

A  
Dissertation  
On

**Multi Factor Model for Authentication in Security of Clouds**

Submitted in Partial Fulfilment of the Requirement

For the Award of the Degree of

**Master of Technology**

**In**

**Computer Science & Engineering**

Submitted By

**Ankit Kumar Jain**

**2K12/CSE/04**

Under the Esteemed Guidance of

**Mr. Manoj Kumar**

**(Associate Professor)**



**DEPARTMENT OF COMPUTER ENGINEERING**

**DELHI TECHNOLOGICAL UNIVERSITY**

**JUNE, 2014**

## **ABSTRACT**

In this dissertation, we present a layered framework for cloud security. Cloud computing is a new way to deliver services over the internet. Cloud computing architecture gives a proper management to share and distribute all available resources and services over the whole world via computer network. Authentication is a key factor for security, which is a mechanism to establish connection that authenticates the person's identity. Traditional authentication approaches are not good enough to provide strong information security in modern cyber-attacks. A number of well-known protocols for authentication are considered the next-generation mobile and computer network services. The potential weaknesses of current existing protocols can be solved by categorization of services and authentication levels in terms of their significance and confidentiality. This can offer mutual and also two-factor authentication that is considered more secure against various phishing attempts than existing authentication protocol.

We propose a new level wise authentication imposing several factors for cloud computing. This proposed framework provides efficient and feasible mechanism which can be easily integrated into existing password authentication techniques. This proposed framework is verified by cloud server which authenticates user data. We are using several factors like arithmetic expression, one time password and magic number.

## **ACKNOWLEDGEMENT**

I would like to express my deepest gratitude to all the people who have supported and encouraged me during the course of this project without which, this work could not have been accomplished.

First of all, I am very grateful to my project supervisor Mr. Manoj Kumar for providing the opportunity of carrying out this project under his guidance. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success. I am also grateful to Dr. Rajeev Kapoor, HOD, Computer Science, DTU for his immense support. I am also thankful to my parents for being there for me at all times. Last but not the least; I am grateful to Delhi Technological University for providing the right resources and environment for this work to be carried out.

**Ankit Kumar Jain**

**University Roll no: 2K12/CSE/04**

**M.Tech (Computer Science & Engineering)**

**Department of Computer Engineering**

**Delhi Technological University**



**Department of Computer Engineering**

**Delhi Technological University**

**Delhi-110042**

## **CERTIFICATE**

This is to certify that the dissertation titled “**Multi Factor Model for Authentication in Security of Clouds**” is a bona fide record of work done at **Delhi Technological University** by **Ankit Kumar Jain, Roll No. 2K12/CSE/04** in partial fulfilment of the requirements for the degree of Master of Technology in Computer Science & Engineering. This work was carried out under my supervision and has not been submitted elsewhere, either in part or full, for the award of any other degree or diploma to the best of my knowledge and belief.

Date: \_\_\_\_\_

**(Mr. Manoj Kumar)**  
**Associate Professor & Project Guide**  
**Department Of Computer Engineering**  
**Delhi Technological University**

## Table of Contents

|   |            |
|---|------------|
| <b>Certificate</b>  | <b>ii</b>  |
| <b>Acknowledgment</b>                                       | <b>iii</b> |
| <b>Abstract</b>   | <b>iv</b>  |
| <b>List of Figures</b>                                      | <b>vii</b> |
| <b>1. Introduction</b>                                      | <b>1</b>   |
| 1.1 Cloud computing   | 1          |
| 1.2 Security issue in cloud computing                       | 2          |
| 1.3 Problem statement                                       | 5          |
| 1.4 Objective   | 6          |
| 1.5 Motivation  | 7          |
| 1.6 Organization of thesis                                  | 8          |
| <b>2. Literature survey on cloud computing</b>              | <b>9</b>   |
| 2.1 Basics of cloud computing                               | 9          |
| 2.2 What is cloud computing                                 | 10         |
| 2.3 Attributes of cloud computing                           | 11         |
| 2.4 Cloud computing architecture                            | 12         |
| 2.4.1 Cloud computing service models                        | 12         |
| 2.4.2 Cloud computing deployments                           | 13         |
| 2.4.3 Cloud computing benefits                              | 15         |
| 2.5 Difference between cloud computing and Traditional IT   | 15         |
| 2.6 Strategic planning for cloud computing services by user | 16         |
| <b>3. Security architecture of cloud computing</b>          | <b>18</b>  |
| 3.1 Security management by provider                         | 18         |
| 3.2 Security issues in cloud                                | 20         |
| 3.2.1 Data centre security                                  | 21         |
| 3.2.2 Server security                                       | 21         |
| 3.2.3 Network security                                      | 22         |
| 3.2.4 Application and platform security                     | 24         |
| 3.2.5 Data security   | 24         |
| 3.2.6 Authentication  | 25         |

|   |           |
|---|-----------|
| 3.3Existing authentication protocol               | 26        |
| <b>4. Proposed algorithm and framework</b>        | <b>27</b> |
| 4.1 Entities which are used in proposed framework | 28        |
| 4.2 Key approaches used                           | 29        |
| 4.3 Registration phase                            | 31        |
| 4.4 Login phase                                   | 32        |
| 4.5 Authentication phase                          | 32        |
| 4.5.1 Level 1 authentication                      | 33        |
| 4.5.2 Level 2 authentication                      | 34        |
| 4.5.3 Level 3 authentication                      | 35        |
| <b>5. Implementation and results</b>              | <b>36</b> |
| 5.1 Registration module                           | 36        |
| 5.2 Login module                                  | 37        |
| 5.3 All authentications modules                   | 38        |
| <b>6. Security analysis of proposed framework</b> | <b>41</b> |
| <b>7. Conclusion</b>                              | <b>43</b> |
| <b>References</b>                                 | <b>44</b> |

## List of Figures

|           |   |    |
|-----------|---|----|
| Fig. 1 :  | Important points of view cloud security             | 4  |
| Fig. 2 :  | Cloud computing evolution                           | 10 |
| Fig. 3 :  | Cloud service model                                 | 12 |
| Fig. 4 :  | Reference architecture for cloud computing platform | 17 |
| Fig. 5 :  | flow chart of registration phase                    | 29 |
| Fig. 6 :  | flow chart of login phase                           | 30 |
| Fig. 7 :  | Flow chart of level 1 authentication                | 31 |
| Fig. 8 :  | Flow chart of level 2 authentication                | 32 |
| Fig. 9 :  | Flow chart of level 3 authentication                | 34 |
| Fig. 10 : | Registration module                                 | 35 |
| Fig. 11 : | Login module  | 36 |
| Fig. 12 : | Authentication 1 page                               | 37 |
| Fig. 13 : | Authentication 2 page                               | 38 |
| Fig. 14 : | Authentication 3 page                               | 39 |

# CHAPTER 1

## INTRODUCTION

---

### 1.1 Cloud Computing

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals to use software and hardware that are managed by third parties at different locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, computer processing power, and specialized corporate and user applications. Cloud can be viewed as a virtual pool of resources that can be accessed by the internet. Cloud service provider (CSP) offer services to the user and they use some kind of interface to communicate with cloud server [1]. Generally, cloud can provide distinct services and depending on the type of services (resources) three type of layer can be defined. First layer provide basic infrastructure components such as CPU, memory, storage and called infrastructure as a service for e.g. Amazon's elastic compute cloud. Second layer provide some platform oriented services known as (PaaS) platform as a service. Google engine is an example for a web platform. Third layer provides some ready to use software resources and also known as software as a service (SaaS) [2,3].

Cloud computing provides users the illusion of millions computing resources available from anywhere, anytime, on demand. This type of Computing requires a framework that can support large datasets housed on clusters of commodity hardware. Now a days most of the services and application are on internet web sites like Google, yahoo, you tube, Gmail has many clicks everyday where real time storage, capturing and analysis of data are common needs of online application. However, security and privacy issues consist of security reasons for users to adapt into Cloud environments. We investigate several Cloud Computing providers about security and privacy issues. We find those concerns are not so efficient and some security aspects should be added in terms of authentication, availability, confidentiality, Data integrity for security. Moreover, released acts on security are out of date or no enough to protect user's private information in the new environment since they are no longer strong enough for users prospective.



The following definition of cloud computing has been developed by the “U.S.NationalInstitute of Standards and Technology” (NIST): “Cloud computing is a model for convenient, on-demand access of network to a shared pool of computing resources (e.g., networks, storage, services, soft wares, and application) that can be provisioned and released with minimal effort of authority or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [3]”.

Most organizations currently are looking in the way of cloud computing to enable a mechanism where user can anytime anywhere access. The cloud computing paradigm has been defined varying from perspectives can simply be described. As a computing era where it can be used as: Platform as a Service (PaaS)– In this consumers are allowed to utilize services from providers, Infrastructure as a Service (IaaS) – In this customers are allowed to access data by paying to providers utilize computing space, and Software as a Service (SaaS) – In this consumers and providers both are allowed to access cloud based software and applications. The advantages of cloud computing are vast – ranging from organization business agility and scalability of system to data maintainability. The cost of service charged by the providers is economical enough which gives organization stakeholders a space to cut down their internal IT budget. The concept of cloud is vast which should have effective security services. The cloud computing technique is used everywhere now a day. But in data privacy authentication protection and data integrity is one of the most challenging task in cloud environment, an organization usually store data in server’s internal storage and then tries hiding the data from outside world. Additionally, cloud supports to deliver the soft wares over the Internet which can be access from many existing tools like web browsers, desktop and mobile based applications. Security is still major component facing by cloud computing developer. In which the authentication between user and server is the central phase of security in the cloud computing. So, it should necessary to allow only authorized user so only they can access stored data [4].

## 1.2 Security Issues In Cloud Computing

**A) Security data and storage:** In Cloud computing protection of data is the most important privacy issues. In this the main concerns is the way by which data is accessed and stored. In the cloud storage environment, important and sensitive data needs to be

confidential. In the service provider's database, protecting privacy of data and managing methods are very crucial and critical by using encryption keys of data in transfer. At the cloud provider, securing of data is depends on cryptographic encryption and shipping self-encrypting is used by hard drive manufacturers. Self-encrypting offer automated encryption with minimal cost impact and better performance [5, 6]. Software encryption is not so secure and also it is slower because here encryption key can be copied off the machine without any detection.

**B) Network and server:** Server-Side Protection: Virtual servers and or cloud servers and their applications, have to be compelled and should be secured in IaaS clouds, each logically and physically. Virtual firewalls are often used to isolate virtual machines from different hosted machines, like development systems to production systems or different cloud-resident systems to development systems. Managing virtual system is additionally vital to avoid vulnerabilities [7]. Preventing leaks between the existing infrastructures could be a major problem with hybrid clouds. The supply of this type of cloud, computed because supply levels for the part clouds, also can be a concern.

**C) End user security issues:** Users need to access resources and services within the cloud and they may bear in some kind of access agreements or conflict of interest. The client have some techniques to find some vulnerable code or any protocols at entry points or in every critical region like servers, mobile devices, firewalls and upload patches on their systems as soon as they discovered [5].

**D) Security as a service:** In Cloud environment the security provided by cloud service providers (CSPs). Security-as-a-service is a security offered as a cloud services and it can be delivered in two methods: In first method user can changing their delivery methods to include services which comprises established information and security vendors. The second method, in this Cloud Service Providers (CSP) is providing security only in terms of cloud service with information security organizations.

**E) Browser security:** In a Cloud computing environment, servers are used for computation purpose. The client nodes are used for input and O/P operations only and for authentication and authorization of information to the Cloud [8]. A standard Web browser is client software which should be Platform in-dependent useful for all users across the world. This can be described into different types: web application, Software as- a-Service, Web 2.0 TLS is used for authentication and encryption.

