A Secure Data Transfer Technique for Cloud Computing

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Computer Science and Engineering

Submitted By
Pankaj Pateriya
(Roll No. 801232015)

Under the supervision of:

Dr. Inderveer Chana
Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

August 2014

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, *"A Secure Data Transfer Technique for Cloud Computing"*, in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Computer Science and Engineering* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Inderveer Chana* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Signature:

(Pankaj Pateriya)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Inderveer Chana)
Associate Professor,
Computer Science and Engineering Department

Countersigned by

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. K. Mohapatra)
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

No volume of words is enough to express my gratitude towards my guide **Dr. Inderveer Chana,** Associate Professor, Computer Science & Engineering Department, for providing her immense help, guidance, simulating suggestions and encouragement all the time. She has helped me to explore this vast topic in an organized manner and provided me all the ideas on how to work towards a research-oriented venture.

I am also thankful to **Dr. S. K. Mohapatra**, Dean of Academic Affairs, **Dr. Deepak Garg**, Head of Computer Science & Engineering Department and **Mr. Ashutosh Mishra**, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

I would also like to thank the staff members and my colleagues who were always there at the need of hour and provided with all the help and facilities, which I required, for the completion of my thesis work.

I extend my thanks to Dr. Maninder, Associate Professor, Computer Science & Engineering Department and Mr. Sukhpal Singh for sharing their expertise and time to help me accomplish this work.

Most importantly, I would like to thank my parents and the almighty for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.

(Pankaj Pateriya)
801232015

ABSTRACT

Cloud Computing offers services to end-users rather than a product, by sharing resources, software and other information under a pay per usage model, hence economic benefit is the key for Cloud in terms of capital and operational expenditure. It permits hosting of different types of applications such as business, scientific and social networking because it has key characteristics like multi-tenancy, scalability, performance and security etc.

Cloud Computing is currently facing challenges like Data Security, Energy Consumption, Server Consolidation, Virtual Machine Migration to name a few. Existing approaches of secure data transfer use two tier authentications, either based on OTP (One Time Password) which is static in nature and requires additional software/hardware or Digital Signature which leads to the problem of key management. This research work focuses on the study of secure data transfer by using different combination of mechanisms which not only ensure two tier authenticities without involving any above mentioned overheads but also maintain the confidentiality of data and integrity of message using one time key generation.

In this thesis, existing secure data transfer techniques have been compared. A mechanism has been proposed and simulated for secure data transfer. This mechanism ensures three way protections in term of authenticity, confidentiality and integrity based on the concept of single key. This technique uses OTP and HMAC with Diffie Hellman Key Exchange to enhance data security in terms of authenticity and integrity in Cloud Computing environment. In this mechanism Optimally Modified HMAC has been used to prevent the man-in-middle-attack. An encryption algorithm has been used to maintain the confidentiality of data in transmits. Flow of the execution stages has been described using Flow Diagram and Sequence Diagram while for simulated environment; MATLAB Toolkit has been used to validate the experimental results of HMAC.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1
Introduction

This chapter introduces Cloud computing, its evolution and various related technologies like distributed computing, grid computing, Cloud characteristics and the services offered by Cloud along with motivation of research and organization of thesis.

1.1 Cloud Computing Evolution

Idea of delivering computing resources using global network was fixed in the sixties by J.C.R. Licklider. This global network so called internet which came into existence in 1969 as a research project at Advanced Research Projects Agency (ARPA) on behalf of the Ministry of Defense, United State (MoD, US) was initially used for military and scientific purposes, its commercialization started since 1988 with services like e-mail and telnet. So internet is the backbone of all these services which are provided by Cloud Service Provider (CSP). Some experts also say that the concept of Cloud computing is the vision of American computer scientist John McCarthy of MIT (Massachusetts Institute of Technology) given in sixties, he stated that "computation can be delivered as a public utility" [1]. Throughout the life span of 60 years, usage of computers has been evolved spirally from centralized and sharable big size computers in 1970 to decentralize and small personal computers in 1999. Computing power has been distributed. In 2010s, again based on the concept of cost effective sharing, industries started to move to distributed center of compact machines for their computational needs. These centers were invisible to the end clients so called Cloud computing [2]. Cloud computing is based on internet computing that relies on the principal of sharing, with the Cloud computing idea of computing-as-a-service comes to true [3][4].

Cloud computing has evolved through various phases which involves Grid computing, Utility computing and Software as a Service (SaaS) as shown in Figure 1.1. Grid Computing can be defined as a collection of distributed computing resources with heterogeneous and non interactive workload from multiple sites

which are used collectively to reach a common aim but scope of grid computing is very limited mostly to scientific and research work [5]. Utility computing [6] involves the concept of metered services where accordingly of usage users have to pay, means commercialization of services (e.g. traditional electricity and telephonic services) which can be seen as a prediction made by Leonard Klienrock, one of the scientist of ARPA network, comes to true about the utilization of computer network which was in very beginning condition during his era of 1969 [7]. So the Grid and Utility Computing are the foundation stones of Cloud computing. Third phase of the Cloud computing evolution`s is "Software as a Service" (SaaS) which gains popularity in 2010, in which applications and data both reside on vendor`s site server, client who want to access the services connects himself with the remote server through internet like social networking. So SaaS offers fully furnished applications using technologies like Java, Ajax etc. SaaS is only a part of services which is provided by Cloud Services Providers [8]. Cloud computing is an umbrella term which in itself also covers Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

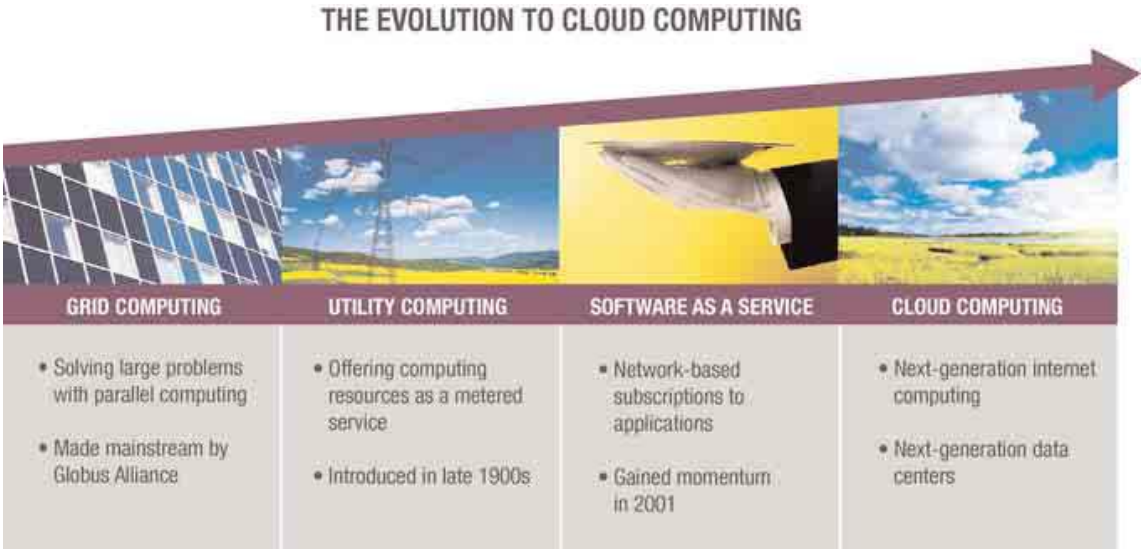

Figure 1.1: Evolution of Cloud computing [9]

Salesforce.com took first step in 1999 by putting the idea of Cloud computing in the market, which delivers its enterprise applications over internet using website.

Following that giant Cloud Service Provider Amazon came into existence in 2002 with its bunch of Cloud based services like computation and storage of big data with high level security [3][10]. Thereafter in 2006, Amazon provided its Elastic Compute Cloud (EC2) as a commercial web services which offered reconfigurable compute capacity in the Cloud. In 2009, Google started offers its Cloud based service like Google Apps which includes data storage, email at professional level, and many more shared services e.g. calendar and spread data sheet, which is seen as a big milestone in the field of Cloud computing. In February 2010, Microsoft launched Microsoft Azure which provided both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Microsoft Azure covers so many Cloud based services e.g. business analytics, data management, identity, access management and many more. Figure 1.2 shows different well known Cloud Services Providers worldwide.

Figure 1.2: Top Cloud computing Services Providers [11]

There is a lot of confusion about the exact definition of Cloud computing. According to research study that backs to 2008 there are minimum twenty two definitions of Cloud computing in common use [12]. Although many column writers and scientists on Cloud, e.g. Michael Brown, Gartner, Rajkumar Buyya, and organization like Open Cloud Manifesto have given their best to frame the proper definition of Cloud computing but because of different people different views, not a

single canonical definition could be framed. Finally in 2011, National Institute of Standards and Technology (NIST) has proposed a standard definition of Cloud computing which covers all the essential characteristics and models based on services and deployments. Table 1.1 shows the definitions given by many well-known scientists and organizations are:

Table 1.1: Definitions of Cloud computing

Author/Organization	Definition
Gartner	A way of computing through which IT related services are provided to multiple end users using internet [13].
Michael Brown	A data processing infrastructure in which the application software and often data reside on server`s side that is connected to the internet [14].
Rajkumar Buyya	Cloud is a parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreement established through ne gotiation between the service provider and consumers [15].
National Institute of Standards and Technology (NIST)	Cloud computing is a model for enabling 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. This Cloud model is composed of five essential characteristics, three service models, and four deployment models [16].
The Open Cloud Manifesto Consortium	Style of computing by which dynamically scale and provision computing resources in cost effective way so that user can make the most without manage the underlying complexity [17].

Figure 1.3 covers all aspects of NIST proposed Cloud computing definition.

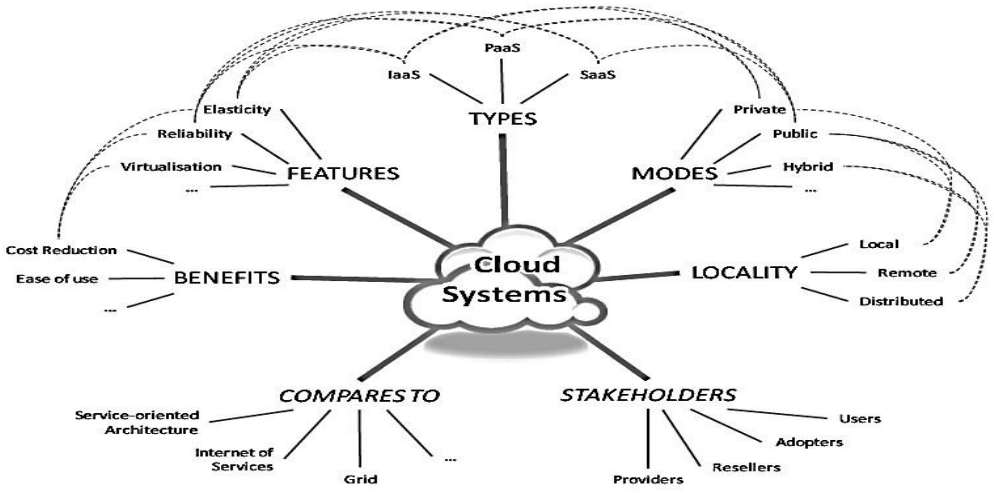

Figure 1.3: Non-Exhaustive View on the Main Aspects Forming a Cloud System [18]

1.1.1 Characteristics of Cloud Computing

The different characteristics of Cloud computing [19][20]21] are described below:

- Reduced Cost: Cloud offers pay per usage billing model. Startup companies or small business entrepreneurs who don't have enough man power, technical skills and can`t take risk by investing in infrastructure, easily start their business with no maintenance cost. Cloud users simply rent the infrastructure and technology according to their needs rather than buying it completely. Saved money can be used in other productive works to boost up the company`s output or productivity.
- Increased Storage: In the recent time, data is growing exponentially. To handle such a big data in itself is a major issue. Handling of big data covers so many aspects like storage, maintenance, security, and analyzing of big data. Cloud Services Providers offer vast storage for data since Cloud can scale dynamically within minute without decreasing performance.
- Flexibility: With Cloud, users can access their files and data from any location and devices e.g. phones, laptops, tablet via internet, called geographic flexibility. Since Cloud Services Providers store user`s data in one central location by which users can easily share their data and work in partnership with others people. Cloud users can buy the suitable storage for storing their files according to their need and eliminate storage capacity planning when no more requirement of it.
- Reliability: Cloud offers undisrupted services e.g. no data loss, no delay in services to the end users by using its redundant resources, extremely available, automatically replicated within its availability zones capability and server end or in transit data encryption.
- Location Independence: Users can access their data which resides on unknown server from any locations through internet services using any devices. Users are totally unaware about their data storage and underlying technical complexity of retrieving data. With these features, data and apps can be stored in optimal location for reducing the access time of data, providing fast recovery and highest security to the data.

