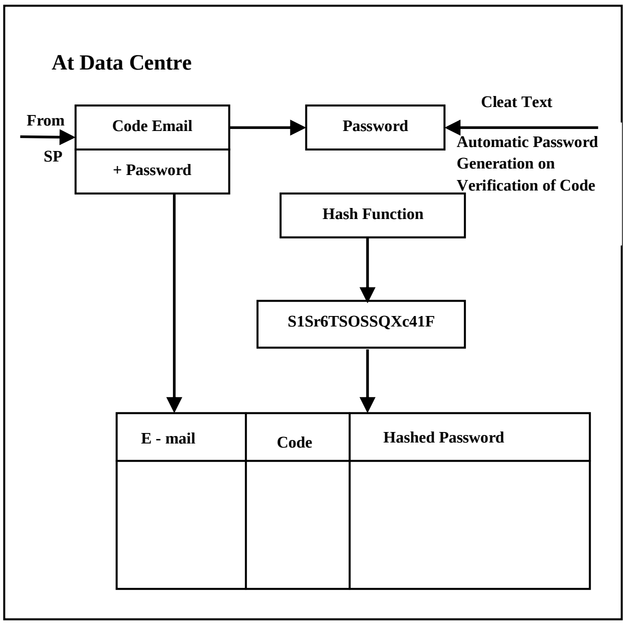

**Fig 6: Hash password generation**

## 4.4 Step 4

Once the connection process is over, the user can login using the password provided by the data centre. The diagrammatic representation is as follows in Fig 7.

After the user gets authenticated at the service provider, the entered password is converted into hashed form and is matched with the stored hash password at the data center which is described in the Fig 8.

### 4.5 Step 5

Once the user is authenticated, the user sends the data using MD5 cryptographic technique.

**Data Centre Access**

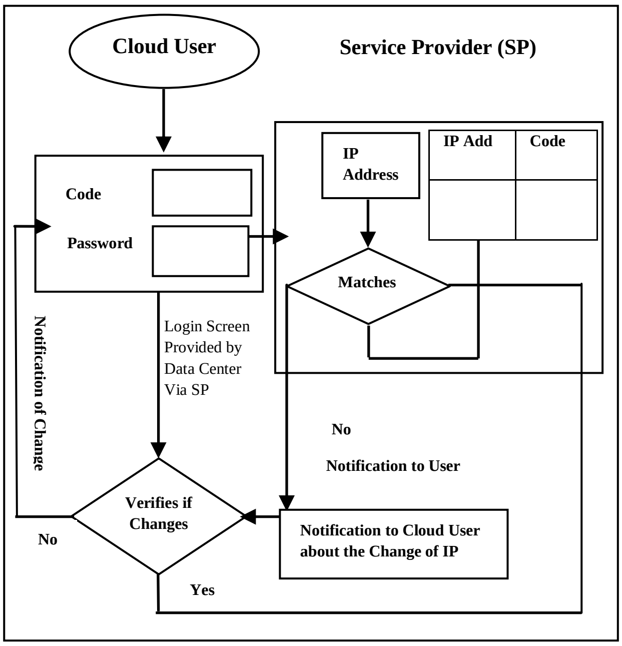

**Fig 7: Hashed password is not visible to anyone in the sp, data centre thus it provides double security**

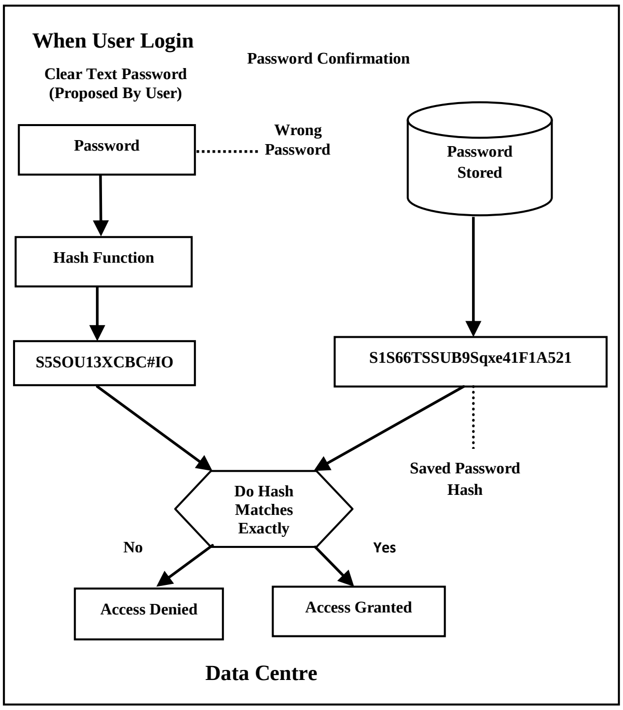

**Fig 8: Comparison of user's password with stored password**

Once the connection process is over, the user can login using the user code and password. When the user enters the code and password, the SP checks the IP address for validity and stores it if the user logins for the first time. If he is a regular user, the SP check the IP address with the stored IP address, in case of a mismatch a notification is sent to the user to confirm the correctness of the IP Address, the code and the password are checked at the data centre.

At the data centre, the user's password is converted to the random hash message digest by the hash function, and is matched with the stored message digest of the password, if matches, access is granted otherwise denied.

## 5. RELATED WORK

Security is a major reliable factor for any organization in order to move to the cloud architecture. Many technologies and methods have been implemented in order to achieve good level of security in cloud. The basic criteria to provide security is the creation of certificates to individual users but this proves to be very complex as the data is stored at the unknown location thus this is not a feasible implementation technique for cloud. Many cryptographic techniques are also used to implement security but due to their complexity of implementation the performance reduces apparently. Very few mechanisms exists which involves the classifications and registration of users along with their monitoring and tracing.