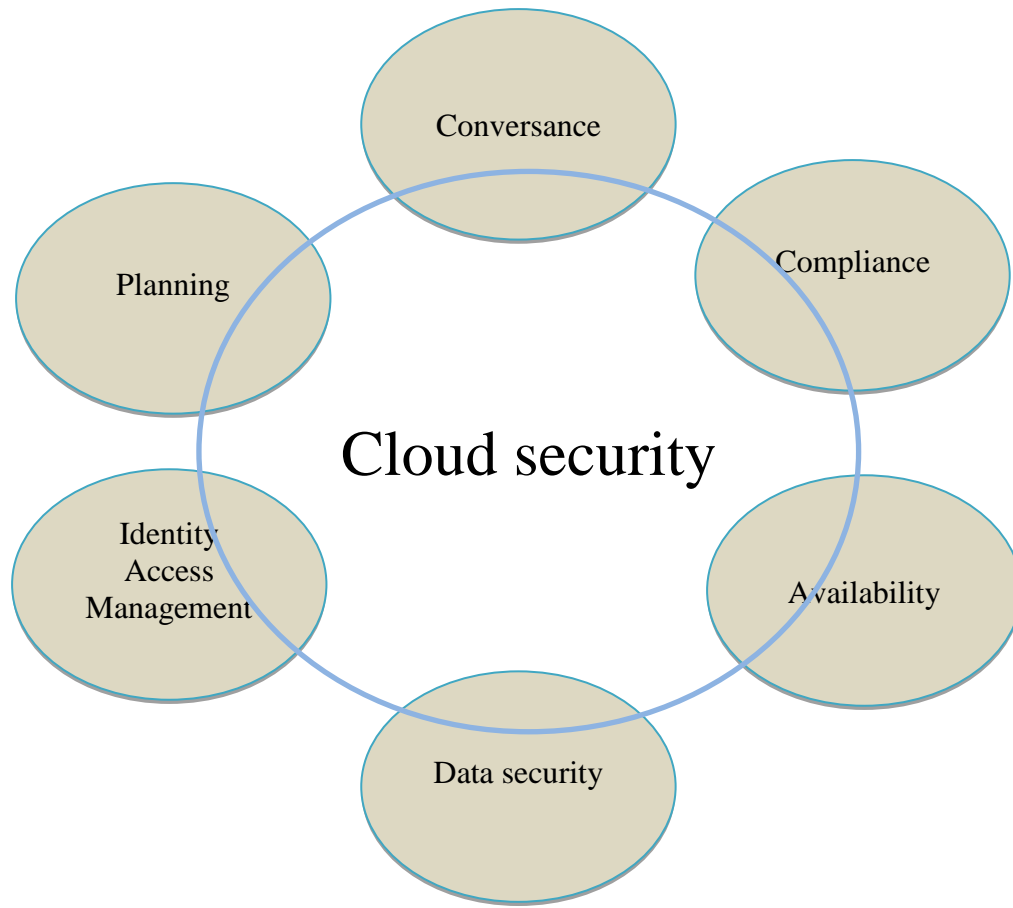


Figure 1: Important points of view cloud

**F) Authentication:** In the cloud computing environment, the primary concern for secure access control is user authentication and it is more important since the cloud and its data are accessible to over the Internet. Trusted Platform Module (TPM) is available and provide stronger authentication than simple username and passwords technique [8]. Trusted Computing Groups (TCG's) is standard about authorized users and other privacy and security issue in real-time scenario between the cloud provider and the user. In cloud, big data, applications and service and resources are collected and cloud computing has very weak authentication technique, then the attacker can easily achieve the user account and log into the virtual machine So authentication is required well enough to provide right user identity so that server can rely on user and make available all concerned services of cloud [9]. In cloud security authentication is central part so there should be a good mechanism for user authentication area.

## 1.3 Problem Statement

As cloud computing has many advantages for both user and cloud service provider. Developing of cloud environment is growing fast in current scenario. As much user demands of this technology, cloud providers are facing new challenges every day to fulfil customer wishes. Large number of users adapted cloud environment. Thus, cloud computing is famous in modern era in terms of storing and accessing of our data. Cloud computing provides various services and features such as a user can access and save his data to cloud virtual servers by using the Internet. Additionally, it also supports to deliver the services and applications over the Internet which can be accessed from tools like desktop, browsers, and mobile based applications. Security is still a major component facing the widespread of cloud computing. The authentication considers the central part of security in the cloud computing. So, it is must to allow that only authorized customer can access stored data [11]

In the last few years cloud computing has been grown from one of the fastest growing part of IT industry. But as more information, services are placed in the cloud, the main concern are how secure environment cloud can provide to its user [10]. Cloud Providers should ensure about security of In the last few years, cloud computing has been grown customer's information and their confidential data. Cloud service provider should be responsible if any security flaw affects their user's service confidentiality. A cloud service provider serve many services to its users such as fast accessing of data from anywhere, scalability, storage, content recovery, protection against adversary, security controls. CSP can offer benefits to users, but privacy and security factor play a vital role in this environment. There are so many authentication schemes that rely on username/password, but unfortunately they are not considered strong techniques of cloud authentication. A more secure and used scheme is the two-factor authentication which is also called 2FA [4], does not only verify the password and user name, but also it deals with a second factor such as a token device, some kind of password and biometric. However, the feasibility of 2FA (second-factor authentication) is also limited by the complexity deployment, high cost and the level of cloud security is compromised when the token is purloined. These schemes are failed to protect well-known attacks such as reflection attacks, replay attacks. We propose an authentication scheme based on several factor and level wise authentication which ensure the required credential of user. Security

analysis and experimental results illustrate that our proposed scheme can withstand the common security attacks as well, and has a good performance of password authentication.

## **1.4 Objectives**

Though IT services from the cloud are becoming increasingly in demand around the world, almost every survey and study shows that there are also many concerns which discourage users away from using Cloud Computing services. A lack of faith in the security of the services provided is frequently cited as being one of the main barriers. As the central information security service provider for the federal government in Germany, the BSI feels it is important that it is actively involved in shaping the development phase for cloud services [12]. Cloud Computing has the long-term potential to change the way information technology is provided and used. But information security is a key factor if IT services from the cloud are to be used reliably. It is not only the traditional attack scenarios that are relevant to cloud systems. There are also specific characteristics, such as the fact that multiple users share a common IT infrastructure. The dynamic sharing of the IT service across multiple locations also represents a particular challenge [12].

Since the data is used to be sent and stored in a cloud computing system through wireless or LAN it becomes dangerous to unauthorized leakage of data, modifications, and spoofing and replay attacks. So here is our objective to find a way to provide good enough authentication mechanism for users so that their data and information could be hide from adversary and also users should not have any unnecessary complex authentication for simple services [11].

## **1.5 Motivation**

Cloud Computing is currently one of the hottest topics in information technology (IT). However, it is not so much that the term ‘Cloud Computing’ represents a host of new technologies, but rather that these technologies are combined and effectively upgraded so that they enable new IT services and new business models. With Cloud Computing, as with many new technologies and services, information security and data protection issues are intensely debated and examined far more critically than is the case with offerings that have been around for a while. It is not only the traditional attack scenarios that are relevant to cloud systems. There are also specific characteristics, such as the fact that multiple users share a common IT infrastructure. The dynamic sharing of the IT service

across multiple locations also represents a particular challenge. Many surveys and studies reveal that potential customers have concern about information security and data protection which stand in the way of a wider deployment. The required trust still needs to be developed if cloud offerings are to be taken advantage of.

Secondly, in current scenario authentication is major concern in mobile as well system cloud. In general, traditional password schemes are used most widely, but they have so many flaw or weaknesses. These drawbacks denote user's problem in memorizing long or alphanumeric or complex passwords, and the security risks can be occurred by depending simple passwords [11]. Passwords have suffered from some attacks such as brute-force attacks and dictionary attacks. Since we know passwords are simply restricted to the symbols which are existed on keyboards. As a result, an intruder may attempt all possible permutation and combinations until finding a correct password; this is called brute-force attack. Additionally, most users tend to pick something such as birth data, contact number, favourite sports, and some relative's name to use as a password. Because these type of passwords are easy to remember. Consequently, attacker can make a table of important words and character transgress the system, which is called dictionary attack. Furthermore, some password based authentication suffers from the malicious attacks such as reply attack, Man in the middle attack. Besides it there are also some problems for cloud like why they face a complex or strong login for authentication each time when they need a common frequent service from cloud. That means it is not feasible for simple user to follow same complex authentication mechanism for different types of services some may be frequent or some very important and unusual. So there should be some categorization of services and should be dealt differently in terms of authentication.

## **1.6 Organisation of Thesis**

Chapter 1 Introduction

Chapter 2 Deals with literature review of cloud computing

Chapter 3 Deals with security issues in cloud computing

Chapter 4 Proposed frameworks and algorithm

Chapter 5 Implementation of proposed work

Chapter 6 Security analysis of proposed work

Chapter 7 finally concludes the work

## CHAPTER 2

# LITERATURE SURVEY ON CLOUD COMPUTING

---

**2.1 Basics Of Cloud Computing:** Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals to use software and hardware that are managed by third parties at different locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available [13]. Cloud computing provides a shared pool of resources, including data storage space, computer processing power, and specialized corporate and user applications. Cloud can be viewed as a virtual pool of resources that can be accessed by the internet. Cloud service provider (CSP) offer services to the user and they use some kind of interface to communicate with cloud server. Most organizations currently are looking in the way of cloud computing to enable a mechanism where user can anytime anywhere access. The cloud computing paradigm has been defined varying from perspectives can simply be described. As a computing era where it can be used as: Platform as a Service (PaaS)– In this consumers are allowed to utilize services from providers, Infrastructure as a Service (IaaS) – In this customers are allowed to access data by paying to providers utilize computing space, and Software as a Service (SaaS) – In this consumers and providers both are allowed to access cloud based software and applications [15]. The advantages of cloud computing are vast – ranging from organization business agility and scalability of system to data maintainability. The cost of service charged by the providers is economical enough which gives organization stakeholders a space to cut down their internal IT budget. The concept of cloud is vast which should have effective security services. The cloud computing technique is used everywhere now a day. But in data privacy authentication protection and data integrity is one of the most challenging task in cloud environment, an organization usually store data in server's internal storage and then tries hiding the data from outside world [16]. Additionally, cloud supports to deliver the soft wares over the Internet which can be access from many existing tools like web browsers, desktop and mobile based applications. Security is still major component facing by cloud computing developer. In which the authentication between user and server is the central phase of security in the

cloud computing. So, it should necessary to allow only authorized user so only they can access stored data.

## 2.2 What is cloud computing?

No definition of the term ‘Cloud Computing’ has yet succeeded in becoming universally acceptable. Definitions are often used in publications and presentations that are extremely similar to each other while nonetheless differing. One definition that is frequently drawn upon by experts is that of the USA’s National Institute of Standards and Technology (NIST), which is also used by ENISA [14]:

“Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources(e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1, 14].”

Under the NIST definition, the five characteristics of a cloud service are listed below:

- a) On-demand self-service: Resources (e.g. server time, storage) are provisioned unilaterally without interacting with the service provider.
- b) Broad network access: The services are available over the network, accessed through standard mechanisms and not tied to a particular client.
- c) Resource pooling: The provider’s resources are pooled to serve multiple consumers (multi-tenant model). The users do not know where the resources are located but they may be able to contractually specify the storage location, e.g. the region, country or data centre.
- d) Rapid elasticity: The services can be rapidly and elastically provisioned, in some cases even automatically. To the consumer, therefore, the resources appear to be unlimited.
- e) Measured services: Use of resources can be measured and monitored and similarly provided to the cloud users in a measured way [1].

This definition reflects the vision of Cloud Computing although the individual points should not be viewed in too dogmatic a manner. For example, in the case of private clouds, there may be no requirement at all for ubiquitous availability.

According to the Cloud Security Alliance (CSA), Cloud computing also has the following characteristics – in addition to the elasticity and self-service referred to above:

- 1) Service oriented architecture (SOA) is one of the basic requirements for Cloud Computing. The cloud services are usually provided via a so-called REST API.



- 2) In a cloud environment, multiple users share common resources which therefore need to be multi-tenant.
- 3) The only resources paid for are those actually been used (Pay per Use model), with flat rate models also being an option.

## 2.3 Attributes of Cloud Computing

- a) Multi-tenancy: Cloud computing is based on a model where resources are shared among multiple users (i.e., multiple users can use the same resource) at the host level, application level, and network level.
- b) Massive scalability: Cloud systems offer the ability to scale to large thousands of systems, as well as it has the ability to scale storage and bandwidth Space massively.
- c) Elasticity: It means Users can increase and decrease computing resources very rapidly as needed.
- d) Pay as you used: it means Users have to pay for the resources which are actually used by them and for only the time required by them.
- e) Self-provisioning of resources: In this Users can self-provision resources, like additional systems (software, processing capability, storage) and network resources.