1.1.2 Cloud Computing Services

Cloud computing is typically divided into three levels of service offerings [19] as shown in Figure 1.4.

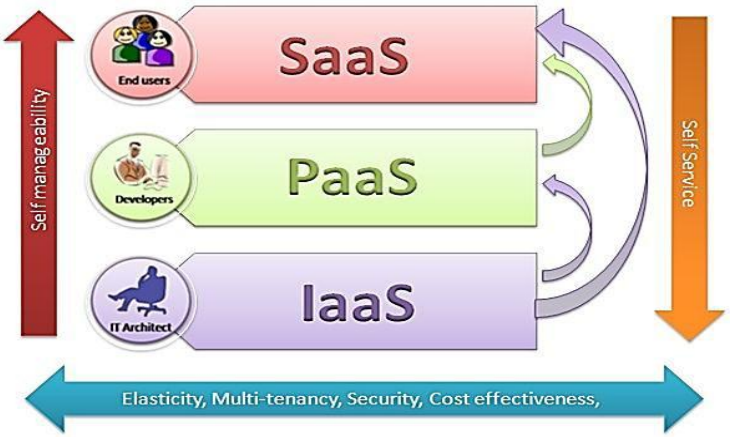

Figure 1.4: Services of Cloud computing [22]

- Software as a Service (SaaS)

Cloud users can access complete application or software remotely as a web service on demand using web browser through internet. Users need not to invest in software license or servers, while for Cloud Services Providers, maintenance costs are lowered because only specific application is hosted. Today Oracle, Salesforce, Microsoft, Google, Amazon have become the giant Cloud Services Providers which deliver Software as a Service business applications. Gmail is an example of Software as a Service.

- Platform as a Service (PaaS)

PaaS provides computational resources to the Cloud users through platform. With PaaS, users' gain a platform upon which they can easily create and manipulate applications. With PaaS, developers need not to buy underlying software and hardware; PaaS makes building, testing and delivering of web applications very easy, cost effective and quick. Using PaaS, vendors deal with storage, N/W, server, and operating system, etc but clients handle records and applications. Amazon's AWS Elastic Beanstalk and Google's App Engine are famous PaaS offerings.

- Infrastructure as a Service (IaaS)

The basic difference between PaaS and IaaS can be defined in term of degree of control

over system resources to the clients. In IaaS, Clients have almost full responsibility to manage the system. With IaaS, Clients decide what configuration of operating system, storage size, networking, type of server and security parameters etc they want. IaaS is suitable for those organizations which have already software packages with themselves and just want to put and run it in the Cloud. Amazon Elastic Compute Cloud (EC2) and Secure Storage Service (S3), Rackspace, GoGrid are the examples of IaaS offerings.

1.1.3 Deployment Models of Cloud Computing

Cloud services can be deployed in one of the following four ways shown in the Figure 1.5[23][24].

- Public Cloud

In Public Cloud, Cloud services and resources are publically available and shared by all users through internet based on pay per use billing model. This is the most common deployment model. Public Clouds consist large number of nodes to support millions of end users demands. The main benefits of using Public Cloud are its cost effectiveness and scalability. Because of its availability to all and resources sharing among the users make it vulnerable to security attacks. Google App Engine, Amazon Web Services (AWS) and Microsoft Azure are some famous Public Clouds.

- Private Cloud

Private Clouds are restricted only within the organizational premises to offer Cloud services to the specific authorized users only. Since it provides access only a limited number of people which makes it more secure from the external threats. Private Clouds provide good control over system resources (e.g. storage, networking and operating system, etc.), which makes it easily customizable. Amazon Virtual Private Clouds (Amazon VPC), VMware Private, Racspace Private and CloudBees are some famous private Cloud services providers.

- Community Cloud

In Community Cloud, different organizations with similar concerns or project (e.g.

joint business project or research) which require a central Cloud computing services work together to achieve common objectives. Community Cloud is a hybrid form of Private Cloud.

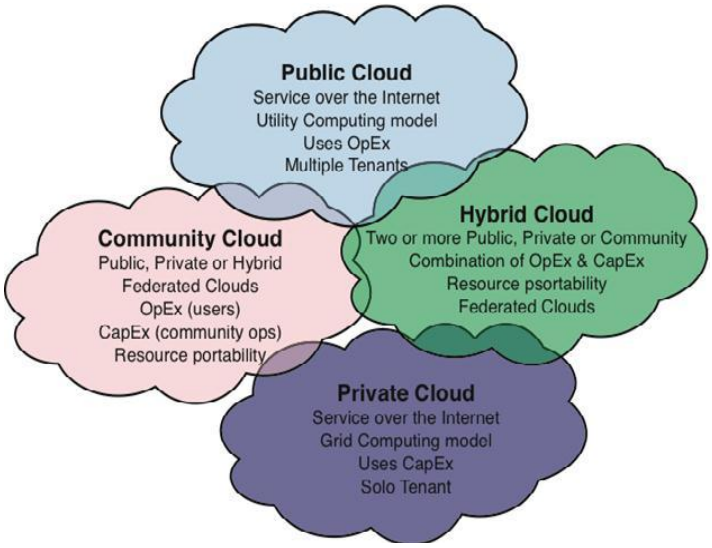

Figure 1.5: Cloud computing Models [24]

- Hybrid Cloud

Hybrid Cloud is a combination of any two of the above discussed three deployment model. With Hybrid Cloud, users enjoy the advantage of both Private Cloud`s security and Public Cloud`s scalability to carry out various functions within the same organization without exposing sensitive applications or data to the third party vulnerabilities. VMware`s Vcare and IBM etc. provide the services of Hybrid Cloud.

1.2 Research Issues in Cloud Computing

Cloud computing is an emerging field and has been widely used by the industry in many respects over the years. Some open challenges [25][26][27][28][29][30] in Cloud computing still need to be addressed carefully to make it more effective in order to fulfill the requirements of end users cost effectively, timely and securely.

- Automated Service Provisioning

In Cloud computing, Service providers must assign and release the resources automatically to meet the fluctuated end users demands efficiently in order to

minimize the operational cost and maximize the performance by achieving service level objectives using minimum resources. To make provisioning of services automated; Application Performance Model (APM) is used that predicts number of resources based on future demands. To make this prediction accurate different approaches are used like Resource Control Theory, Queuing Theory and Statistical Machine Learning. So for the researchers, this is still a challenge to make an effective Application Performance Model that considers all the parameters regarding automated service provisioning.

- Virtual Machine Migration

Virtualization means to create virtual form of something like operating system, server, network and storage devices in order to run multiple operating systems on a single machine, increase productivity using server consolidation, combine the independent resources by splitting the bandwidth of network and allocate them to different servers, pooling of different storages that appears as a single central storage which is also called Storage Area Network (SAN) respectively. Virtual Machine Migration means to move running virtual machines from one physical server to other in order to make Cloud system more fault tolerant and all time available to end users. Virtual Machine Migration is also used to balance the load across storage server. The main research issue is to migrate complete virtual machine with current state of memory from source server to destination server within few mille seconds transparently and securely.

- Server Consolidation

Server Consolidation means to reduce the servers to the appropriate number that are enough to handle the client`s request so that energy and cost can be saved. Server Consolidation is based on virtual machines live migration, So that all the virtual machines residing on underutilized servers are migrated to another appropriate server in order to keep former on energy saving state. In Server Consolidation, researchers need to explore several issues like typify the workloads (e.g. Homogeneous, Heterogeneous and Hybrid), servers (e.g. Innovative Server, Mission Critical Server and Productive Server etc).

- Energy Management

In recent years, Energy management has become a serious issue before the researchers to solve, with a good tradeoff between energy reduction and performance. Data centers with thousands of servers consume huge amount of energy to power and keep servers cool. Energy efficient hardware devices, server consolidation using virtual machines live migration, protocol that meet government`s term and conditions and energy aware job scheduling are some of the ways to make Cloud energy efficient and green.

- Fault tolerance

Fault in term of hardware or software must be tackle carefully without delaying to provide reliable service is a key issue in Cloud computing to be addressed. A survey conducted by Gibson and Schroeder [31] reveals that cloud suffers mainly because of hardware failures occur in hard-disk, memory and processor.

- Interoperability

Effectively shift applications using autonomous agent from one cloud to other in case of getting required performance or to handle provider's side transparency issues is a key challenge for cloud researchers.

- Data Security[32][33]

(i) Resource Location Issue: In Cloud computing, Cloud users store their data on unknown locations, possibly in other country, and because of this data is not only affected by Cloud Services Provider`s policies but also the laws of hosted countries. For example according to Dropbox`s conditions and terms, providers have the right to reveal the data in fulfillment of the government laws which is really dangerous situation. So European countries have made a law that Cloud`s data can`t move to that countries which don't provide a high level security.

(ii) Multi-Tenancy Issue: Protect user`s data from unauthorized users running processes on the same physical server.

(iii) Authentication: User`s data resides on Cloud provider's infrastructure, the data integrity may be violated by others without user`s awareness. The proper

authenticity of the user`s data in this scenario is very essential and hence needs to be assured.

(iv) System Monitoring and Logs: Monitoring Logs contain sensitive information which can`t be disclosed to the customers or third party either on request by provider. It really requires a service agreement between Cloud service providers and users.

(v) Cloud Standards: There should be a common standard across different Cloud vendors so that interoperability could become possible and this will also increase the scalability and security across Clouds.

Different organizations such as Cloud Security Alliances (CSA) and National Institute of Standard and Technology (NIST) try to provide best solutions and standards to tackle all these security related issues, a lot of research work is going on in the area of cloud security because security is the first serious concerns reported by Cloud users.

1.3 Research Motivation

Based on the IDC (International Data Corporation) survey report [34] security is the most important issue among Cloud users. Hence researchers need to tackle this issue carefully and ensure security at each level of Cloud. In 2013 Cloud Security Alliance (CSA) [35] mentioned Notorious Nine threats, in which data breaches by malicious insider is one of the core issue, which can be tackled using proper multi tier authentication and in-transit encryption.

In Software as a Service (SaaS), applications and data both reside on unknown remote server which is accessed through internet, hence is open to outsider attack. So it becomes necessary to maintain integrity and confidentiality of data from unauthorized users. In Data Security, authenticity and integrity is most important issue mentioned in survey of security in Cloud [33].

Various existing techniques manage the security of data by providing access only to authorize users using different combination of mechanisms in order to ensure authentication but either it is static in nature or provides simple credential

authentication. Aim of this thesis is to provide a robust security to the data in SaaS delivery model by using different combination of mechanisms in order to ensure multitier authentication using one time key generation, confidentiality using encryption and integrity of message over network using HMAC (Hashed Message Authentication Code).

1.4 Organization of Thesis

The rest of the thesis is organized as follows:

Chapter 2 – This chapter describes in detail the literature survey done to study the concept of secure data transfer in Cloud computing, concept of authentication, Existing approaches of securely data transfer in Cloud and data transfer architecture in Cloud.

Chapter 3 – This chapter describes the problem Analysis of the thesis work. It gives the gap analysis and problem statement.

Chapter 4 – This chapter describes in detail the solution of the problem with the help of layered architecture, execution steps, detailed data flow diagram (DFD) and sequence diagram.

Chapter 5 – This chapter focus on the implementation details and experimental results – description of MATLAB, snapshots of the proposed mechanism designed to study the technique.

Chapter 6 – This chapter describes the conclusion, contribution of the work done and future research directions.

Chapter 2
Literature Review

This chapter discusses the state of the art and research issues related to securities of data in Cloud, life cycle of data, existing approaches and comparison among them.

2.1 Existing Security Scenario Security in Cloud

Traditionally data was stored on users own premises so data owner need not to worry about the data, but now in the current era of Cloud computing where huge amount of data is stored in the unknown remote locations, several securities issues need to be addressed. Cloud computing is a way to enhance capabilities and capacity dynamically with minimal investment in terms of infrastructures, technologies and software licensing. Despite of so many advantages, customers are least willing to use Cloud incase of confidential data. The most important reason behind this is security. Based on the IDC (International Data Corporation) enterprise survey depicts in Figure 2.1, security is the main challenge followed by availability and performance.