Guiten ZHAO et. al[6] Has proposed authentication system based on identity and combined key is implemented and tested. It's made up of client subsystem, Web server subsystem and authentication subsystem.

Eun-Jun Yoon et. al[7]Proposed a system robust ID-based remote user authentication scheme on ECC. The proposed scheme is divided into three phases: system initialization phase, user registration phase, and mutual authentication with key agreement phase. This scheme has some limitations. ECC-based authentication schemes still have some disadvantages; (1) It needs a key authentication center (KAC) to maintain the certificates for users' public keys like PKC. (2) When the number of users is increased, KAC needs a large storage space to store users' public keys and certificates. (3) The computation loads and the energy costs of mobile devices are very high because users need additional computations to verify other's certificate.

Jan Wiebeliz et. al[8] proposed a new concept for dynamic firewall operation including the use of TCP three-way handshake for the users authentication information needed by dynamic firewall operation. The firewall utilizes this information in-order to authorize the connections established during the sessions based on user's proven identity. The limitation is the creation and protections of certificates, which is not suitable for cloud computing environment. The use of complex cryptographic methods reduces the performance level and one of the greatest hurdle is the monitoring and tracing of cloud users.

Dimitrios Zissis et.al[9] demonstrates the use of certificates at various levels to enable secure data transfer and access. Certificates include user, application, and hardware types. The major drawback is the maintenance of these certificates at various levels and creating a trust relationship between them.

Luis Rodero Merino et. al[10] proposes a multitenant platform that ensures that no malicious or faulty code from any tenant can interfere with the normal execution of the other users code or the platform itself. It uses the J2EE. The problematic issues are isolation, potential problems like visibility of object references from mutable parts of classes and blocking through shared data structures.

Hongwei Li et. al[11] shows the authentication mechanism for the cloud user. This is based on identity-based hierarchical model for cloud computing (IBHMCC). For accessing the cloud service it uses the subsequent encryption and signature schemes for authentication. The limitation of this technique is consumption of more bandwidth.

S.Timm et. al[12] has proposed an idea for authentication in which the billing information is used to identify the customer by the commercial clouds and private clouds makes use of X509 certificates or PKI/ssh infrastructure for authentication. Limitation, Selected OS & kernel are allowed to run.

Hyosik Ah et. al[13] Applied technique for Access control and user authentication are security technologies used for platforms. Access control is the technology that controls a process in the operating system not to approach the area of another process. This paper proposed solution as no complex procedure at client side, validation performed at SP & data centre.

According to Farzad Sabahi et. al[14] Internet is a communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet.Limitations are Similar to physical computer in the Internet that have an IP address, a virtual machine in the Internet has an IP address as well. A malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack.

S. Subashini et. al[15] throws light on different security measures applied at different layers. Limitation: Cloud has heterogeneous system so the security cost is no doubt high.

## 6. CONCLUSION

In this research paper the authenticity is provided through encryption/decryption of MAC code and generation/comparison of hashed password. Use of hashed password limits the requirement of securing password at all the components and over the network.

The authenticity of data center is provided through the encrypted e-mail carrying the password. This is a very strong feature providing secure password as once generated and converted cannot be accessed by anyone except user. The confidentiality and integrity is provided through hashed password and MD5 digest. A very strong feature is the division of login process and data at different levels.

Keeping in mind of the security required, this paper has proposed a strong authentication, confidentiality and integrity mechanisms for storing the data of client at the data center. The modernization of this method is to place identity and information separately on different level thus providing five - level security which have no direct communication between them, all working at different places.

## 7. ACKNOWLEDGMENTS

The grandeur of achieving this research paper goes to our guide for our parents for their moral support. We are also thankful to our guide for enlivening us to write this research journal.

## 8. REFERENCES

[1] "Cloud Computing and Computing Evolution", Markus Böhm, Stefanie Leimeister, Christoph Riedl, Helmut Krcmar Technische Universität München (TUM), Germany

[2] Understanding Cloud Computing Vulnerabilities

[3] **"**A Threat Free Architecture For Privacy Assurance In Cloud Computing IEEE Paper 2011"

[4] "Security in Cloud Computing – Vulnerabilities, Challenges, Models and Path Ahead", Anand Mukundan

[5] Security in Public and Private Cloud Infrastructures, Joyent White paper

[6] Guifen ZHAO, Implementation and Testing of an Identity-based Authentication System, of Information Technology Beijing Municipal Institute of Science & Technology Information Beijing, China

[7] Eun-Jun Yoon,"Robust ID-based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC", School of Electrical Engineering and Computer Science Kyungpook National University Daegu 702-701, Republic of Korea ejyoon@knu.ac.kr

[8] Jan Wiebelitz, "Transparent Identity-based Firewall Transition for eScience", Germany. er.de

[9] "Addressing Cloud Computing Security Issues", Dimitrios Zissis, Dimitrios Lekkas

[10] Luis Rodero-Merino, "Building Safe Paas Clouds: A Survey on Security in Multitenant Software Platforms"

[11] Hongwei Li, "Identity-Based Authentication for Cloud Computing"

[12] S. Timm, "Authentication, Authorization, and Contextualization in Fermi Cloud"

[13] Hyosik Ahn, "User Authentication Platform using Provisioning in Cloud Computing Environment"

[14] Farzad Sabahi, ""Cloud Computing Security Threats and Responses"

[15] S. Subashini, "A survey on security issues in service delivery models of cloud computing"

[16] Sambhaji Sarod, "The Effective and Efficient Security Services for Cloud Computing"

[17] Danish Jamil, "Security Issues In Cloud Computing And Countermeasures"