Cloud computing is a natural development of the general adoption of simulation, service-based architecture, involuntary, and utility computing. Details are outlined from end-users, who no more have a need for special knowledge in, or control over, the technology substructure "in the cloud" that helps them as illustrate in figure.

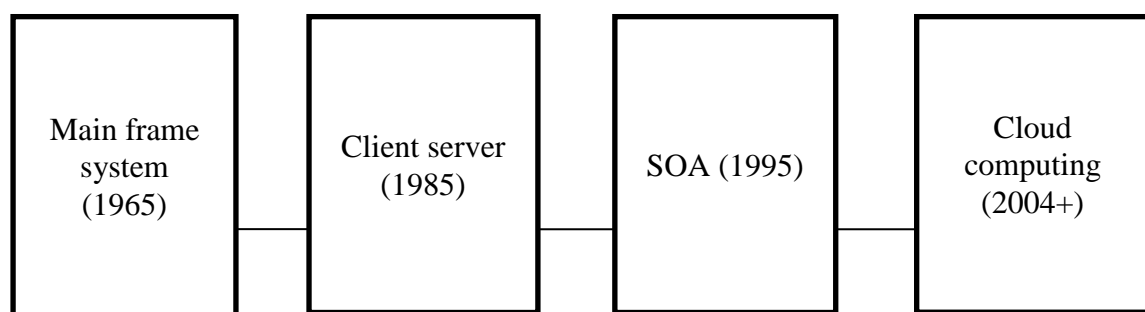


Figure 2: Cloud computing evolution

## 2.4 Cloud Computing Architecture

### 2.4.1 Cloud Computing Service Models

A) Cloud Software as a Service (SaaS): Software Application and Information clouds, In this user can Use provider's applications through network, examples of cloud provider Google Apps, Yahoo, Gmail etc. Any provision of applications that meet the Cloud Computing criteria falls into this category. No limits are set here on the range of offerings. Examples are applications for contact data management, financial accounting, text processing and collaboration. The term “as a Service” is also used for many other offerings, such as ‘Security as a Service’, ‘BP as a Service’ (Business Process) and ‘Storage as a Service’, so that one often speaks of “XaaS”, i.e. “something as a service”. Most of these offerings can at least roughly be assigned to one of the categories above [15].

B) Cloud Platform as a Service (PaaS): It is Development clouds, where customer can deploy created applications to a cloud, here cloud provider examples are Google App Engine, window azure. A PaaS provider provides a complete infrastructure and, on the platform, provides the customer with standardized interfaces to be used by the customer’s services. For example, the platform can provide multi-tenancy, scalability, access controls, database accesses, etc. as a service. The customer has no access to the underlying layers (operating system, hardware), but can run their own applications on the platform, for which the CSP will usually provide its own tools.

C) Cloud Infrastructure as a Service (IaaS): In Infrastructure clouds, storage, capacity of network, processing and other system fundamental computing resources examples are Drop box, Amazon Web Services, Google drive etc. With IaaS, IT resources such as processing power, data storage and networks are available as a service. A cloud customer buys these virtualized and, to a large degree, standardized services and adds their own services on top for internal or external use. For example, a cloud customer can rent server time, working memory and data storage and have an operating system run on top with applications of their own choice.

The service models also differ in terms of the customer’s influence over the security of the services provided. In the case of IaaS the customer has total control of the IT system, from the operating system upwards, since everything is operated within their area of responsibility. With PaaS the customer only has control over their applications running on

the platform, while with SaaS they hand over almost all control to CSP. From this point onwards, we distinguish cloud among service as a clouds and platform and infrastructure as a service cloud which, under the definition above, represent the full range of cloud service models.

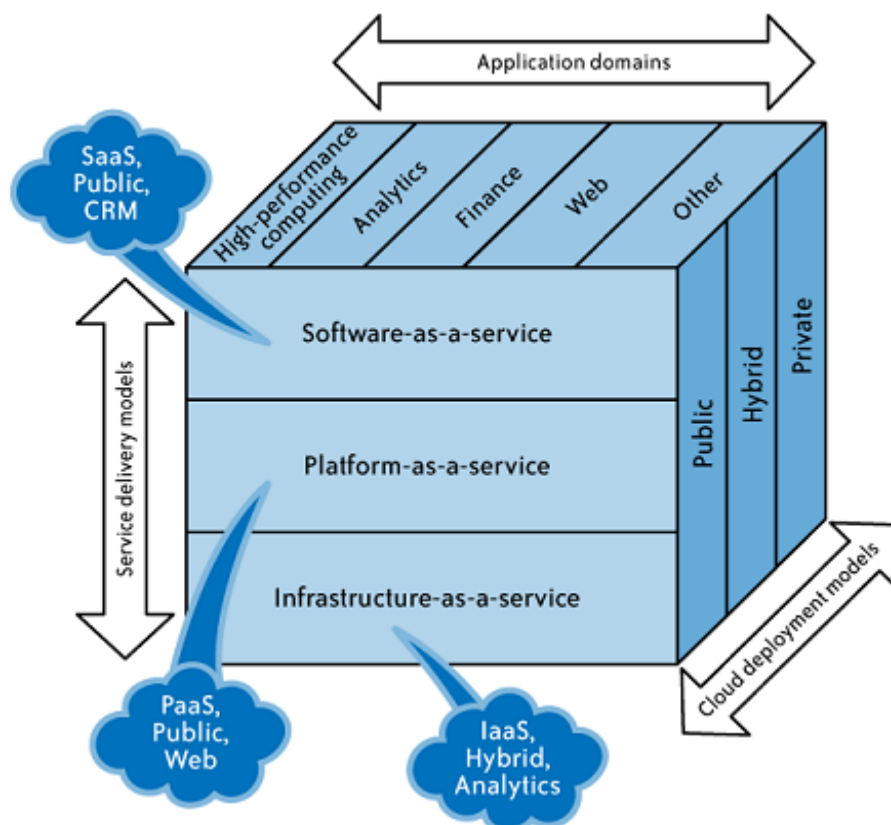


Figure 3: Cloud service model

## 2.4.2 Cloud Computing Deployment Models

The term cloud is a known for the Internet and is a representation of the complex interfacing devices and connections which form the Internet. Public and private and hybrid clouds are subparts of the Internet and they are defined based on their bonding to the enterprise. Public and private clouds also referred as external or internal clouds. This discrimination is based on what relationship has enterprise with cloud. The public and private cloud concepts are very important in some places because they support cloud computing which performs the provisioning of scalable, dynamic virtualized resources all

over Internet attachments by a seller or an IT organization to their customers for a fee. The users who use these services offered via cloud network may not have knowledge of, and expertise in, and control over the infrastructure that helps them.

The majority of cloud computing network consists of some reliable application and services which can be delivered through data centres and servers. The services are accessible from everywhere which has networking infrastructure available. The cloud system resembles as a single point of access for users across the world.

A) Public clouds: public clouds (or external clouds) describe cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications or web services, from an off-site, third-party provider who shares resources and bills on a fine-grained, utility-computing basis. A public cloud is hosted, operated, and managed by a third-party vendor from one or more data centres. The service is offered to multiple customers (the cloud is offered to multiple tenants) over a common infrastructure; In a public cloud, security management and day-to-day operations are relegated to the third-party vendor, who is responsible for the public cloud service offering. Hence, the customer of the public cloud service offering has a low degree of control and oversight of the physical and logical security aspects of a private cloud. Public cloud is used if the services can be used by the commonality or by a large group, for example an entire industrial sector, and if they are supplied by one provider.

B) Private cloud: Private cloud or internal clouds are terms used to describe offerings that emulate cloud computing on private networks. These (typically virtualization automation) products claim to deliver some benefits of cloud computing without the pitfalls, capitalizing on data security, corporate governance, and reliability concerns. Organizations must buy, build, and manage them and, as such, do not benefit from lower upfront capital costs and less hands-on management. The organizational customer for a private cloud is responsible for the operation of his private cloud. Private clouds differ from public clouds in that the network, computing, and storage infrastructure associated with private clouds is dedicated to a single organization and is not shared with any other organizations. In a private cloud the cloud infrastructure is only run for one institution. It may be organized and managed by the institution itself or by a third party and it may be located in the institution's own data Centre or in that of a different institution [15, 16].

C) Hybrid cloud: A hybrid cloud environment consisting of multiple internal and/or external providers is a possible deployment for organizations. With a hybrid cloud, organizations might run non-core applications in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud. If multiple cloud infrastructures, each of which is independent in itself, are commonly used via standardized interfaces, this is referred to as a hybrid cloud.

### **2.4.3 Cloud Computing Benefits**

- a) Lower computer costs
- b) Improved performance
- c) Reduced software costs
- d) Instant software updates
- e) Improved document format compatibility
- f) Unlimited storage capacity
- g) Device independence
- h) Increased data reliability.

## **2.5 Difference between cloud computing and traditional IT**

With outsourcing, an institution's work, production or business processes are wholly or partly handed over to external service providers. This is an established part of modern organizational strategies. Classic IT outsourcing is usually set up in such a way that the entire infrastructure hired is used exclusively by one customer (single tenant architecture), even though outsourcing providers normally have multiple customers. Outsourcing agreements are also usually signed for lengthy time-scales.

The use of cloud services is similar in many ways to classic outsourcing, but there are certain differences which need to be taken into account

- a) For financial reasons, multiple users in a cloud share a common infrastructure true.
- b) Cloud services are dynamic, so they can be scaled upwards and downwards far more quickly. Thus cloud-based offerings can be adjusted to the customer's actual needs more swiftly.
- c) The managing of services that are used from the cloud is usually done via a web interface by the cloud user themselves. Thus, the user can automatically tailor the services used to suit their needs.

- d) The technologies used in Cloud Computing enable the IT service to be dynamically shared across multiple locations which may be geographically much dispersed (both nationally and internationally).
- e) The customer can easily administer the services used and their resources via web or other suitable interfaces, and little interaction with the provider is required.

## **2.6 Strategic Planning For Cloud Computing Services by Users**

Before business-critical data or applications are outsourced to the cloud, a cloud strategy needs to be defined in which the main underlying principles are clarified. For this purpose, there should always be a specific security analysis for the data or applications that are to be outsourced. The cloud strategy should define, for example, what the IT structure looks like (e.g. in the case of IaaS), how existing IT systems or business processes can be delimited and separated, what all the underlying operational and legal parameters look like, and what the protection requirement is for the data or applications that are to be outsourced. In fact, CSPs have typically tailored their offerings to particular types of information and applications. In so doing, however, they are faced with the challenge of not knowing the specific protection requirement for their customer's data. They might offer a high or very high level of protection for all their customer data, but this would be too expensive for data with a normal protection requirement.

To be able to offer every cloud customer a service that is persuasive in both functional and financial terms for customers from different sectors, CSPs should bring up the subject of data security at an early stage with their cloud customers. CSPs should tell their customers which security measures are included as standard with their offerings, which can be procured as a supplement, and which security measures the customer is responsible for him. This also helps to avoid misunderstandings. For example, the CSP often has to bear enormous losses caused by incidents such as losing data even though it was the cloud customer that failed to ensure their data was sufficiently secure, because they opted for a level of protection that was too low or accepted a risk that was too high. For this reason it is also vital for the CSP that the cloud customer understands the protection requirement for the outsourced data or applications and that they are clear about the protection level being offered. In this way, the CSP can also bring the customer's attention to any potential security benefits which may arise from using cloud services. Therefore the user must first work out the basic issues relating to security during

the process of making the strategic decision, as to whether – and in which form – a cloud service is to be deployed. This applies to both public and private clouds, and equally to IaaS, PaaS and SaaS.