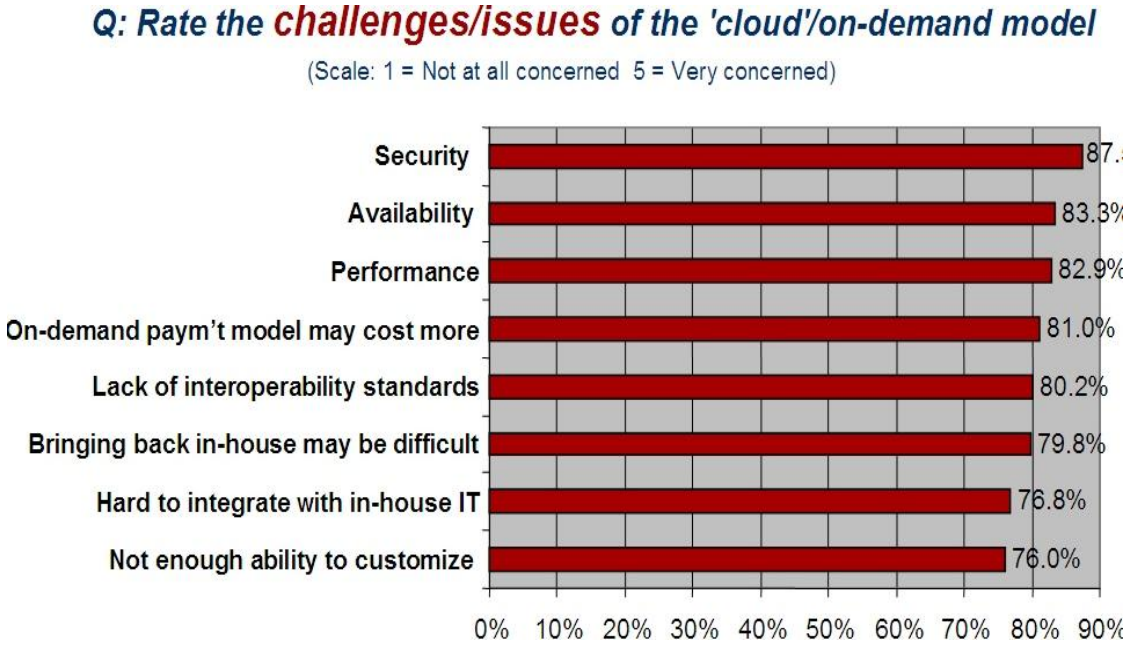

Figure 2.1: Ranking of Security in IDC Survey [34]

Security in itself is broad term which covers numerous aspects.

CSA (Cloud Security Alliance) has identified “notorious nine” computing threats for 2013 as follows [35]:

(i) First is Data Breaches, in which virtual machines on the same server can extract the valuable information from others using side channel attack but this attack, can be mitigated using encryption.

(ii) The second threat is Data Loss, attackers can delete or modify user data. Possible solution for this is to keep back up of data but it will increase the exposure of data to breaches.

(iii) Third security threat is service Traffic Hijacking in which if attackers gain access to user credentials he can easily monitor your activities, transaction and redirect the user to any sites. Possible solution for this is two step authentications.

(iv) Fourth threat in the list is insecure APIs (Application Program Interface) and interfaces.

(v) Denials of Service is fifth threat, availability and response time are major factors for the point of view of end users, if attackers are not possible to entirely shut down user application then they may create a cause which increases the processing time which is not tolerable. With virtualization single machine can be divided into many virtual machines which is a possible solution for denial of service.

(vi) Sixth security threat is Malicious Insiders; he may be employee, contractor or business partner.

(vii) Seventh on the list is Cloud Abuse, such as a bad guy using a Cloud service to break an encryption key too difficult to crack on a standard computer.

(viii) Eight on the list of top security threats to Cloud computing is Insufficient Due Diligence; that is, organizations embrace the Cloud without fully understanding the Cloud environment and associated risks and hence users don`t fully utilize the Cloud resources .

(ix) Shared Technology vulnerabilities are the last but not least security threat

mentioned by CSA. Cloud service providers use shared infrastructure in terms of CPU (Central Processing Unit) caches and memory that were not designed to offer strong isolation.

Hence as the IDC survey reveals that security is a major concern for Cloud with 87% votes, and in the specific field of security, data security in terms of data breach and loss are top two points which need to be addressed carefully.

2.2 Authentication in Cloud

Authentication is a process which decides the legitimate users by verifying the details provided by the end users. In most applications, one tier traditional credential authentication (e.g. user name and password) is used but it is not safe enough in the case of Cloud. It is very necessary to provide strong authentication for executing important transactions over internet. Authentication is the first phase depicted in the Figure 2.1 which needs to be passed by the users to gain access over resources there after proper authorization, data is transmitted over network securely. Physical threat is not addressed in this thesis.

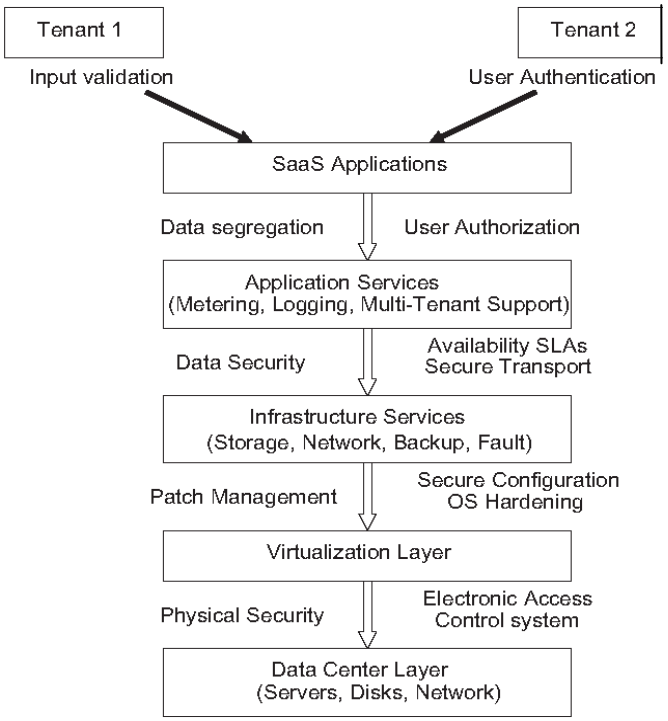

Figure 2.2: Security for SaaS Stack [36]

To improve the security, multi tier or multi factor authentications should be used in the Cloud [37]. Multi factor authentications depends upon the principal of something we know already e.g. stored password and something recently provided by the Cloud side automated server to us e.g. secret code to registered devices.

Various factors defined by NIST which should be incorporated by authentication system [37] are:

- Something user knows: Shared secrets are the information, users share with the trusted Cloud services provider. Since it may be a password which is stored in the memory so it is called as something that is known rather than something one has. This method covers only single level of authentication which is weakest form because password is entered using keyboard in the system hence vulnerable to keyboard logging or shoulder surfing attacks.
- Something user has: Registered device or something which users have with themselves at the time of authentication e.g. mobile or keys.
- Something user is: Personal attributes which uniquely belong to the user only. E.g. voice or finger prints, retina-iris scanning, facial expression, thumb prints, DNA and many things.

A strong authentication system must incorporate all three factors to resist the attacks mentioned below:

- Man-in-the-middle: In this attack, malicious attacker situated himself in between client and verifier to intercept and alter the data flows between them.
- Verifier impersonation attack: An attack where the attacker impersonates the verifier in an authentication protocol, usually to learn a password.
- Password guessing attacks: Here attacker usually guesses the password in repeated login trials.
- Replay attack: Here an attacker records and rerun some portion of a last one good protocol run to the verifier.
- Eavesdropping: Here attacker illegally listen or intercept the private communication, such as phone call, fax transmission.

- Session hijacking: Session hijacking occurs when a session token is sent to a client browser from the Web server following the successful authentication of a client logon by guessing the session token.

Authentication in Cloud is provided by various ways e.g. SMS OTP (one time password), Telephony OTP, E-mail OTP, Static PIN, Pluggable USB, User`s known password, KBA (Knowledge Based Answers/Questions), Digital certificate, Federated IDs (A token is issued in trusted languages like SAML- Security Assertion Markup Language) that validates the user`s identity.

2.3 Hybrid Approaches of Security in Cloud Computing

A single technique can`t provide security in depth in Cloud, it really requires a strong authentication, confidentiality in transit and data integrity. Various approaches have been discussed below which provide different tier of authenticity in order to ensure security.

- Sulochana and Parimelazhagan [38] have described a puzzle based authentication scheme in Cloud computing in which user first registers and solves the puzzle, puzzle solving pattern and time is stored and validated by local server and if user get authenticated, start accessing the Cloud services. Although this scheme ensures 2 tier authentications but static in nature, if attacker once identified the stored pattern, he could easily break the security.
- Yogita et al. [39] have described that not a single technique is enough to provide security in Cloud, she has used Diffie Hellman with digital signature for providing 2 tier authentication. But digital signature uses so many parameter that`s why it is heavy enough and also requires a proper key management.
- Arasu et al. [40] have given a approach of Hash Message Authentication Code (HMAC) in which key, message and hash function is concatenated together for ensuring authentication. This approach describes only single tier authentication which is weak in case of Cloud computing.
- Neha and Ganesan [41] have used Diffie Hellman Key Exchange mechanism for connection establishment and Elliptic curve cryptography for data encryption. In this paper authors used a traditional one tier authentication which is vulnerable to

security attacks.

- Govind et al. [42] have provided security using digital certificate authentication method. Here author uses RSA Algorithm for encryption/decryption which is followed by the process of digital certification. This method ensures only single tier authentication using Digital certification which raised a problem of key management.
- Maninder and Sarbjeet [43] have provided an advance multi tier authentication scheme for enhancing security in financial transactions, in which in first tier, user has to simply pass the traditional login authentication and in second tier a fake screen will appear before user from local server, which is filled by the user by predefined stored pattern, if it is correct then only server will allow access to the resources. Problem with this approach is that it is static in nature, once user identifies or observes the pattern of fake screen from behind, he can easily break this authentication.
- Satish and Anita [44] have proposed a method of fake screen for ensuring two tier authentication in Cloud computing. In this method of authentication, first user registered himself with Cloud server, and then registered his device. So secret code has been sent to the registered devices which ensure second level of authentication. This method involves additional hardware which is costly and must be along with you every time when you are going to login in the system.
- Parsi and Sudha [45] have proposed method that use RSA algorithm for authentication and data transfer securely. This method involves a phase of key generation, encryption and decryption.
- Timm et al. [46] from Fermi Private Cloud have used a method of X.509 digital certificate for authentication purpose, which is used by many open source Cloud services provider like Eucalyptus and Nimbus. Digital certificate requires both public key and private key for authentication, hence key management is serious issue which needs to be tackled. Apart from this problem, digital certificate requires many others parameters as a purpose of authentication which really makes it heavy enough. Various hybrid approaches of security in Cloud which have been discussed above summarized in a table 2.1. Which covers the proposed method with given

year, authentication tier and flaws.

Table 2.1: Comparison of Hybrid Approaches of Security in Cloud

Sr. no.	Technique (Year)	Security Technique	Tier	Flaws
1	A Puzzle Based Authentication Scheme for Cloud computing(2013)	Solve puzzle for authentication	2	Static in nature, once stored puzzled is identified then
2	Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption algorithm to Enhance Data Security in Cloud computing(2013)	Ensure security using Diffie Hellman + Digital Signature	2	Key management is a problem
3	Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm(2013)	Ensure authentication and privacy using HMAC.	1	Weak authentication process
4	Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography(2012)	Ensure Security using Diffie Hellman+ECC	1	One way traditional Authentication
5	Third party auditing for secure data storage in Cloud through digital signature using RSA(2012)	In this Third party is used to store the encrypted data using private and public key in RSA algorithm, Digital signature for authentication	1	Costly because of third party involvement, one way authentication
6	Design and Implementation of Multi-tier Authentication Scheme in Cloud(2012)	Ensure authentication using traditional login and fake screen examination	2	Static in nature, once attackers detect the pattern of fake screen, security may be easily broken.
7	Multi Authentication for Cloud Security – A Framework(2014)	Ensure two tier authentication using registered devices	2	Require additional hardware
8	Data Security in Cloud computing using RSA Algorithm(2012)	Ensure one tier authentication using RSA cryptography	1	Data integrity not assured
9	Authentication, Authorization, and Contextualization in Fermi Cloud(2010)	Authentication based on x.509 digital certificate	1	Certificate expiration problem, key management problem
10	A Physiological Authentication Scheme in Secure Healthcare Sensor Networks(2010)	A novel two-tier authentication approach based on physiology, RSA digital signature	2	Key management is a problem, costly because usage of additional hardware devices

2.4 Data Transfer Architecture in Cloud computing:

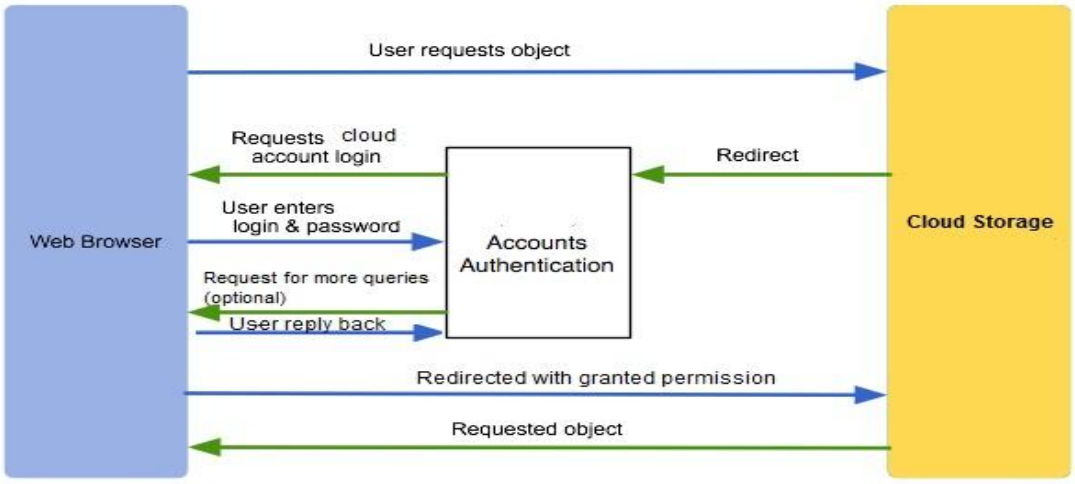

Figure 2.3: Data transfer after Authentication in Cloud

User requests to the Cloud services using web browser, so first he will redirect automatically to account authentication server. Account authentication server first requests to the user about his stored authentication details, these details may be anything e.g. credential login/password supported by Nebula open source Cloud, Digital Certificate X.509 supported by Eucalyptus and Nimbus open sources Cloud. After first step of verification, if server supports for multi factor authentication, it will continue to ask queries by sending some pin or password to registered device that will be re-entered by the user, if given information is correct he will be redirected to the Cloud storage with generated cookies. Now data transfer takes place between end user and Cloud storage securely using proper encryption method for providing confidentiality.

2.5 Conclusion

Various approaches of secure data transfer has been analyzed that focus mainly on authentication parameter. These approaches have been categorized on single and multi tier authentication. This authentication may be using digital certificate, HMAC or OTP on registered devices.

Chapter 3
Problem Analysis

Previous chapter analyzed various techniques for solving the issues related to data security in Cloud. This chapter focuses on the gaps in literature review.

3.1 Gap Analysis

Cloud provides "data storage" as a service, secure and fast transmission of data from Cloud storage is a major challenge. Data in transit is open to be attacked by middle man. Deyan Chen and Hong Zhao [47] have mentioned in their survey that Cloud services are dependent on internet, particular method is not enough to handle all data security issues like confidentiality, authenticity and integrity, for these different integrated techniques and mechanisms should be used. Many researchers [39] found it useful to use a perfect blend of different techniques to ensure the safety of data on Cloud.

Based on the literature survey there are various techniques (as shown in Table 3.1), which manage these security issues (e.g. integrity, authenticity, confidentiality) but these are not efficient because for authentication either they rely on digital signature which requires both private and public key, so key management is an issue or rely on OTP for strong authentication which requires additional hardware which is costly.

Table 3.1: Different Data Security Techniques for Cloud

Technique (Year)	Security Technique	Tier	Issues
Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption algorithm to Enhance Data Security in Cloud computing(2013)	Ensure security using Diffie Hellman + Digital Signature	2	Key management is an issue
Authentication, Authorization, and Contextualization in Fermi Cloud(2010)	Authentication based on x.509 digital certificate	1	Certificate expiration problem, key management problem

Multi Authentication for Cloud Security – A Framework(2014)	Ensure two tier authentication using registered devices	2	Require additional hardware
Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography(2012)	Ensure Security using Diffie Hellman+ECC	1	One way traditional Authentication
A Physiological Authentication Scheme in Secure Healthcare Sensor Networks(2010)	A novel two-tier authentication approach based on physiology, RSA digital signature	2	Key management is a problem, costly because usage of additional hardware devices

3.2 Problem Statement

Security can be enhanced using strong authentication. Authentication on which Cloud computing heavily depends for security, provides the facility of using different mechanism for ensuring authentication e.g. Digital Signature and OTP.

The problem is to determine what kind of approaches should be used to a single server that will provide the most efficient authentication, confidentiality and integrity using perfect blend of different mechanisms. In current approaches of authentication key management is an issue, or either they rely on additional hardware for their OTP.

The aim of this thesis work is to provide a mechanism which ensures three way protections in term of authenticity using OTP concept, confidentiality using encryption/decryption, and integrity using HMAC for secure data transfer over network. One time shared secret key has been used for this complete scenario.

3.3 Objectives

(i) To study the existing approaches of secure data transfer over network in Cloud using proper authentication.

(ii) To develop an algorithm which securely transfers data over network and provides three way protection in terms of authenticity, integrity and confidentiality.

(iii) To verify and validate the proposed techniques.

3.4 Conclusion

Problem has been formulated based on Gap Analysis which addresses the issue of key management in digital signature authentication, additional hardware/software requirement for multi-tier authentication and integrity and confidentiality of messages in transmits.

Chapter 4

Proposed Method

This chapter discusses about how the problem stated in previous chapter can be solved with the help of layered diagram, data flow diagram and sequence diagrams.

4.1 Design of Solution

The solution to the problem (secure data transmission in Cloud) has been depicted through architecture of the proposed technique and Data Flow Diagram. Following section presents the design of the solution using architecture and data flow diagram and sequence diagram of the proposed technique.

4.1.1 Architecture of Proposed Technique

In the proposed architecture shown in fig Figure 4.1, Multi factor authentication through OTP (One Time Password) and message integrity through HMAC (Hashed Message Authentication Code) have been ensured using Diffie Hellman key exchange algorithm. Once shared secret key is generated in between Cloud Storage Server and Cloud user, it is used throughout the session for reducing the total time. But using single key is vulnerable to man in middle attack hence we have proposed the concept of OTP just after login process but before HMAC formation. OTP will be generated automatically by authentication server after adding current login number to shared secret key. Once user passes the two tier of authentication then he replies back to the server with the operation (e.g. Uploading/ Downloading) what he wants to perform using HMAC. HMAC ensures message integrity and prevents non repudiation attack because HMAC is formed using same shared secret key, hence no one can change the source of message until he knows the shared secret key of both parties. This message is decrypted by the server thereafter secure network link has been opened in between user and Cloud storage so user can upload or download file from Cloud storage in encrypted form during transmission which ensures confidentiality as well. This method requires no additional software/

hardware for authentication, no need to worry about the key management because each time new key is generated for each operation which results in more security with less space required and fast in execution because single key is used throughout the session.

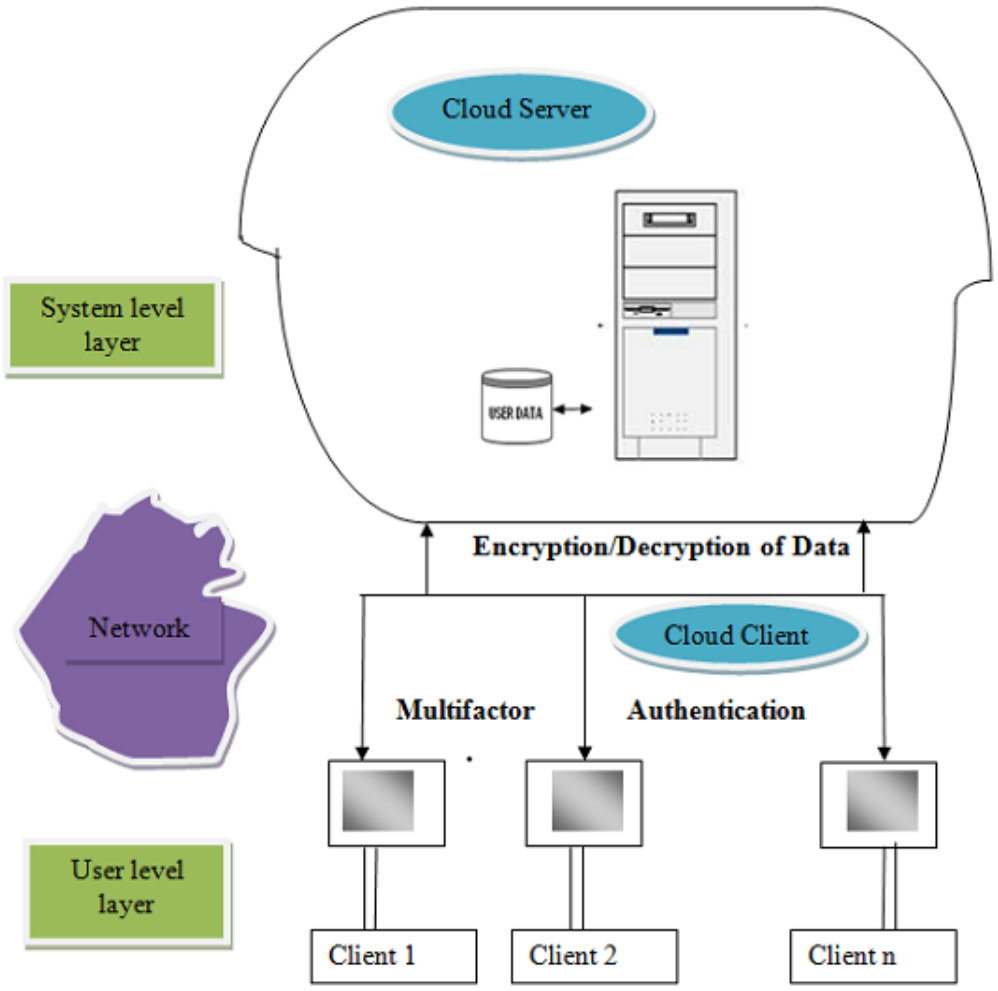

Figure 4.1: Proposed Architecture

Below are the different execution steps of proposed technique that enhance the security of data in Cloud by combining different mechanisms.

4.1.2 Execution Stages

- Assumptions:

  (i) Users are already registered to the Cloud.

(ii) Server is intelligent enough to decrypt the HMAC using the same client side coding and maintain the login number of each user.

1. Login
   1.1 Credential authentication using username/password
   1.2 Diffie Hellman key exchange
2. Double authentication using OTP (Shared Secret Key+ Current Login Number) generation
3. HMAC (Shared Secret Key || Operation || Method)
4. Downloading/ Uploading Data Encryption
5. Data is retrieved and stored to Cloud Storage
6. Logout

4.1.3 Detailed Execution Stages

Stage 1. Login: First credential login will take place between Cloud user and server using stored user name and password. This is the first tier of authentication. After successful login user will choose the random numbers and prime numbers to generate the shared secret key using Diffie Hellman algorithm.

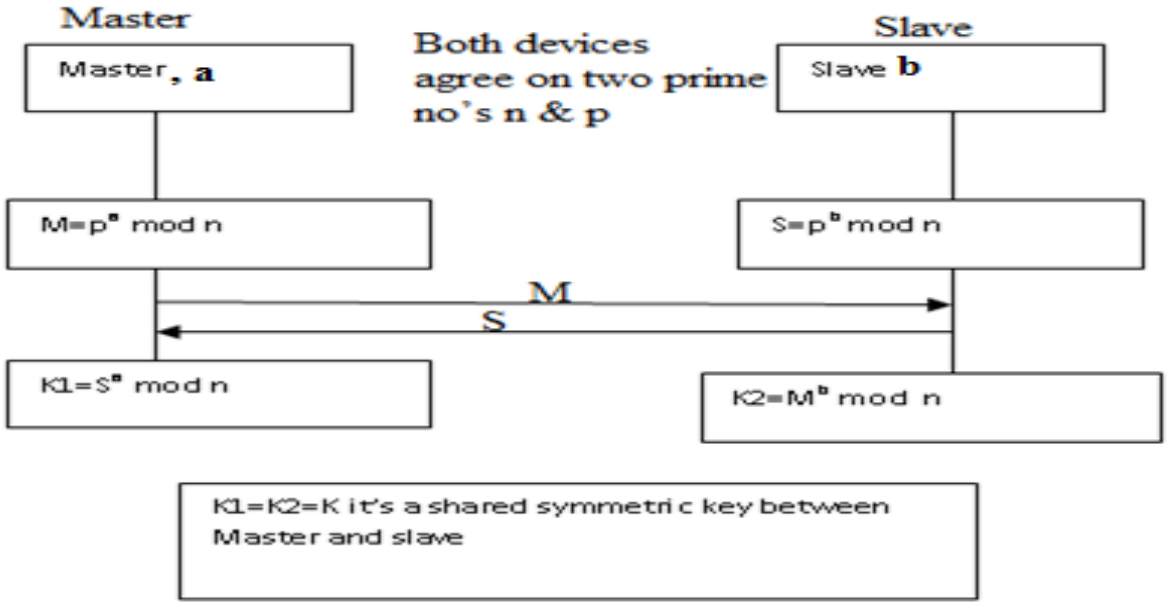

Figure 4.2: Shared Secret Key Generation using Diffie Hellman

Stage 2. OTP: Server will dynamically calculate the OTP by adding the current login number of particular user to the shared secret key which has been generated in first step; it will be asked by the user as a double authentication. This is the responsibility of server to maintain the login number of each user. Suppose generated shared secret key is K and current login number is N then OTP will be K+N.