This process includes the following steps:

- a) Analysing the structure of the IT systems (e.g. with IaaS) and applications order to enable a delimitation and to identify all the interfaces.
- b) Specifying the protection requirement for data, applications and IT systems.
- c) Dividing up the data, applications, systems and cloud services into protection requirement categories.
- d) Clarifying the underlying operational and legal framework.
- e) Defining the specific security requirements for CSPs

# CHAPTER 3

## SECURITY ARCHITECTURE OF CLOUD COMPUTING

### 3.1 Security Management by the Provider

Figure illustrate architecture of reference which shows the components to many Cloud Computing platforms. This architecture is used as a basis for guidelines that follow. The reference architecture shown takes into account the ideas in similar reference architectures, such as those used by NIST, IBM and the Cloud Computing Use case group [1].

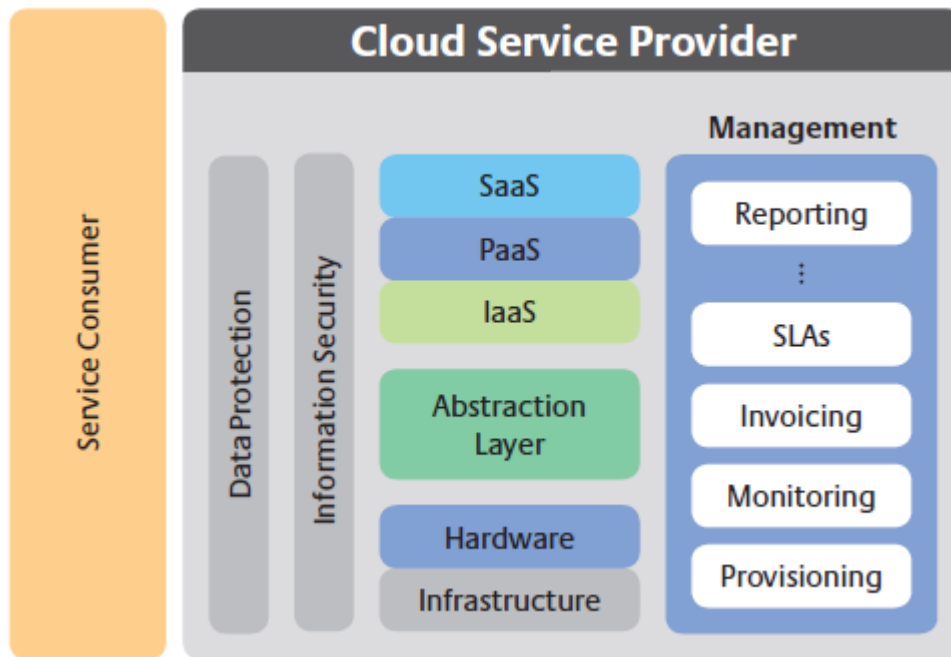


Figure 4: Reference architecture for cloud computing platform

A close look at the underlying reference architecture reveals that a provider needs to address a large number of tasks in order to provide cloud services. The tasks typical to a public CSP include:

- Providing a catalogue of services which describes the services being offered.
- Provisioning and de-provisioning resources such as virtual machines, load balancers, virtual data storages, IP and MAC addresses.



c) Invoicing for the services used in a way that the customer can clearly understand.

Another key task is to monitor the services provided to be able to comply with the guaranteed service quality. This monitoring is a continuing process. Any faults or failures in resources, e.g. virtualization servers, virtual machines, load balancers, etc. need to be detected quickly so that appropriate countermeasures can be taken as rapidly as possible. Besides security management, other tasks that are usually part of a CSP's repertoire are:

- A) Patch and change management
- B) Configuration management
- C) Network management
- D) System management
- E) Application management Reporting

Trusting the CSP and their offerings is currently cited as a key motivator when users are asked why they decide for or against cloud offerings. Trust is based on the assessment as to whether a provider has covered all the risks, both those in the data security area and in areas such as data protection, technology and the law – sufficiently, adequately and sustainably. It is a good idea for CSPs to get their information security management system certified so that they can provide evidence that they provide sufficient security even when there is a high level of protection required in terms of confidentiality and availability. CSPs should preferably be certified in compliance with ISO 27001 based on IT, ISO 27001 or other established standard. The CSP having an efficient information security management system (ISMS) is an essential basic, if Cloud Computing is to be reliable and secure. Key parts of ISMS are a functioning information security organization and an information security concept as tools for managing the implementation of the security strategy. A CSP should use the security organization chart to give their customers the names of suitable contact persons able to answer the customer's security questions.

Here and in the following, the security recommendations listed are firstly subdivided according to whether they are aimed at private or public clouds, and secondly assigned to one of three categories. In this context B stands for basic requirement (aimed at all cloud service providers)

C+ (=Confidentiality high) covers additional requirements for areas with a high confidentiality protection requirement.

A+ (=Availability high) covers additional requirements for areas with a high availability protection requirement.

A right-pointing arrow represents an average threat level and an up -pointing arrow an elevated threat level for private or public clouds.

| Security Management for Providers   | Private ⇨ |    |    | Public ⇨ |    |    |
|---|-----------|----|----|----------|----|----|
|   | B         | C+ | A+ | B        | C+ | A+ |
| Defined procedural model for all IT processes (e.g. as per ITIL, COBIT)   | ✓         |    |    | ✓        |    |    |
| Implementing a recognised information security management system (e.g. by BSI standard 100-2 (IT-Grundschutz), ISO 27001)                       | ✓         |    |    | ✓        |    |    |
| Sustainably implementing an information security concept for the cloud  | ✓         |    |    | ✓        |    |    |
| Evidence of adequate information security (certification)   |           | ✓  | ✓  |          | ✓  | ✓  |
| CSP has an adequate organisational structure for information security (including named contact persons to answer customers' security questions) | ✓         |    |    | ✓        |    |    |

TABLE 1: Security recommendation list according to type of cloud

## 3.2 Security Issues in Cloud

If a Cloud Computing platform is to be made operationally secure, all the issues potentially posing a threat to the confidentiality, integrity and availability of the data stored there needs to be examined. Besides a well-structured procedural model for all IT processes, it is important that security architecture be set up to protect resources (employees, infrastructure, networks, IT systems, applications, data, etc.) and that the customer is securely isolated. A robust separation of customers at every level in the Cloud Computing stack (application, servers, networks, storage, etc.) is a fundamental requirement that each Cloud Computing platform should meet [6]. This requirement applies equally both to public and private clouds. The issues described below should be examined when setting up solid security architecture for Cloud Computing.

### **3.2.1 Data Centre security**

Data Centres form the technical basis for Cloud Computing. To this extent, it is important that every CSP ensures their systems are secure in compliance with the current state the technology. This includes permanent monitoring of access, for example using video monitoring systems, movement sensors, alarm systems and trained security personnel. Any provision components which are essential for operations, for example the power supply, air-conditioning and Internet connection, should be designed to be redundant. Modern fire protection precautions also need to be taken, and tested on a regular basis. Overall, a data centre should form a security area that affords adequate protection against damage by the elements, e.g. caused by storms and flooding, and against unauthorized entry [7]. If a customer requires a particularly high level of availability for their services, the CSP should also reserve capacities in backup or redundant data centres which can compensate for another data centre failing. The data centres should be located far enough away from each other geographically so that a controllable damage event, e.g. fire, explosion, road, rail, water or air accidents and natural disasters with a limited impact such as flooding does not simultaneously affect both the data centre originally being used and the one containing the backup capacities. In the SaaS area, many providers do not operate their own infrastructure. If this is the case, the requirements set out here must be met by the subcontractor used by the SaaS provider, i.e. in this case the data centre operator.

### **3.2.2 Server security**

The servers represent the environment for performing the processes and their computations. For this reason the operating systems deployed on the servers should be hardened to the extent that they offer the smallest possible area to attack. To achieve this, when the basic installation is being undertaken, only the necessary software packages should be added and any superfluous programs and services should be disabled or, better, uninstalled. Standard measures to protect IT systems, such as host firewalls, host-based intrusion detection systems, etc. should be implemented and regular integrity reviews run on important system files [16]. Host-based intrusion detection systems are characterized by the fact that they are run on the IT system to be monitored. They are typically deployed to detect attacks made at the application or operating system level. Examples of

such attacks are policy violations by users, failed login attempts and malware such as Trojan horses.

The technical basis for providing and using cloud services reliably and securely are provided by a broadband connection, standardized and widely-used transmission protocols, a service-oriented architecture and, above all, virtualization. Providers deploy different hypervisors for server virtualization. The hypervisor is the central component of server virtualization controlling access to shared resources. With a few exceptions, no attacks on the hypervisor have yet appeared in the wild [ ] - they have only been described in theoretical terms or as proof-of-concept. Should an attack succeed, however, the consequences are devastating. The hypervisor can be attacked, for example, by manipulating CPU registers that control the virtualization functions. Errors in implementing the resources provided by the hypervisor to the virtual machines (VMs) can also cause the hypervisor to be compromised. To this extent, CSPs who deploy server virtualization should revert to certified, hardened hypervisors. The recommendations that manufacturers publish on configuring virtualization servers securely should be used when hardening hypervisors. Certification should be based on the globally accepted “Common Criteria for Information Technology Security Evaluation”, known as the Common Criteria for short. PaaS or SaaS providers using server virtualization, such as Microsoft with the Windows Azure platform, should also guarantee the security of the guest operating systems.

### **3.2.3 Network security**

In the past, Cloud Computing platforms have often been misused either by placing malware there which is then used to send spam, or their processing power has been exploited to crack passwords using brute force attacks or to hide command and control servers (C&C servers) used to control botnets. To prevent these and similar attacks as well as the misuse of resources, each CSP should take effective security measures to defend against network-based Attacks. As well as the usual IT security measures such as anti-virus protection, Trojan detection, spam protection, firewalls, Application Layer Gateway and IDS/IPS systems, and particular care should be taken to encrypt all communication between the CSP and the customer and between the provider’s sites. If a third party provider is required to deliver the services, the communication with them also needs to be encrypted. Because of the concentration of resources in centralized data

centres, an attack which is a particular threat to public Cloud Computing platforms is the Distributed Denial of Service attack [13].

According to a report by Arbour Networks, a provider of security solutions, attacks (such as the DNS Amplification/Reflection Attack) can now achieve enormous bit rates (over 100 Gbps) [7, 13]. A standard backbone is designed for a far lower data rate. As a result, many CSPs can hardly defend against Denial of service attacks using high data rates. This can have serious consequences for both the victim themselves and other connected customers. Against this background, each public CSP should undertake suitable measures to defend against denial of service attacks. Owing to the fact that many CSPs can scarcely protect themselves against denial of service attacks using high data rates, the option exists to buy these mitigation services from larger Internet service providers (ISPs) and regulate their use in agreements. Measures should also be implemented to detect internal denial of service attacks by cloud customers other cloud customers .The incorrect configuring of a system is frequently the reason for successful attacks. As Cloud Computing platforms consist of many different components.

The overall configuration is very complex. Changing a configuration parameter for one component (e.g. virtualization server) can, when interacting with other components (e. g. network or storage) lead to security vulnerabilities, faulty functions and/or failures. For this reason, the components need to be securely and carefully configured. All CSPs should also ensure that their networks are suitably segmented, preventing any faults from spreading freely. In this context the option exists to define and set up different security zones within the provider's network, based on the protection requirement. Examples include:

- a) Security zone for managing the cloud
- b) Security zone for the live migration, if server virtualization is being used
- c) Security zone for the storage network
- d) With IaaS, customer to have their own security zones for the virtual machines

The CSP's management network should be isolated from the data network. If the cloud infrastructure or cloud services are being administered remotely, this needs to be accomplished via a secure communication channel (e.g. SSH, TLS/SSL, IPSec, VPN).If a service consumer has particularly high availability requirements in terms of the services they are drawing down, the CSP's sites should be networked on a mutually redundant basis.

### **3.2.4 Application and platform security**

In the case of offerings in the PaaS area, customers no longer have to worry specifically about database accesses, scalability, access controls, etc., as the platform provides these functionalities for them. Due to the fact that the customers use the platform's core functionalities to develop their own software, they can only succeed in developing software securely, if the entire software stack on the platform is developed and upgraded professionally and securely. CSPs typically deploy not just a large number of different software components, but they also continue to upgrade them in order to be able to optimally provide their customers with the services in the runtime environment. When developing software, all CSPs must have established security as a fixed component in the software development life cycle process (SDLC process). Security issues need to be addressed at each phase of the software development process, and programs and modules may only be deployed if they have been properly tested and approved by the CSP's security manager.

While software developed by the customer requires a secure basis (to be provided by the CSP), security issues also need to be considered in this respect. It is recommended that the CSP provides appropriate user guidelines for customers to create secure applications so that the programs the customer develops themselves fulfil certain minimum requirements in terms of security, documentation and quality. This is not only helpful for the customers but also emphasizes the provider's expertise and reduces the danger of security vulnerabilities in customer software impacting on other customers. If the CSP also calls in other suppliers to provide the platform's services, these requirements apply equally to them. Alongside code reviews, automated review tools should also be deployed and vulnerability tests run [23]. Automated review tools can, for example, detect common programming errors such as infinite loops and null pointer exceptions. Where there is a higher level of protection requirement, the CSP should also automatically check the code the customers have developed themselves for vulnerabilities.

### **3.2.5 Data security**

The data life cycle comprises its generation, data storage, data usage, data distribution and data destruction. Each CSP should support all these phases in the data life cycle with appropriate security mechanisms. A number of storage technologies, e.g. NAS, SAN, Object Storage, etc., are used to store data. Common to all these storage technologies is

the fact that many customers share common data storage. In this type of constellation, a secure separation of customer data is essential and should, therefore, be guaranteed [22]. As with traditional IT, in Cloud Computing data losses are a threat that must be taken seriously. To avoid data losses, each CSP should do regular data backups based on a data security plan. Technical defects, incorrect parameterization, obsolescent media, inadequate data media administration and non-compliance with regulations stipulated in a data security plan can result in an inability to reinstall backups and reconstruct the data inventory. So there is a need to sporadically check whether the data backups created to restore lost data can be re-used. Depending on the length of time between backing up the data and restoring the data due to data loss or some other incident, the most recent data modifications may be lost. So a CSP should immediately notify its customers if data backups need to be restored, and in particular indicate the status of the backup. The backing up of data (scope, save intervals, save times, storage duration, etc.) should be transparent and auditable for the customers.

### **3.2.6 Authentication**

In Cloud Computing, hardware, software and services are used by many users. The role of identity and authorizations management is to ensure that only authorized persons may use the IT resources [24]. Access to all the IT systems or services must be made secure by identifying and authenticating the users or IT systems seeking access. For security-critical application areas, strong authentication should be used, i.e. two-factor authentication as is normal, for example, in online banking. Any network access should, in principle, be made secure by strong authentication [18]. These strict requirements apply particularly to the CSP's staff. They, too, should only gain access to the IT resources being administered via strong authentication, i.e. for example via a hardware-based authentication system using chip cards or USB sticks or via one-time passwords that can also be generated by hardware devices. This is absolutely indispensable for access via the Internet. If a CSP administrator accesses the CSP systems from a secured company network via a VPN for which they have already had to authenticate themselves with two factors, then in this case a second two-factor authentication can be dispensed with [25, 26].

Where security requirements for the services provided are high, service users too can only be given access to the services after a strong (e.g. two-factor) authentication, if the access to the service used ensues directly via the Internet [4]. If a customer accesses the cloud

services for which they must authenticate themselves with two factors via a VPN from the secured company network, no additional two-factor authentication to use the cloud services is necessarily required. In the case of encrypted communication between a CSP and service consumers, access to the services can be restricted to particular IP addresses or domains in order to increase security.

### **3.3 EXISTING AUTHENTICATION PROTOCOL**

In this section we analysed some existing authentication schemes which are rely on client-server architecture. We know Authentication is a simple mechanism where one presents a set of information to a system. If their all credentials have a match on the server, the server returns a value which shows authorization; otherwise authentication fails for that user [9]. The main goal of authentication is to verify specific information about the user which represents authenticity of correct user [17]. Right now most of web serviced sites have adopted a simple user ID/password mechanism for fulfilling the goal of identification and authentication. Many more solutions are there which can identify the user. The most popular and widely used authentication scheme is, in which, the server stores the value of a user's password. In this scheme, a table of password is used to verify the correctness or validity of users, but if this password table is stolen, or modified by someone like adversary [20]. Some recent password authentication schemes which are based on smart card have also been proposed [17]. In Smartcard the long term secret key is stored and it is considered that the smartcard is never detected or compromised by adversary [24].

So basically these schemes are based on one factor authentication. Even two factor authentication can be broken by compromising both factors [28]. Cloud computing is also based on client server architecture, where, lots of people uses same infrastructure at a very large scale. But it needs stronger authentication than traditional client server architecture system. Some systems use complex authentication via smartcard system, where users can have their user id and password, and also a passkey which generate and change by time within 60 seconds from the smart card..



## CHAPTER 4

# PROPOSED ALGORITHM AND FRAMEWORK

---

As we have seen from above that authentication is the main key for information security. And Most of the current existing user authentication techniques have many security flaws. Password based authentication is very commonly used scheme now a days, but this scheme is also vulnerable to replay, eavesdropping, brute force, dictionary attacks [29]. We have proposed and create a new framework for the purpose of authentication of user to access several cloud computing services and applications from cloud server. In this chapter, we implemented various phases of secure authentication. We have already known that authentication is very important key in secure communication. For this purpose, we proposed a framework which is based on some tricky known factors like one time password, arithmetic expression and a magic number. These factors are used in different levels of authentication. Firstly we need to decompose services into three levels in terms of frequently used services and confidentiality level of documents. That means if a service is common for user or it is used frequently then we can categorize it into first level and it will be kept in level 1 authentication. For example pictures and music and some normal documents can be categorized into this. Like this in second level we can put moderate important documents and according to this we can categorize this level by another authentication factor. Finally, in last level we can keep some very important data like personnel stuffs and official documents and papers.

Many of the current existing authentications are rely on static passwords which can be easily breakable whereas our proposed scheme is based on some kind of dynamic behaviour which is secured by multi-factor secret-splitting mechanism and it is more efficient and user friendly. So for proper framework we need to design various phases like registration page, login page, and then all level of authentication pages. For all factors imposing in authentication we have to keep user's credentials. For this purpose we need a database. Some assumptions are made like user and cloud service provider are supposed to be trusted. After registration no user is trusted. Users are required to fill those credentials correctly to authenticate themselves. They need to provide real and correct identification details during login and authentication level. Once mutual authentication is established they can use services, applications and resources. After authentication it is considered that server is never compromised with adversary

## 4.1 Entities Which Are Used In Proposed Framework

- A) Cloud service provider (CSP): Cloud service provider is known as administrator of cloud who takes care of ongoing changes in database and provides access to user after successful authentication of user's identity. It is core entity in client server architecture.
- B) User: he is a customer who uses cloud environment and cloud service and application for computing purpose. He has to register himself in authentication framework by filling all necessary credentials to the server.
- C) Cloud access management server (CAM server): This entity responsible for all management and cloud computing
- D) Browser and Internet: It is used to access all cloud services and also used for register and authentication by user.
- E) Mobile phone: Mobile phone no is used where server sends secret key and one time password (OTP). So we can say mobile phone is used for secure communication between CSP and user.
- F) Email id: An email id is used to send secret hash function and a value for registration purpose. It is also used in case of forget password and secret key change phase.

## 4.2 Key approaches used

- A) Arithmetic expression: Arithmetic expression is a very simple expression which has two operands (1-9) and one operator (+, %, -, \*). It is generated randomly by cloud server and shown to user just as normal expression. After that user needs to solve the value of expression by modifying the operands with the help of hash function and secret key. The hashed function is sent to user's email id normally. This hashed value is used for authentication of user by CAM server [27].
- B) One time password (OTP): one time password is a six digit number which is sent to user's contact number and user needs to acknowledge to the server by type that OTP. It is used for authentication of valid user.
- C) Magic number: It is a number which changes every time you login. First time magic number is provided to user in registration phase. After that user has a secret increment value by which he/she can track of this magic number.

## 4.3 REGISTRATION PHASE

In this phase user needs to register themselves at cloud server we will say it cloud service provider (CSP). For this user needs to provide all identification details to server after filling all details server process these details and save contact no and email id of that particular user for authentication purpose. In this phase users are required to provide appropriate information so that server can communicate to themselves. We have to follow some steps to achieve registration successfully.

Step 1: User request to server for new account.

Step 2: User needs to fill user name which must be unique.

Step 3: User needs to fill his/her contact no must be in 10 digits.

Step 4: User needs to fill a valid email id.

Step 5: User needs to create a password. It must be long at least in 6 digits or character.

Step 6: User needs to confirm that password.

Step 7: After filling all above credentials he needs to submit all data. Now server stores all data and sends a hash function to user's email id.

Step 8: A secret key is sent to user's contact number

Step 9: An arithmetic expression is shown to user which is of 3 operand and 2 operators.

Step 10: Now user required to calculate that expression (v1) by the help of that hash function and secret key and needs to put the answer is in required field.

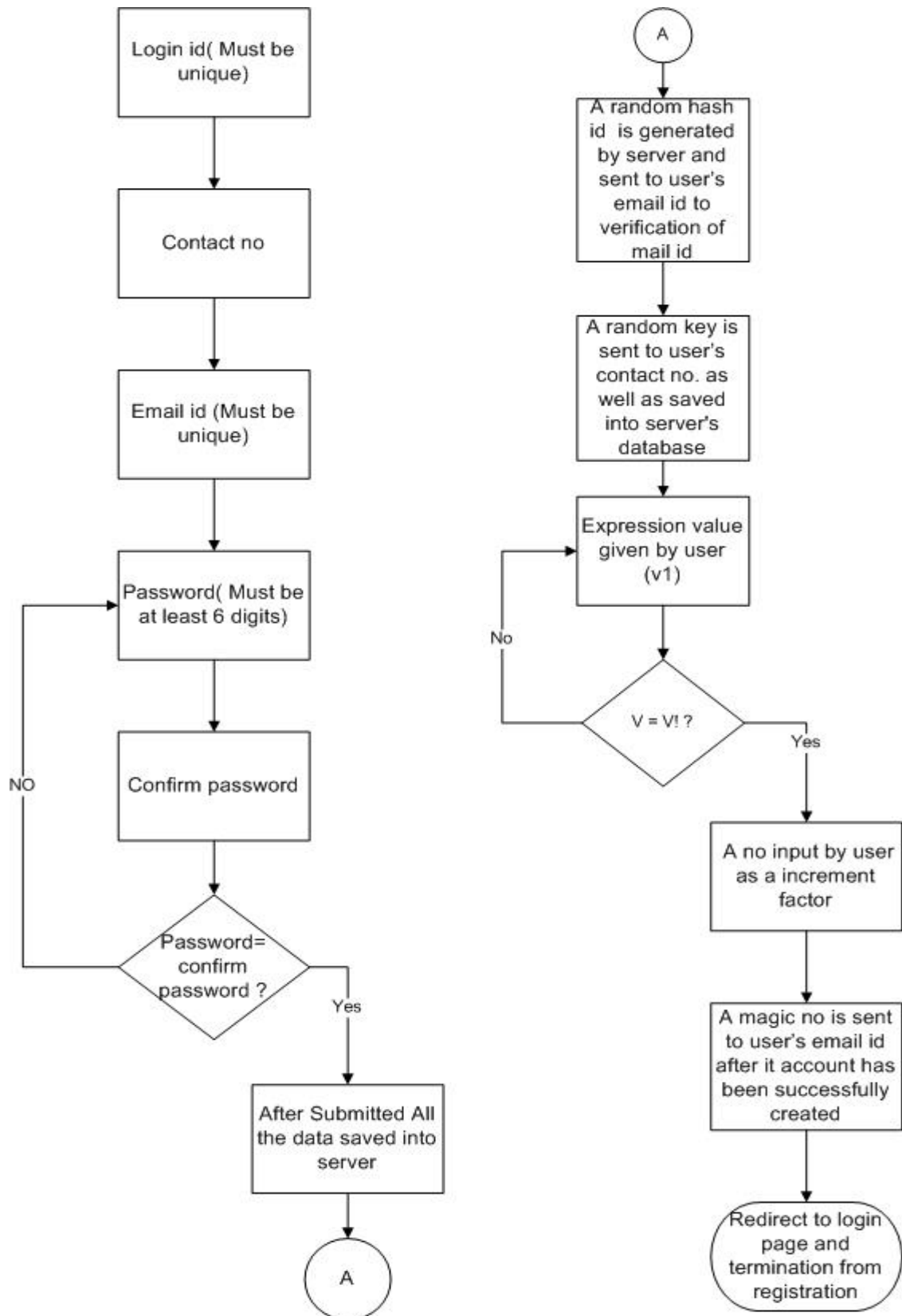


Figure 5: flow chart of registration phase

Step 11: CAM server checks whether  $v = v1$ . If it is true server shows an input field where user needs to take an integer increment factor. After submitting that integer a magic number is sent to user's email id and also stored into server.