Stage 3. HMAC: HMAC (Hashed Message Authentication Code) is used to provide message integrity so that intruder can`t alter the operation in transit. This will be used by Cloud user to generate a value by combining the same shared secret key along with operation (upload/download) and method (SHA256). In this mechanism final HMAC value has been calculated by X-ORing the HMAC of original key in binary form of 64 bits with HMAC of original key in reverse binary form of the same length. In this thesis this process of HMAC formation has been optimized by executing it in parallel.

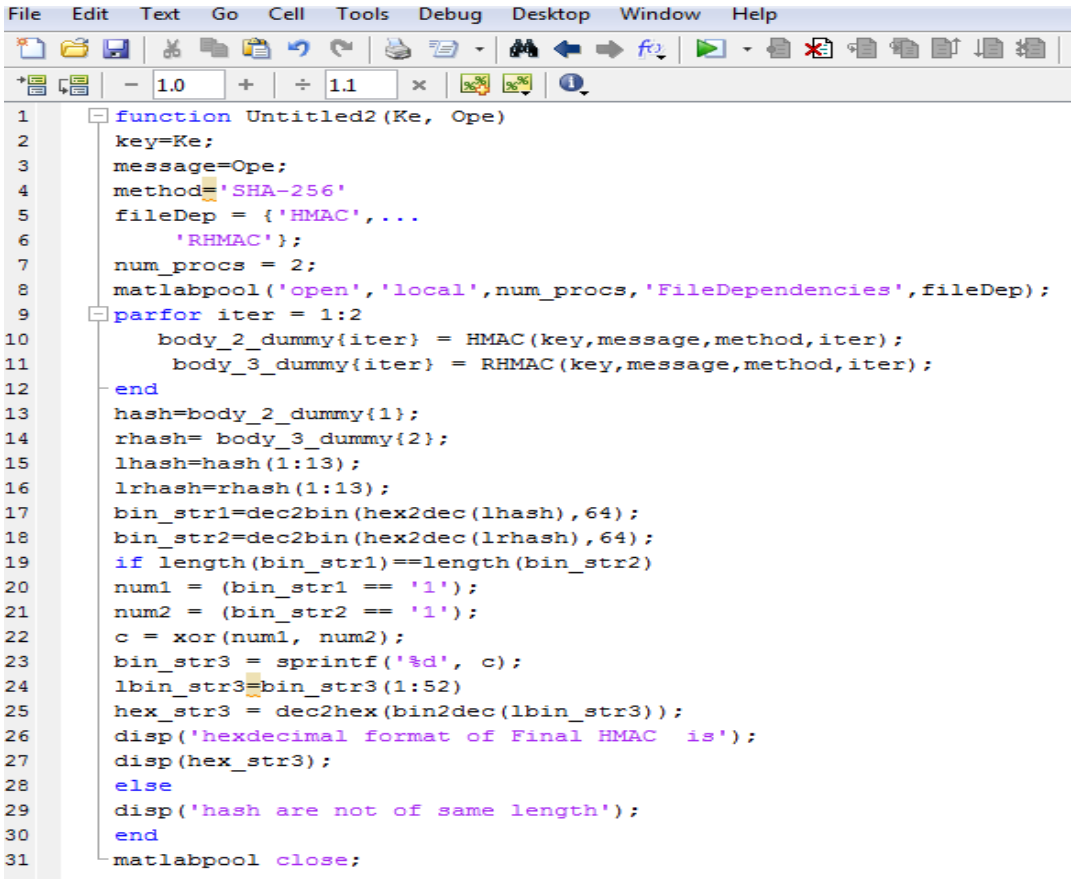

Figure 4.3: Parallel Algorithm of Modified HMAC

Stage 4. Using Advance Encryption Scheme data is transferred between Cloud User and Cloud Storage in encrypted form to make it confidential from unwanted persons.

Stage 5. Data is then stored and retrieved from Cloud.

Stage 6. Finally connection is disabled between Cloud`s client and Cloud.

4.1.4 Data Flow Diagram

Data Flow Diagram of Secure data transfer using two way authentications (via Credential and OTP) has been designed for thesis in Figure 4.4, which shows the Detailed level DFD of the proposed method with two entities Cloud User (registered) and Cloud Servers(e.g. Authentication Server, Storage Server etc).

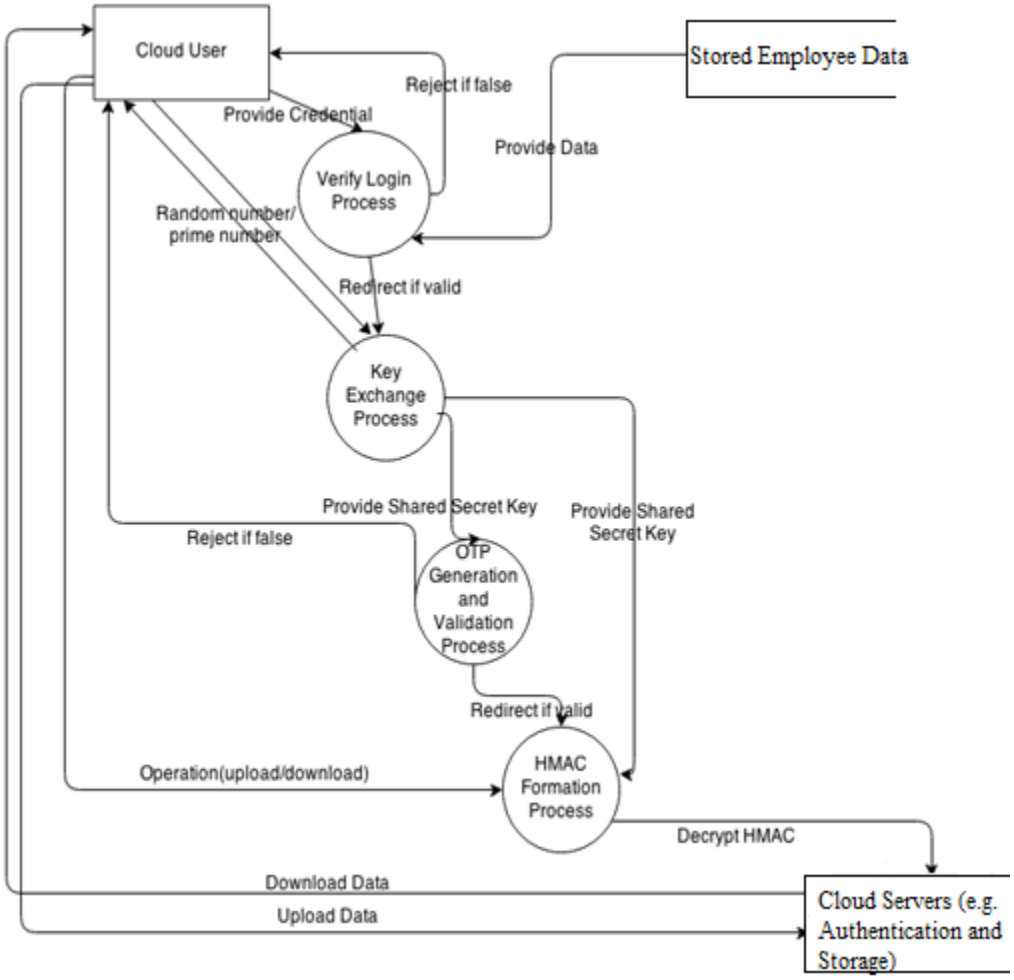

Figure 4.4: Data Flow Diagram of Proposed Method

4.1.5 Sequence Diagram

Figure 4.5 shows the sequence diagram for secure data transfer on Cloud via two way authentication between Cloud User and Cloud Server. It shows the interaction between Cloud user and Servers that how user passes two tier authentications then download/upload data from Cloud storage.

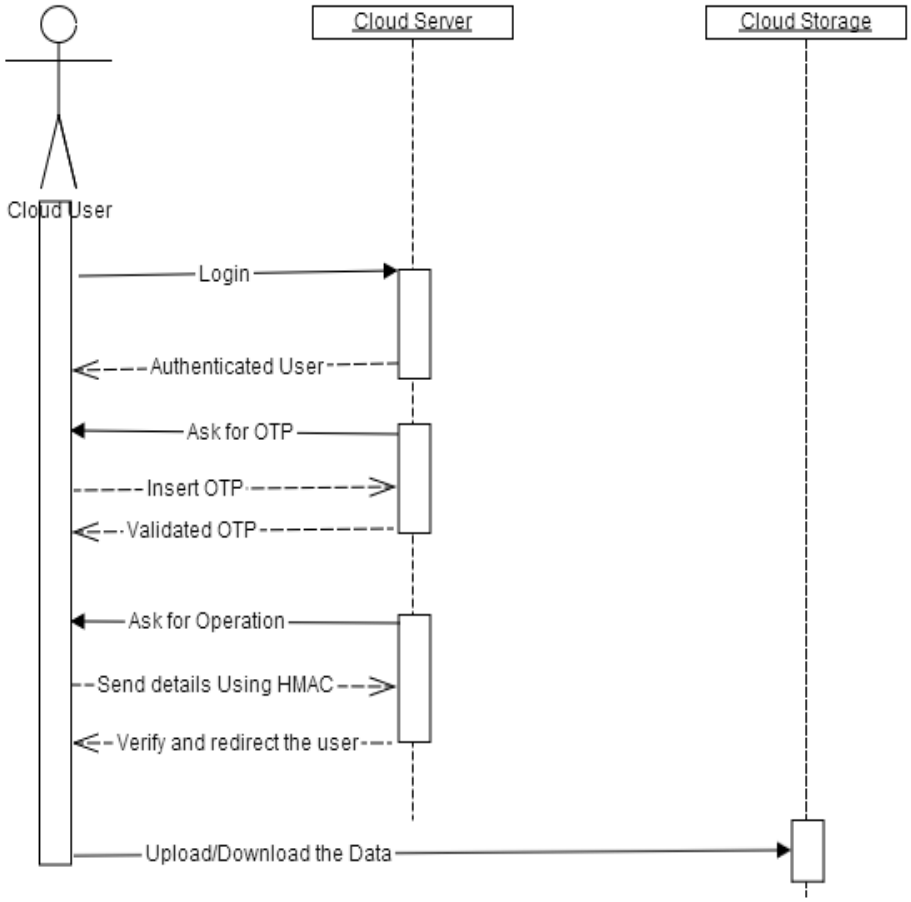

Figure 4.5`: Sequence Diagram of Proposed Method

4.2 Conclusion

Proposed mechanism of secure data transfer has been depicted using Data Flow Diagrams and Sequence Diagram while parallel algorithm of Modified HMAC has been scripted using Matlab tool.

Chapter 5
Experimental Results and Analysis

This chapter focuses on tools for showing the flow of execution, implementation of securely data transfer mechanism on MATLAB and experimental results of HMAC formation.

5.1 Tools for Setting up Simulation Environment

Cloud applications have different composition, configuration and deployment requirements. Various tools required to show the simulation of secure data transfer technique which ensure proper authentication, integrity via HMAC on Cloud is described below.

- MATLAB

MATLAB is an interpreted language and environment for numerical calculation. It allows programmers to execute numerical computations, and visualize the outcome without any need of difficult and time unbearable programming. MATLAB permits its users to accurately solve problems, generate graph with no trouble and produce code efficiently. It is developed by MathWorks. It is written in c, c++ and java. You can speed up your MATLAB programs or Simulink models by running them in a high-performance computing environment, such as those now offered by Amazon EC2 and other Cloud computing services. MATLAB offers the following novel features [48]:

- Parallel Computing Toolbox provides the ability to run MATLAB workers locally on your multicore desktop to execute your parallel applications allowing a user to fully use the computational power of desktop. Using the toolbox in conjunction with MATLAB Distributed Computing Server, one can run own applications on large scale computing resources such as computer clusters or grid and Cloud computing resources.
- Support for simulation of network connections among the simulated system elements.

- MATLAB is simple, portable, scalable and easily integrated into organization`s structure.
- Typical Technical Computing User Tasks Performed by MATLAB

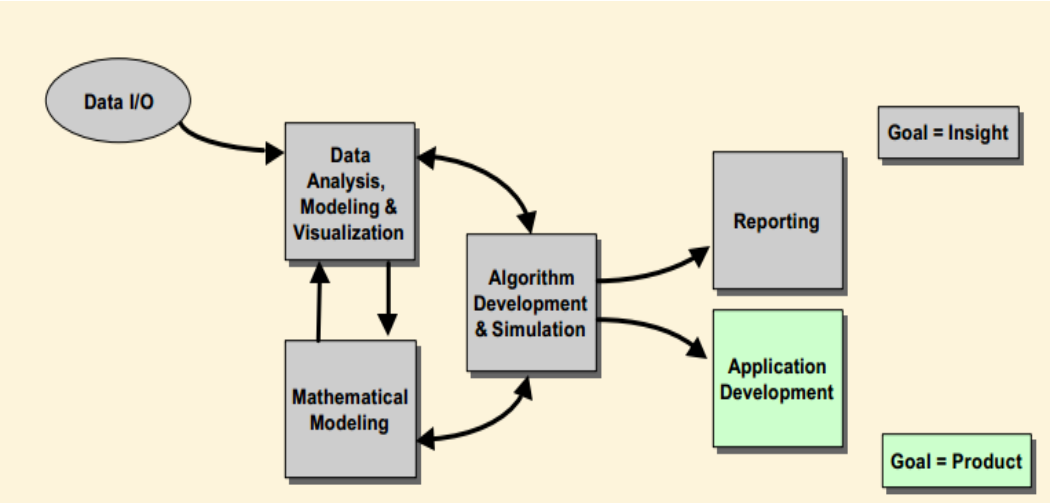

Figure 5.1: Computing User Tasks Performed by MATLAB [49]

MATLAB analyzes the data and performs 3D visualization. It supports tool boxes and block sets for performing various mathematical computations and modeling. Programmers can write algorithms in MATLAB language and simulate the result using SIMULINK.