Step 12: Now your registration has been done successfully. And we will redirect to login page. If it is not true server shows a message "mismatch verifier".

Step 13: After all verification of user registration is complete server store all credential like secret key, mobile no, magic number, increment factor etc.

## 4.4 Login

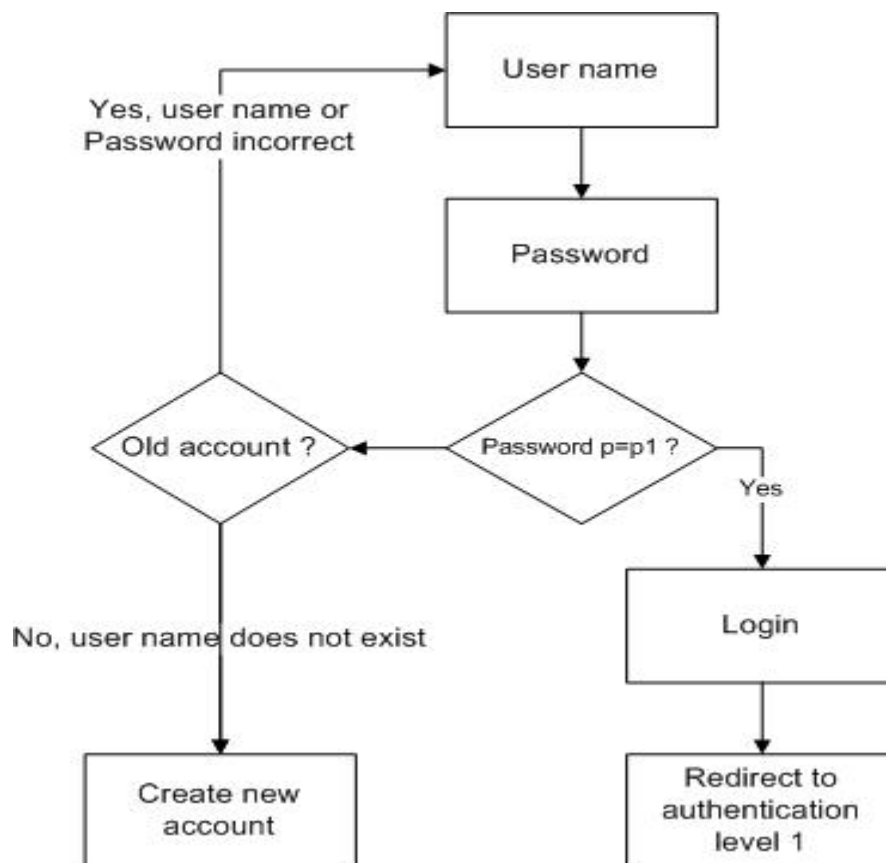


Figure 6: flow chart of login phase

Step 1: User provide his user name which he gave at the time of registration.

Step 2: User fills the password field.

Step 3: After filling those above field server checks whether this user name is exist or password is Correct.

Step 4: If server finds that username in database and password is correct then it allows user to login otherwise it shows a message that user name or password is incorrect.

Step 5: If user is new user or does not have any account. He can choose create new account from this page.

Step 6: Once he chooses create new account field he will redirect to registration page.

## 4.5 Authentication phases

### 4.5.1 Level 1 authentication

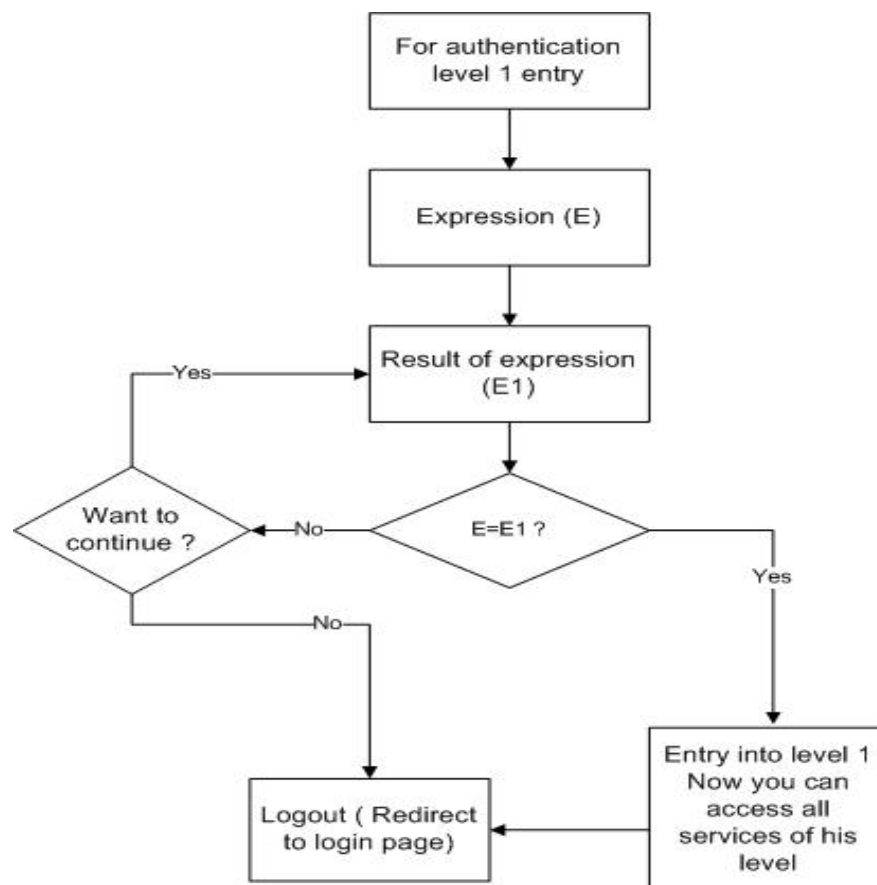


Figure 7: Flow chart of level 1 authentication

Step 1: After successfully login we redirect to authentication phase. In this we can go to first Level of services.

Step 2: For authentication here, an expression is shown to user.

Step 3: user needs to find the result with the help of secret hash function and secret key which are previously given to user in secret manner.

Step 4: Now server checks the result whether it is correct or not. If it is correct server allows user to enter into level 1 and now user can access this level services and resources. If result is not correct then user can again try or logout from there.

### 4.5.2 Authentication level 2

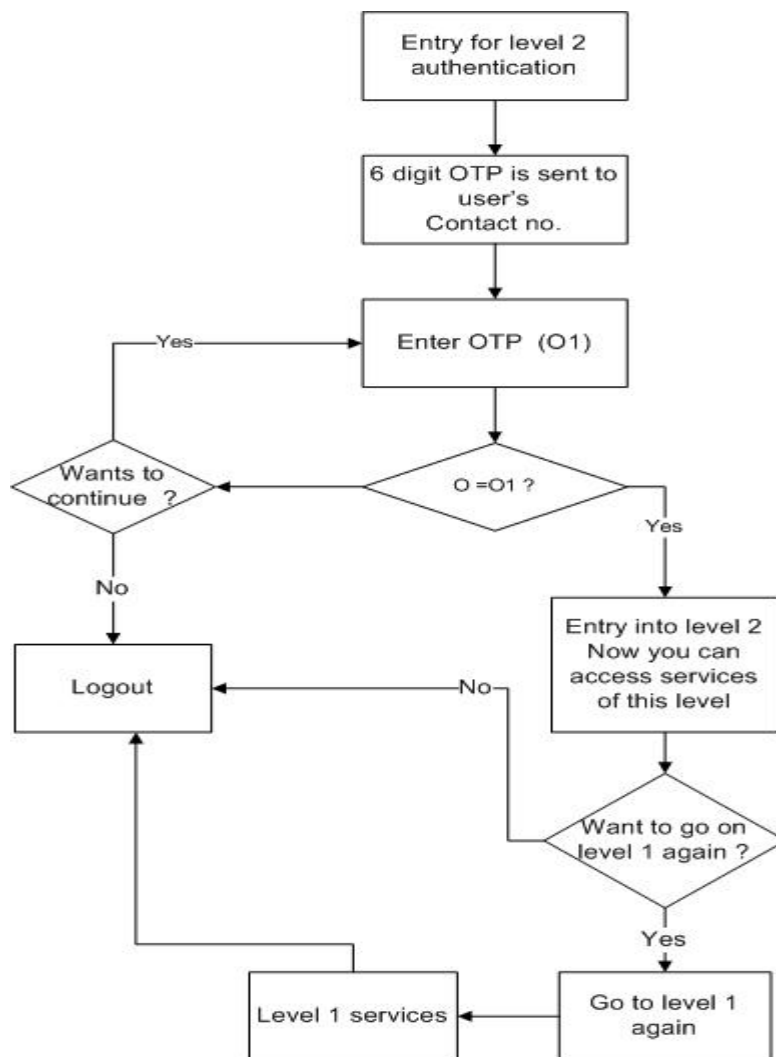


Figure 8: Flow chart of level 2 authentication

Step 1: After successful authentication into level 1, user have option to go on another level.

Step 2: User needs to click on field of level 2 and then server generate a OTP (one time password) and sent it to user's contact no.

Step 3: After receiving OTP in mobile phone user needs to type that OTP in required field to complete this authentication

Step 4: Server checks the correctness of OTP and allow user to entry into level 2 where user can access services from here.

Step 5: If user misses that OTP, he/she can refresh for new OTP or they have an option for logout also

Step 6: If anytime user wants to go on level 1 he can go by simply click on downgrade to level 1 field.

### **4.5.3 Authentication level 3**

Step 1: After successfully completion of second level authentication user can move to level 3 which is for highly sophisticated resources.

Step 2: for this authentication user needs to fill a magic no by the help of a secret constant increment factor.

Step 3: If user forget his magic no, he can get it by simply click on forget magic number field. Server will send previous magic number through a mail to user's email id. Now if user is valid then he knows that secret constant factor and can move into this level of cloud services.

Step 4: Server now checks whether it belongs to correct user or not by matching magic number. If it matches server allows user to enter into third level.

Step 5: Here also user anytime can move into second level and also if he does not wants to proceed he can simply sign out himself.