5.2 Implementation of the Proposed Technique

Mechanism of secure data transfer on Cloud via two tier authentication has been simulated using MATLAB tool, network deployment is shown as snapshots in Figure 5.2.

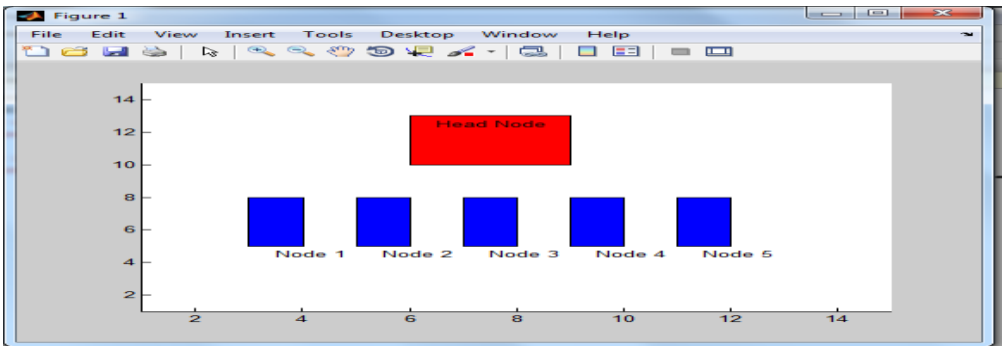

Figure 5.2: Network Deployments Diagram

This is the network deployment diagram of simulation in which client nodes upload and download data from cloud server storage.

User 1 wants to perform operation (e.g. upload and download) on Cloud.

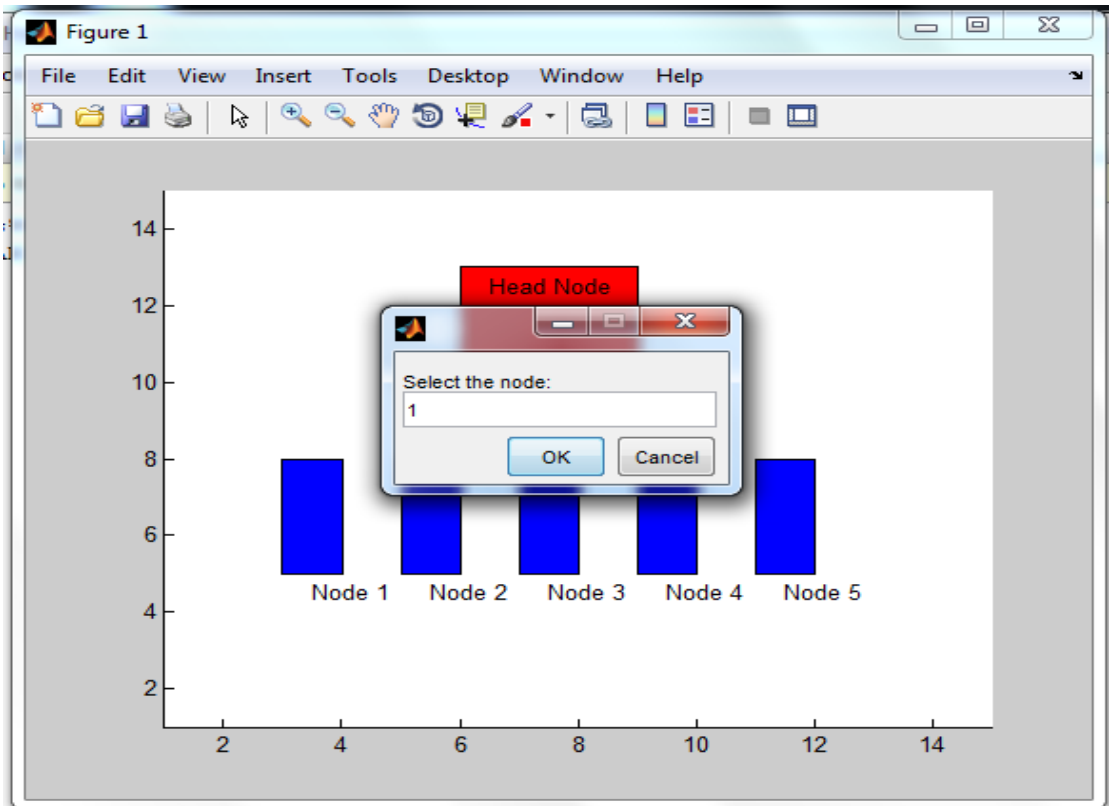

Figure 5.3: Selection of Node

Now first user1 will have to pass credential login authentication by entering the correct number of head node and sub node.

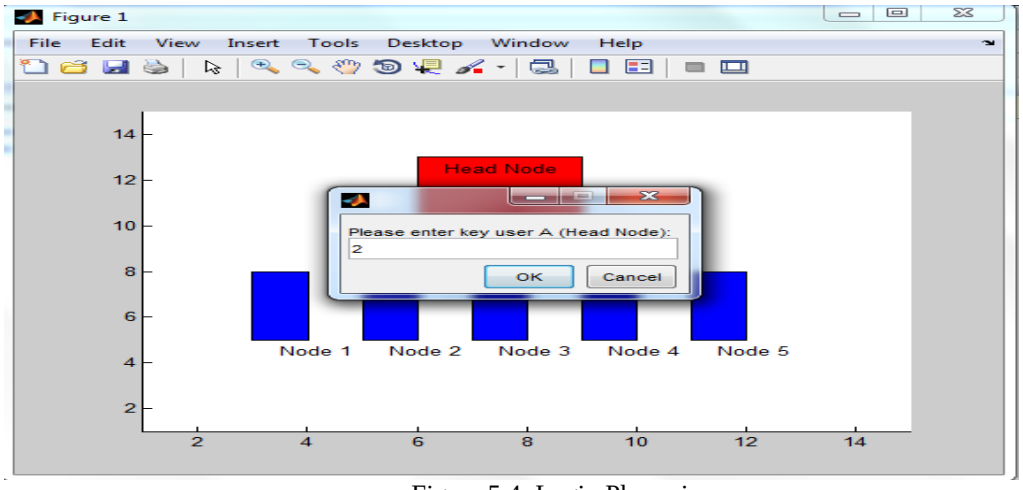

Figure 5.4: Login Phase i

User A which represents head or Cloud node has entered 2 which will be checked against client`s entered number.

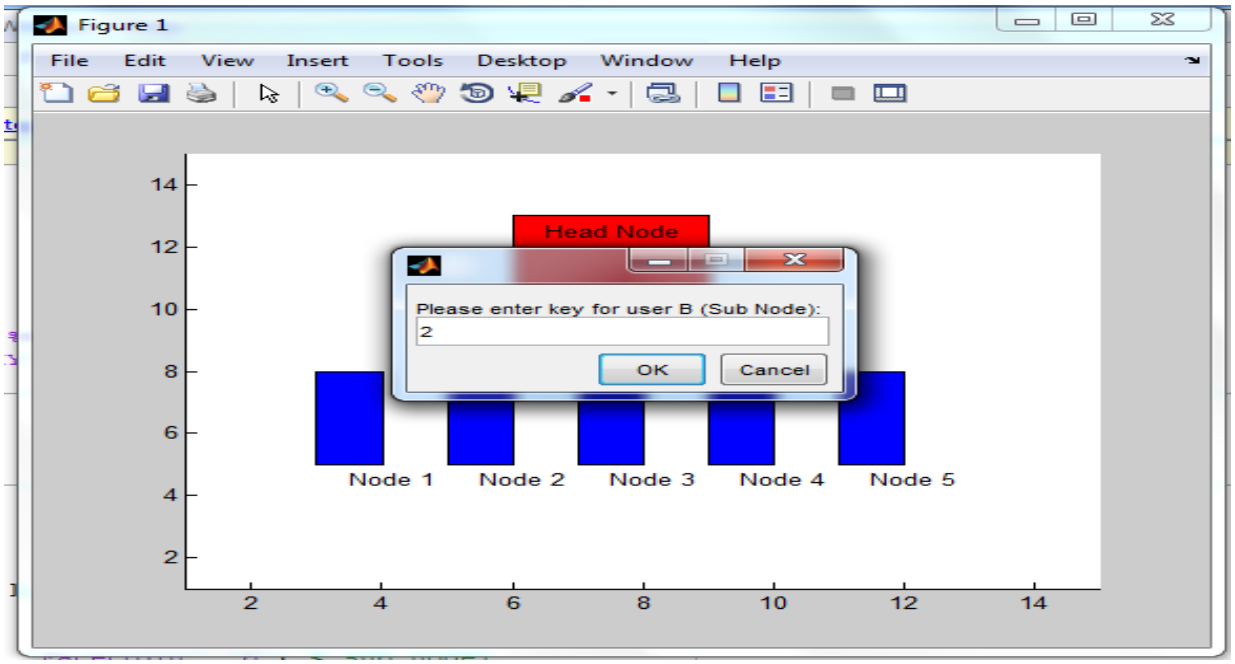

Figure 5.5: Login Phase ii

Now connection has been established in between user node and head node or Cloud node.

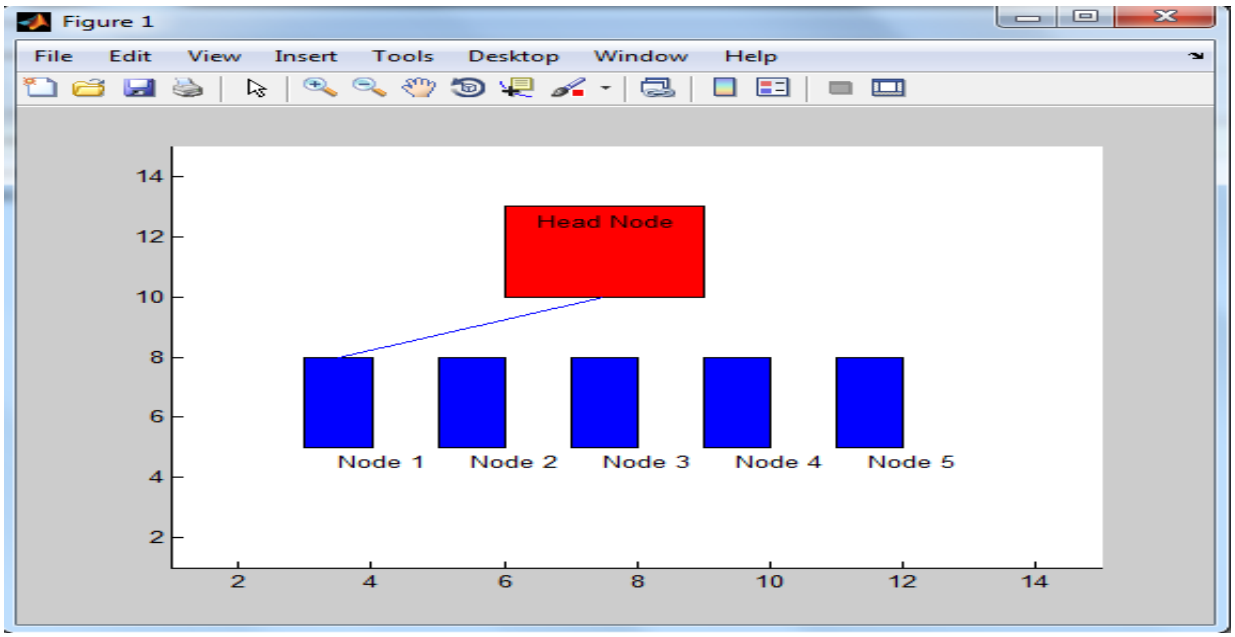

Figure 5.6: Login Successful and Connection Establishment

Now first shared secret key will be exchanged between user and Cloud server.

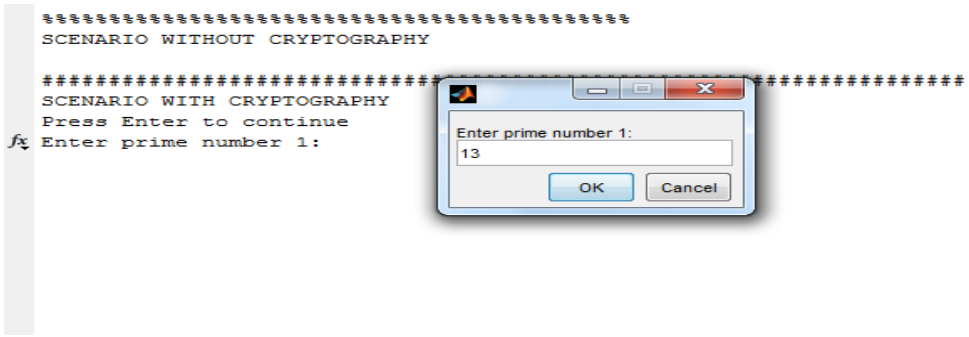

Figure 5.7: Diffie Hellman Key Exchange Phase i

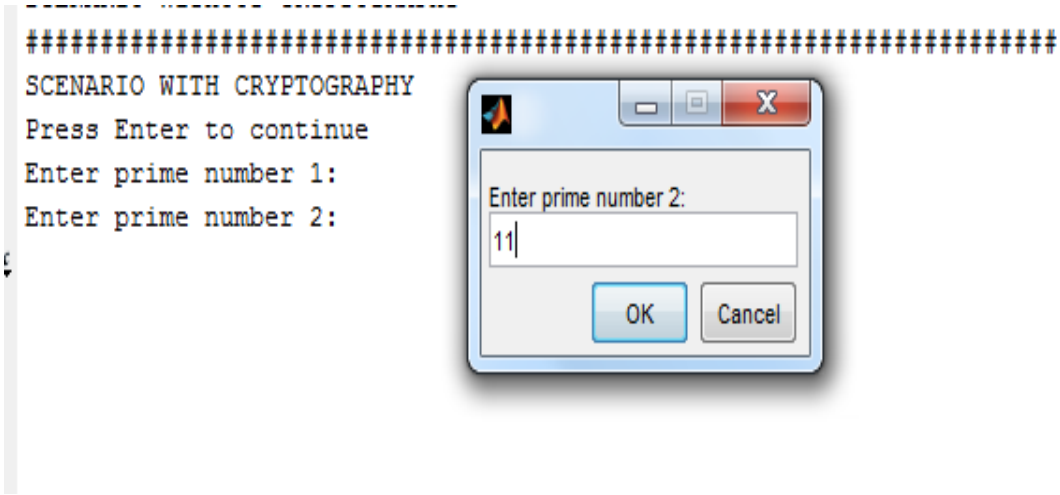

Figure 5.8: Diffie Hellman KeyExchange Phase ii

Figure 5.7 and 5.8 shows that Server and Client enter the prime number that is pre requisite for the generation of shared secret key. Now server or master chooses his random number.

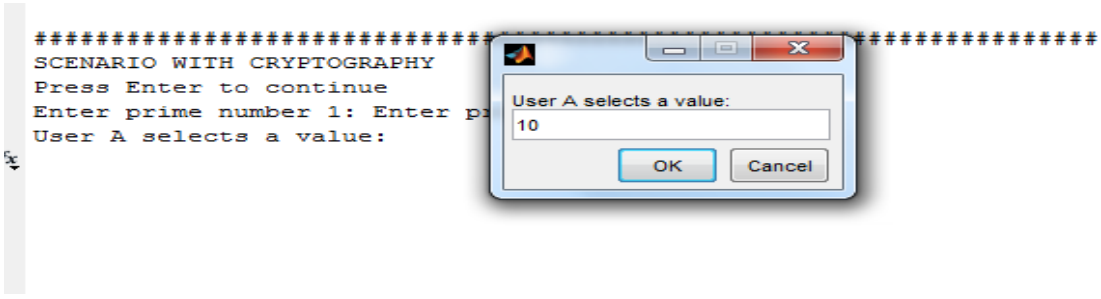

Figure 5.9: Diffie hellman Key Exchange Phase iii

user chooses his own private number

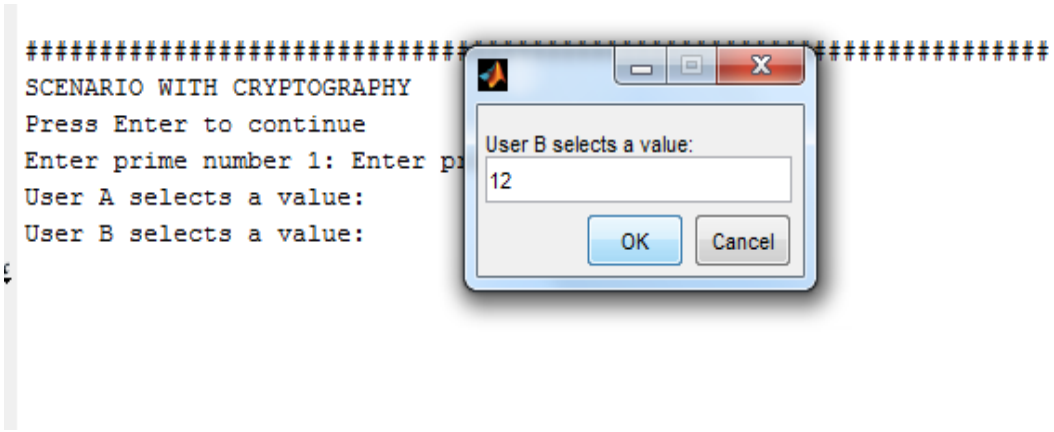

Figure 5.10: Diffie Hellman Key Exchange Phase iv

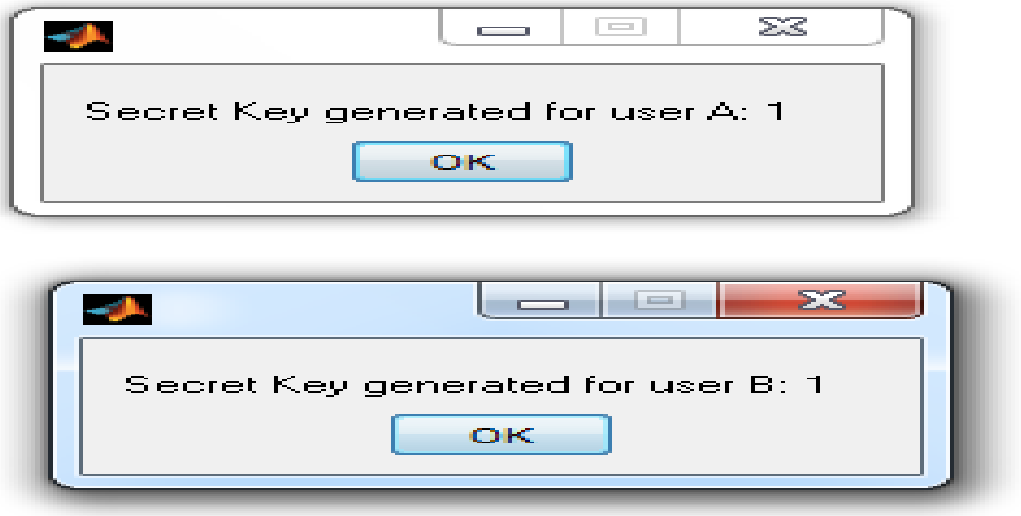

Figure 5.11: Shared Secret Key Generation

Shared Secret Key in between server and client is 1. Based on this Secret Key, OTP is generated. Login number of each user is maintained by the server, so OTP is a summation of current login number and currently generated Shared Secret Key.

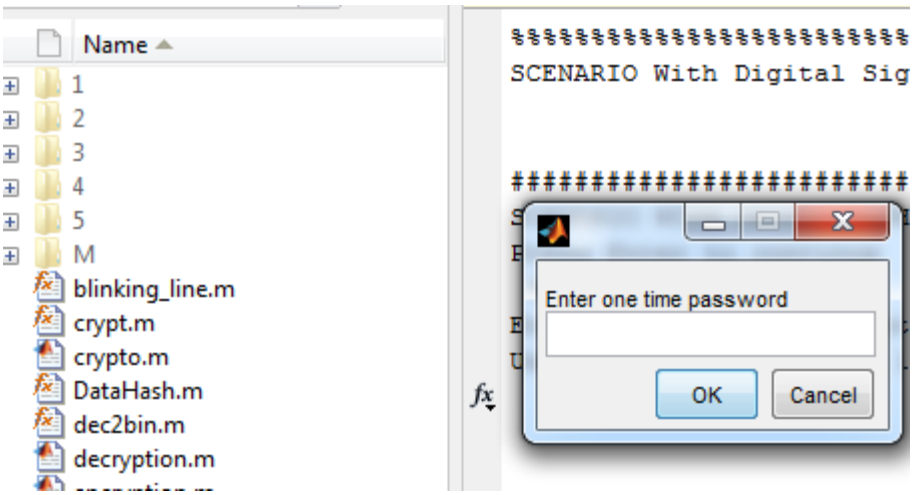

Figure 5.12: OTP Generation

Enter one time password if this is equal Current Login Number + Secret Key (1+1=2) then it will generate HMAC and file will be transferred in encrypted form.

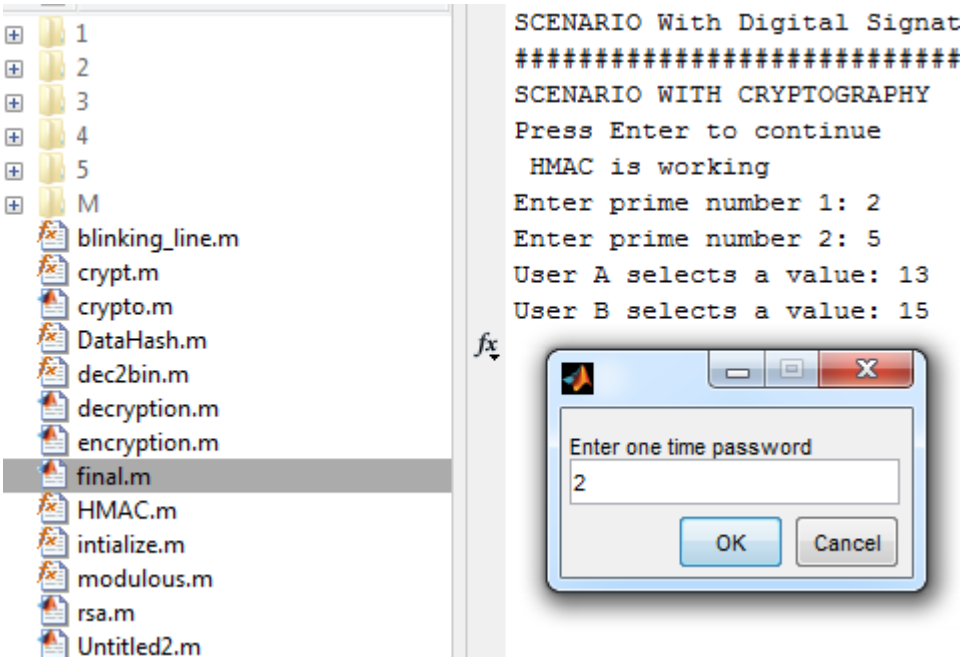

Figure 5.13: OTP validation

OTP is validated by the server, if this is correct then HMAC will be generated based on Shared Secret Key and operation.

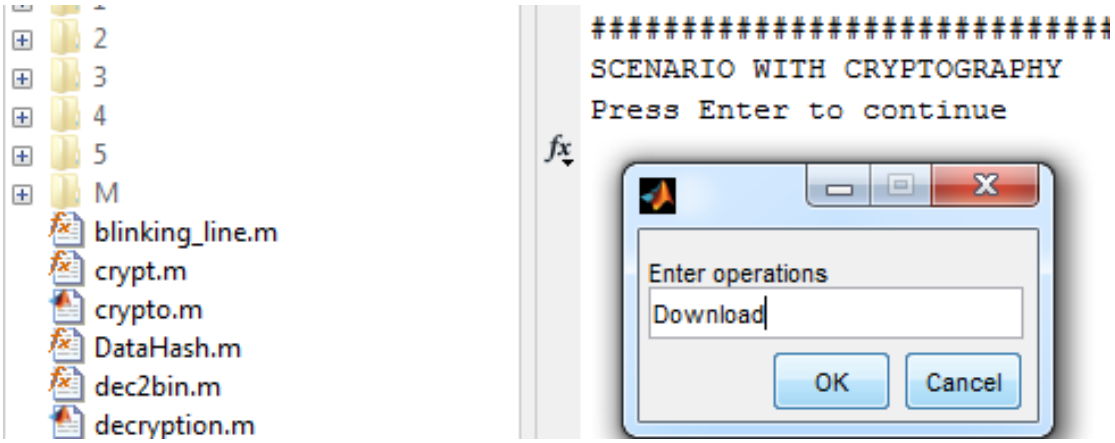

Figure 5.14: Enter Operation

User will enter the operation what he wants to perform over Cloud.