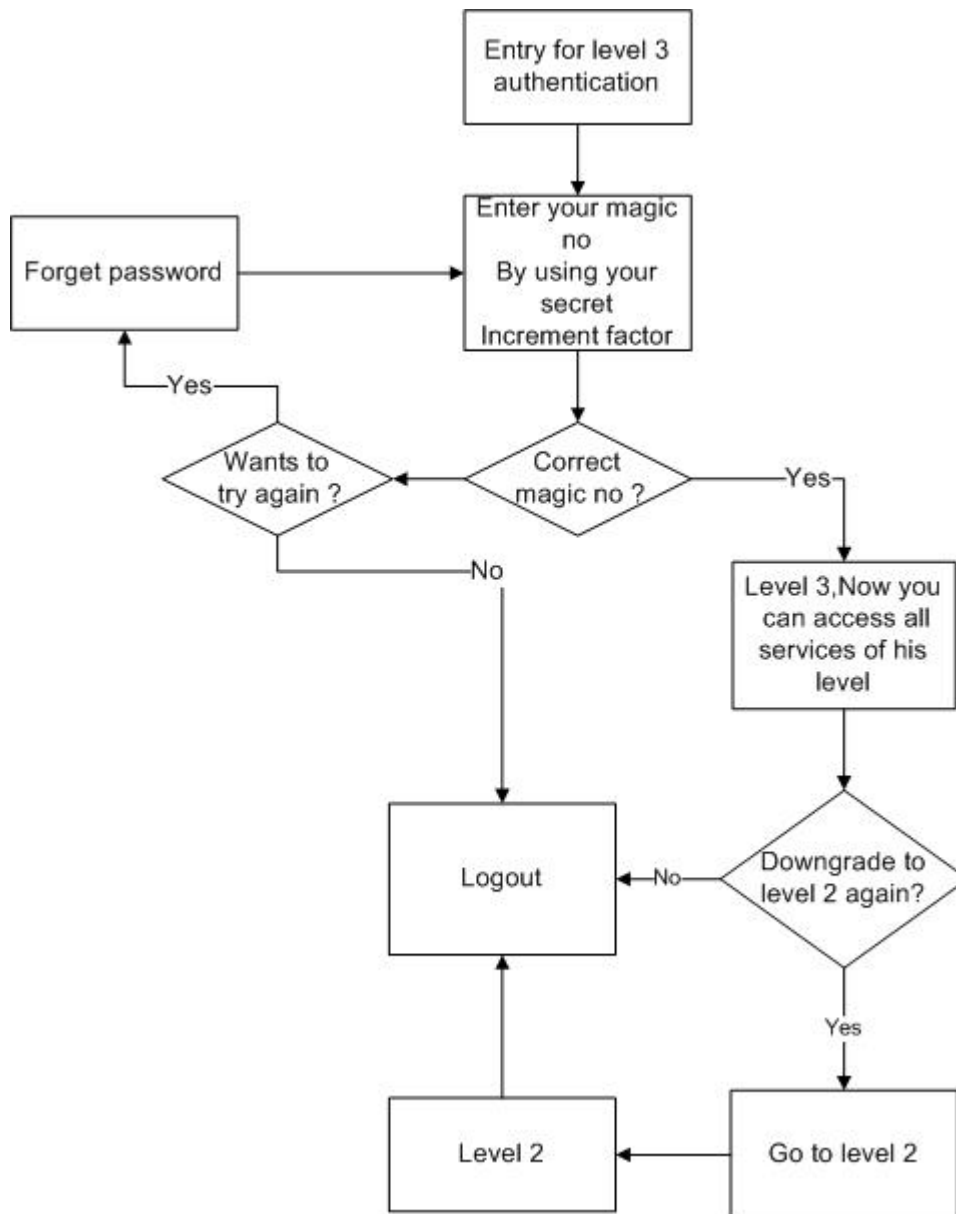


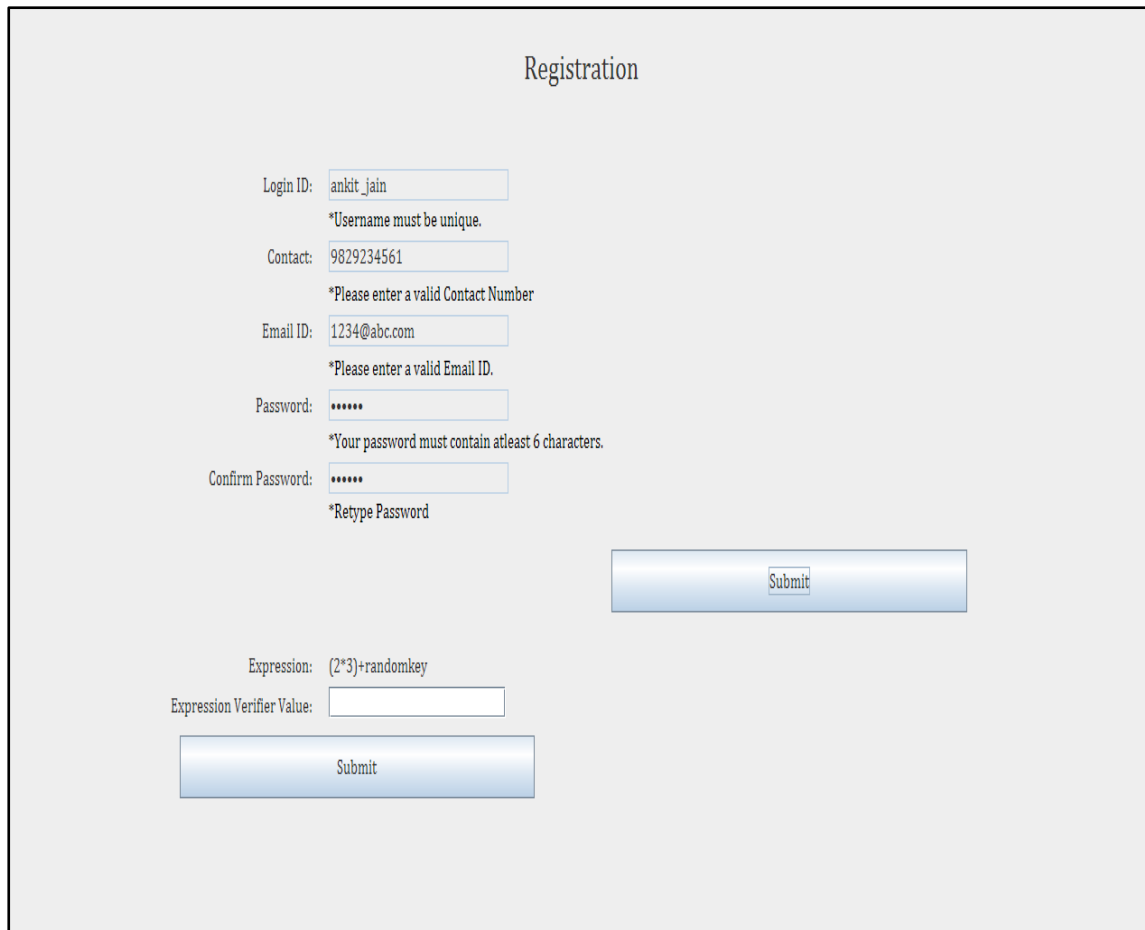
Figure 9: Flow chart of level 3 authentication

## CHAPTER 5

# IMPLEMENTATION AND RESULTS

---

### 5.1 Registration module



The screenshot shows a web form titled "Registration". It contains several input fields and validation messages:

- Login ID:** . Below it, a message: *\*Username must be unique.*
- Contact:** . Below it, a message: *\*Please enter a valid Contact Number*
- Email ID:** . Below it, a message: *\*Please enter a valid Email ID.*
- Password:** . Below it, a message: *\*Your password must contain atleast 6 characters.*
- Confirm Password:** . Below it, a message: *\*Retype Password*

There are two "Submit" buttons. The first one is a large blue button to the right of the password fields. The second one is a smaller blue button below the "Expression Verifier Value" field.

**Expression:**  $(2*3)+\text{randomkey}$

**Expression Verifier Value:**

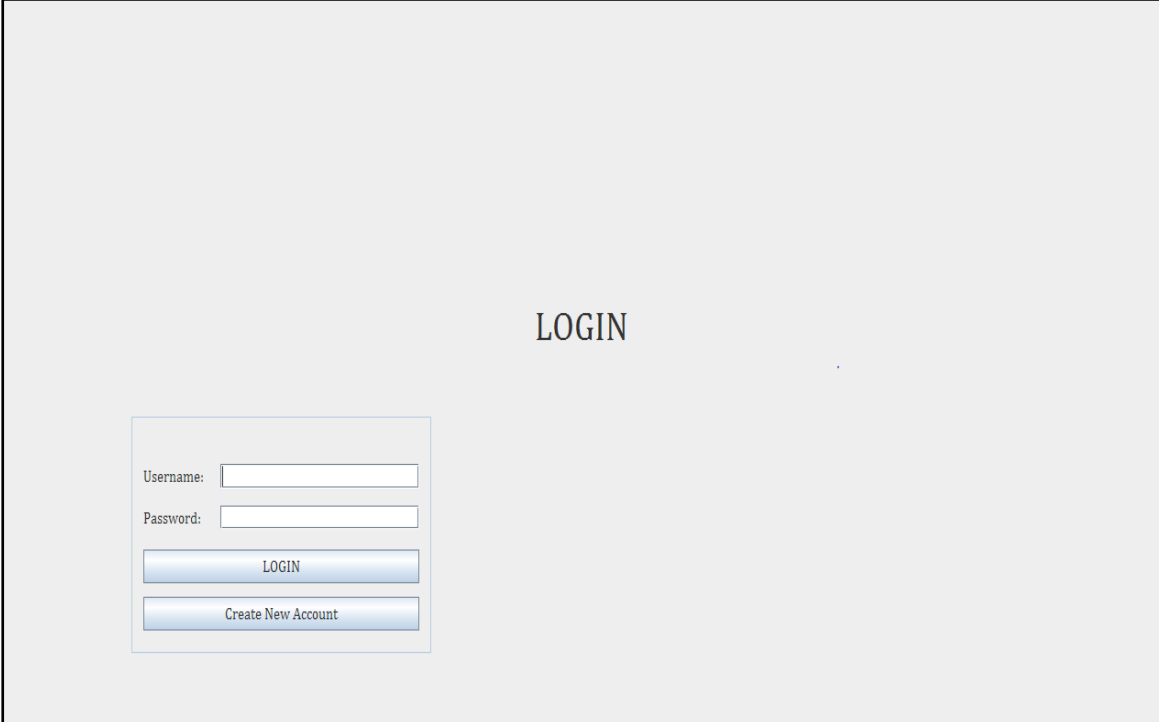
Figure 10: registration module

Registration is very important phase for authentication because it provides all necessary information of user to server so that server can identify user and his validity. In registration phase user needs to deposit his all required credentials like user name (must be unique), contact no, email id, password (at least of 6 characters or digits). After filling all these entries server stores all of them and sends a hash function to user's email id and a secret key value to user's contact no.

An arithmetic expression is shown to user which is of 3 operand and 2 operators. No user required to calculate that expression ( $v1$ ) by the help of that hash function and secret key and needs to put the answer is in required field. CAM server checks whether  $v = v1$ . If it is true server shows a input field where user needs to make a integer increment factor. After

submitting that integer a magic number is sent to user' email id and also stored into server. Now your registration has been done successfully. And it will redirect user to login page.

## 5.2 Login module

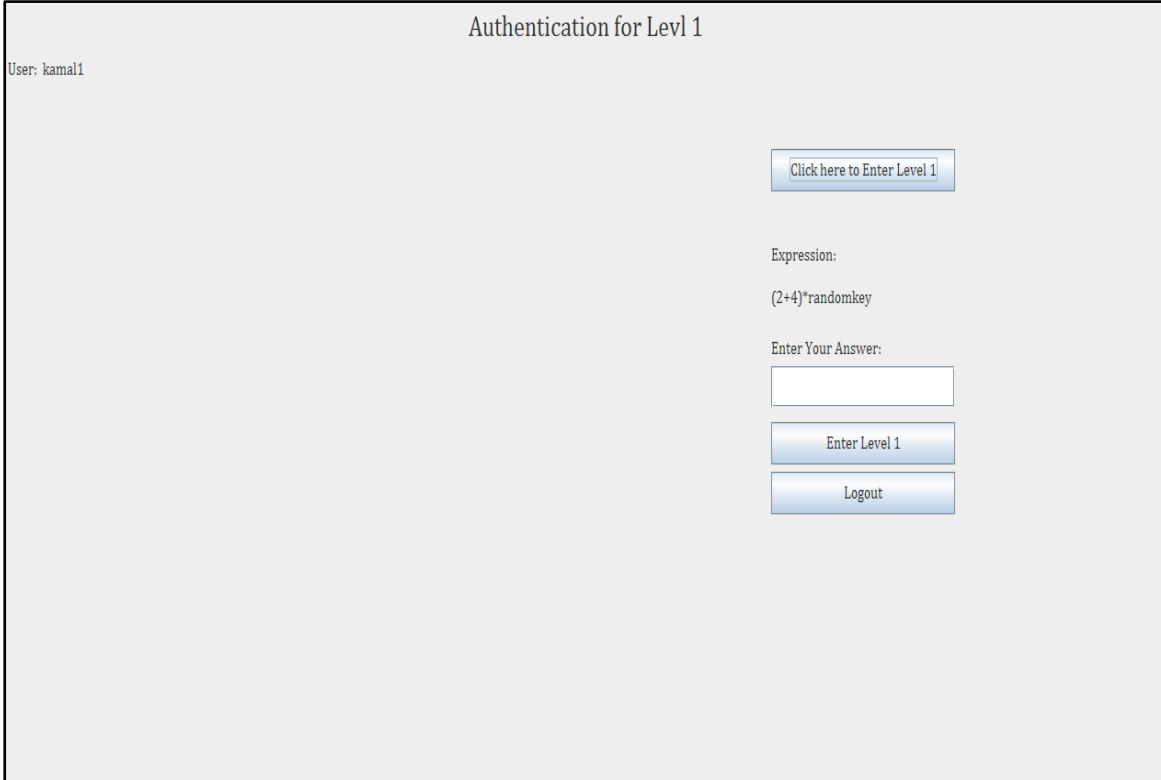


The image shows a login module interface. At the top, the word "LOGIN" is centered. Below it, there is a form with two input fields: "Username:" and "Password:". Below the "Password:" field are two buttons: "LOGIN" and "Create New Account".

Figure 11: login module

In this phase user can login himself by providing appropriate information. For login only user id and password is required. User provides his user name and password which he gave at the time of registration. After filling those above field server checks whether this user name is exist or password is Correct. If server finds that username in database and password is correct then it allows user to login otherwise it shows a message that user name or password is incorrect.

## 5.3 Level 1 authentication



Authentication for Level 1

User: kamal1

[Click here to Enter Level 1](#)

Expression:  
(2+4)\*randomkey

Enter Your Answer:

[Enter Level 1](#)

[Logout](#)

Figure 12: authentication 1 page

Authentication is performed here is quite different. We have categorized services into 3 different levels and so their user authenticity requirement is also different. For this 3 different type of factors are used. Here on this level I have used arithmetic expression which is of 3 operands and two operations. A hash function and secret key is also secretly sent to user to solve that expression.

For authentication here, a expression is shown to user. user needs to find the result with the help of secret hash function and secret key which are previously given to user in secret manner. Now server checks the result whether it is correct or not. If it is correct server allows user to enter into level 1 and now user can access this level services and resources. If result is not correct then user can again try or logout from there.

## 5.4 Level 2 authentication

Authentication for Level 2

User: kamal1

Current Level: 1

One Time Password

346276

OK

Click here to Enter Level 2

Enter OTP:

Enter Level 2

Downgrade to Level 0

Logout

Figure 13: authentication 2 page

In this level I have used OTP for authentication. It is simply a six digit value which is sent to user's mobile number during authentication. It is secretly sent to user and it is random six digit number also it vanishes after 2 minutes of its generation.

After receiving OTP in mobile phone user needs to type that OTP in required field to complete this authentication. Server checks the correctness of OTP and allows user to enter into level 2 where user can access services from here. If user misses that OTP, he/she can refresh for new OTP or they have an option for logout also. If anytime user wants to go on level 1, he can go by simply clicking on the downgrade to level 1 field.

## 5.5 Level 3 authentication

Authentication for Level 3

User: kamal1 Current Level: 2

[Click here to Enter Level 3](#)

Enter Magic Number:

[Forgot Password](#)

[Enter Level 3](#)

[Downgrade to Level 1](#)

[Logout](#)

Figure 14: authentication 3 page

In this level I have used a magic number which is initially sent by a server to user's email id secretly. But every time it changes by a constant factor. For this there is a constant increment factor and only respective user knows about that.

If user forget his magic no, he can get it by simply click on forget magic number field. Server will send previous magic number through a mail to user's email id. Now if user is valid then he knows that secret constant factor and can move into this level of cloud services. Now Server checks whether it belongs to correct user or not by matching it to original magic number. If it matches server allows user to enter into third level. Here also user anytime can move into second level and also if he does not wants to proceed he can simply sign out himself.

## CHAPTER 6

# SECURITY ANALYSIS OF PROPOSED FRAMEWORK

---

**A) Secure Credential Management:** The cloud management server stores all the credentials and useful information of the user in a secure and trusted database. Server always checks the availability of user's unique ID each time of new registration [19].

**B) Secure Credential Change:** Proposed framework provides users to change password, key, mobile phone, constant factor, and secret key using user friendly and secure manner, at any time. This change facility makes the proposed framework inherently secure and stronger compared to the static password based mechanism.

**C) Replay Attack:** Three authentication levels which are rely on three factors-1) secret key (K) and arithmetic expression, 2) one time password (OTP), magic number. Also valid user login ID and password is required for authentication. So it makes very difficult to adversary to apply replay attack.

**D) Man in the Middle Attack (MITM):** In this framework suppose attackers anyhow manage to find the user ID and password and are able to login into the system. However, they cannot access overall services and application resources, because user needs authentication every time which requires secret key (K), one time password (OTP), and a special magic number. And these secrets are exchanged only between the user and the server using separate secure OOB channel [17, 18].

**E) Stolen Verifier Attack and Unauthorized Access Attack:** In our proposed scheme, all authentication factors are not available simultaneous. Thus, even if one credential is stolen or lost, authentication needs other parameters for login. Also the framework provides credential change facility and in case of a theft, the user can change the required parameters. Hence stolen verifier attack and unauthorized access attack is not applicable in this framework.

**F) Impersonation attack:** In the proposed framework, secret key for arithmetic expression is never transmitted through the public channel. Secret key is the key factor for each authentication. Only hashed value  $V=h(E, X)$  of arithmetic expression is transmitted to the server. Also the scheme uses high entropy OTP, delivered to user using a separate out of band channel for authentication. Hence the proposed scheme is strong and safe against impersonation attack.

**G) Phishing attack:** In this framework mutual authentication between the user and the CAM server, based on multi-factor credentials is performed. Secret key, OTP, magic number and mobile phone are required for authentication. Only the genuine server can send proper authentication information. And user responses can be verified by genuine server only.

**H) Password guessing attack:** In the proposed framework authentication is based on many factors using secret key, arithmetic expression, OTP and magic number. The use of OOB secure channel for exchange of credentials which provides more robustness to the scheme. In the proposed framework, just password guessing is not sufficient for authentication. It also requires secret key (K), user's mobile phone and secret magic number.



## **CHAPTER 7**

### **CONCLUSION**

---

The advantage of the present use of smart phone is taken in our proposed framework. The proposed framework provides an efficient and feasible solution by enhancing the conventional user ID and password based authentication with driving dynamically several factor secret-splitting based authentication scheme. It designs more secure authentication framework for cloud users which can protect from many types of security attacks.

We presented a strong authentication protocol that is quite suitable for cloud-based services. In comparison with existing protocol such as traditional user ID and password, this protocol does not need any physical tokens and it is also protect against replay attacks. The basic strength of this framework is the fact that user is authenticated himself dynamically instead of statically. This authentication framework has lots of security features, such as credential and identity management, session access mutual dynamic authentication, token agreement between the cloud management server and user. And it is user friendly also. The end result is a user authentication system that establishes specific level of security for the users to meet their dynamic requirement of security levels for the cloud computing resources and services.

## REFERENCES

---

- [1] Mell, P, and Grance, “*The NIST Definition of cloud computing*,” Computer and Information Sciences, vol. 53, no. 6, pp.1-10, 2009
- [2] Vaquero, L., Rodero-Merino, L., Caceres, J, and Lindner,” Abreak in the clouds: Toward a cloud definition,” ACM SIGCOMM Computer Communication Review, vol.39, pp.50-55,2009
- [3] Lee Badger, Robert Bohn, Shilong Chu, Mike Hogan, Fang Liu, Viktor Kaufmann, and Jian, “Useful Information for Cloud Adopters,”NIST Cloud Computing Program, vol .2,no.1, pp.1-73 , 2011.
- [4] S. Lee, I. Ong, H.T. Lim, and H.J. Lee, “Two factor authentication for cloud computing,”International Journal of KIMICS, vol. 8, Pp. 427-433.
- [5] V.KRISHNA REDDY 1, and Dr. L.S.S.REDDY, "Security Architecture of Cloud Computing", International Journal of Engineering Science and technology (IJEST), Vol. 3 No. 9 September 2011.
- [6] Kuyoro S, Ibikunle F., and Awodele O. "Cloud Computing Security Issues and Challenges"
- [7] Danish Jamil Hassan Zaki, "Cloud Computing Security" International journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4
- [8] R. M. Needham and M. D. Schroeder, “Using encryption for authentication in large networks of computers,” Commun. ACM, vol. 21, no. 12, pages 993–999, 1978.
- [9] Daniel Mouly , “ Strong User Authentication, Informa-tion Systems Security”, vol. 11, no.2, pp. 47-53.
- [10] J. Heiser and M. Nicolett, “Assessing the security risks of cloud computing,” Gartner Report, 2009, online Available: <http://www.gartner.com/DisplayDocument?id=685308>

- [11] S. Shin, K. Kobara, and H. Imai, "A Secure Construction for Threshold Anonymous Password-Authenticated Key Exchange", IEICE Transactions on Fundamentals, Vol.E91-A, No.11, 2008, pp.3312-3323.
- [12] Federal Office for Information Security (BSI), IT-GrundschutzMethodology,BSI standard 100-2, Version 2.0, May 2008
- [13] Rajan,S., and Jairath,A, "Cloud Computing: The Fifth Generation of Computing, Communication Systems and Network Technologies", IEEE Xplore, pp 665-667.
- [14] ENISA, Cloud Computing: Benefits, Risks and Recommendations for information Security,November (2009)<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk>
- [15] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol.34, No.1, pp.1-11,jan 2011.
- [16] M. Zhou, Z. Rong, W. Xie, W. Qian, and A. Zhou , "Security and Privacy in Cloud Computing: A Survey", Proc. of the Sixth InternationalConference Semantics Knowledge and Grid ( SKG'10), Beijing, China, pp.105-112, Nov. 2010.
- [17] S. Shin, K. Kobara, and H. Imai, "A Secure Construction for Threshold Anonymous Password-Authenticated Key Exchange", IEICE TransactionsOn Fundamentals, Vol.E91-A, No.11, pp.3312-3323 ,2008
- [18] M. Abdalla, M. Izabachene, and D. Pointcheval, "Anonymous and Transparent Gateway-Based Password-Authenticated Key Exchange", Proc. International Conference on Cryptology and Network Security (CANS'08), Hong Kong, China, Dec. 2008, pp.133-148.
- [19] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, D. Zou, "A Practical Privacypreserving Password authentication Scheme for Cloud Computing", Proc.of the IEEE 26th International Parallel and Distributed Processing SymposiumWorkshops & PhD Forum (IPDPSW'12), May 2012, Shanghai, China, pp.1204-1211.

- [20] L.Lamport,"Password Authentication with Insecure Communication," Communications of the ACM, vol. 24, pp. 770-772, 1981.
- [21] C. Lin, Hwang, T., "A password authentication scheme with secure password updating," Computers & Security, vol. 22, pp. 68-72, 2003.
- [22] Wang C, et al. (2009) "Ensuring data storage security in cloud computing," Proceedings of The 2009 17th International Workshop on Quality of Service (IEEE):1-9.
- [23] Michael E. Whitman "In defense of the realm: understanding the threats to information security" International Journal of Information Management 24 (2004) 43-57.
- [24] B. Lampson, Abadi, M., Burrows, M., and Wobber, E., "Authentication in Distributed Systems: Theory and Practice," ACM Transactions Computer Systems, vol. 10, pp. 265-310, 1992.
- [25] M. Peyravian, and Zunic, N., "Methods for Protecting Password Transmission," Computers & Security, vol. 19, pp. 466-469, 2000.
- [26] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang, "A password authentication scheme over insecure networks, J. Comput," System Sci. 72 (4) (2006) 727-740.
- [27] E.J. Yoon, and K.Y. Yoo, "New authentication scheme based on a one-way hash function and Diffie-Hellman key exchange," 4th International Conference of Cryptology and Network Security, CANS 2005, LNCS vol. 3810, Springer-Verlag, pp. 147-160.
- [28] G. Yang, D. S. Wong, H. Wang, and X. Deng, "Two-factor mutual authentication based on smart cards and passwords," Journal of Computer and System Sciences, vol 74, 2008, Pp. 1160-1172.
- [29] Dimitrios Zissis, and Dimitrios Lekkas, "Addressing cloud computing security issues" Future Generation Computer Systems 28 (2012) 583-592.