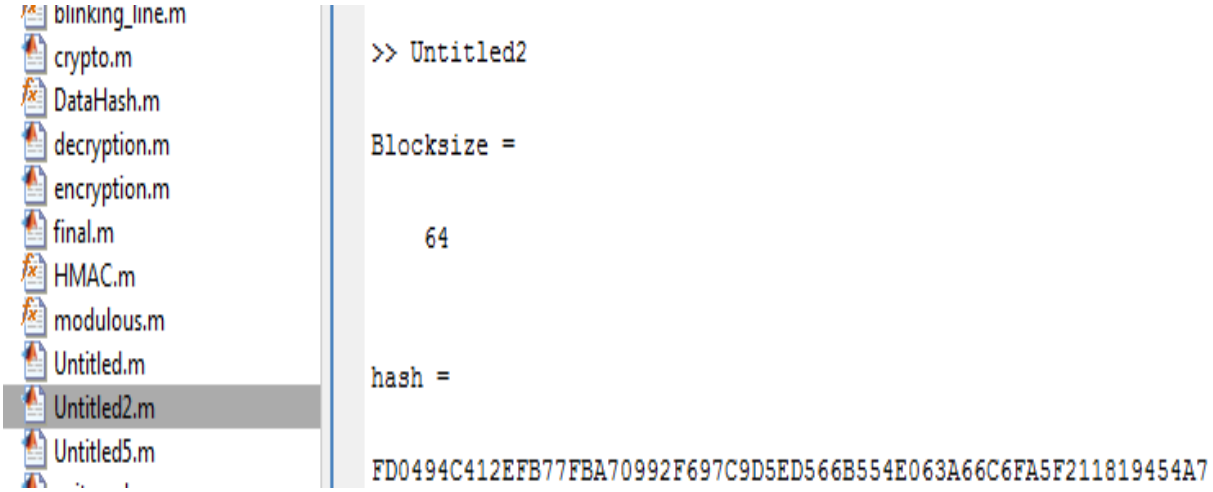

Figure 5.15: HMAC Formation

Data in encrypted form while being transmitted.

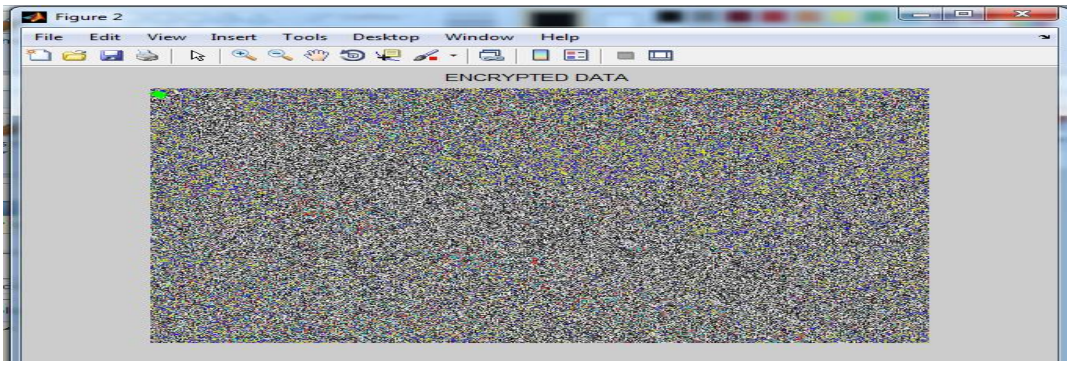

Figure 5.16: Encrypted Data in Transmission

Data is transferred successfully to the user.

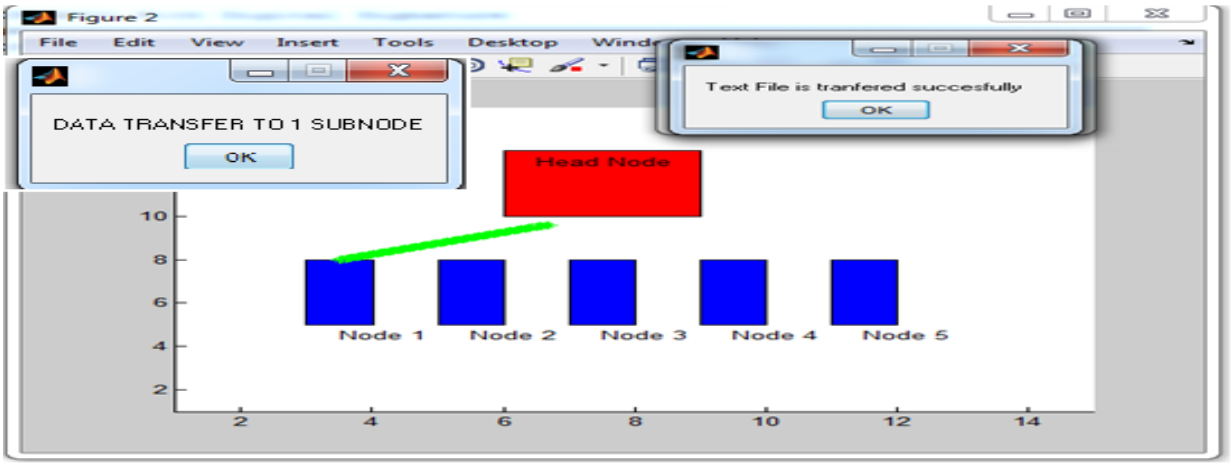

Figure 5.17: Successful Transmission

5.3 Performance Analysis and Conclusion

5.3.1 Execution Time Improvement over Modified HMAC

Elapsed time for Modified HMAC approached presented in the paper [50] is 1.9967second and parallel form of this approach derived in this thesis which takes 1.2077 seconds have been compared using Bar Graph.

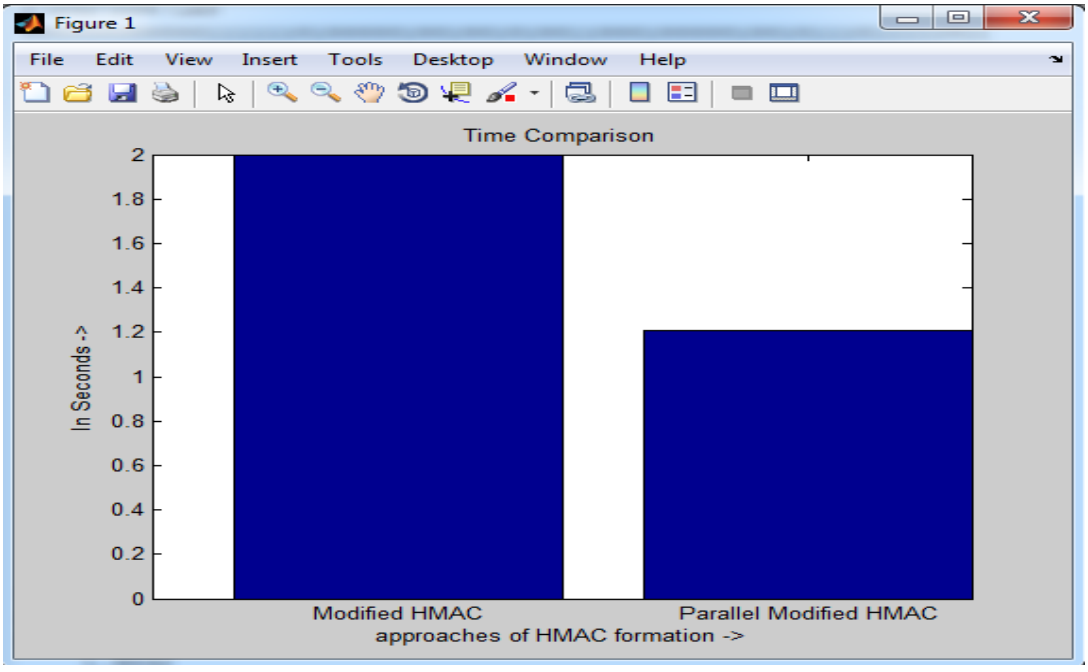

Figure 5.18 Execution Time of HMAC

5.3.2 Validation of the Proposed Approach

(i) Online guessing: This technique must be executed over public network. A malicious attacker can intercept the transmitted message from public network. Online guessing is not possible because if attacker breaks the first tier of authentication, he has to pass the second tier by entering OTP (K+N) which is formed using shared secret key with challenge which is known to only end user.

(ii) Verifier impersonation: Assume adversary has successfully stolen the verifier of password from the server, he/she can`t recover password from OTP because this is a onetime session generated password. Even if attacker impersonates the verifier in an authentication protocol, he can not alter the message because message is sent using HMAC (shared secret key || message || method), which manage the integrity of the message because shared secret key known only to end users.

(iii) Eavesdropper: Eavesdropping can be prevented by the proposed approach because encryption algorithm has been used while transmitting data so no one can decipher the private communication of end users.

(iv) Man-in-the-middle: Let A, B and C are three users, A wants to communicate with B, but all communication is passing through C, but in our mechanism C can`t alter the message because we have maintained message integrity has been maintained using HMAC, which can be decrypted only by those users who know shared secret key.

5.3.3 Space Requirement

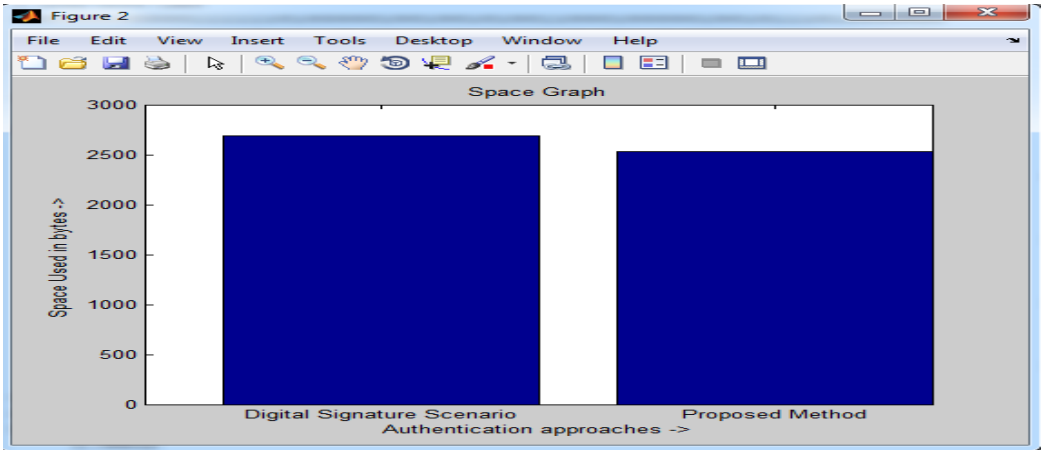

Figure 5.19: Space Requirement

In the proposed approach users need to store only login credential which requires 253 byte on an average in multitier authentication, to store login number it will take further 1byte for each user which is negligible as compared to digital signature apart from credential login; key also has to be stored in digital repository which is of 128 bits or 16 byte, hence requires additional space. This graph shows the space requirements for 10 users in our proposed scheme and digital signature authentication scheme.

5.4 Conclusion

In this thesis several existing attacks and mechanisms of secure data transfer over network in Cloud have been examined. A mechanism has been proposed which provides strong authentication via OTP generation and integrity via HMAC based on same shared secret key generated by Diffie Hellman algorithm. Result of HMAC formation has been collected using MATLAB tool.

Chapter 6

Conclusion and Future Scope

This chapter discusses the conclusions of the work presented in this thesis. This chapter ends with a discussion of the future direction which can be taken further.

6.1 Conclusions

This thesis gives an introduction to Cloud computing and background of various secure data transfer mechanisms to manage the authenticity, confidentiality and integrity of messages. In this work a secure data transfer mechanism has been proposed which uses Diffie Hellman key exchange algorithm for 3 way protection. Execution stages have been presented using flow and sequence diagram while encryption/decryption working and experimental result of HMAC has been collected using MATLAB R2011b tool which shows proposed parallel execution of Modified HMAC takes less time 1.2seconds as compared to existing one 1.9seconds.

6.2 Thesis Contribution

a) In this thesis existing secure data transfer techniques have been analyzed and compared according to their features.

b) A secure data transfer technique has been designed and the design of this technique has been depicted through its architecture, Data Flow Diagram and Sequence Diagram.

c) The designed has been proposed while encryption/decryption working and parallel algorithm for Modified HMAC has been coded on MATLAB tool which shows improvement over existing Modified HMAC.

6.3 Future Scope

a) This work shows the secure data transfer via two tier authentication using OTP and HMAC which protect data against different attacks like On-Line guessing,

Eavesdropper, Verifier impersonation and Man-in-the-middle. In the future, Replay attack can also be considered and prevented using Time Stamp in HMAC.

b) It is also foreseen to perform real test with distributed computing on Amazon cloud along with Matlab tool.

[1] "Cloud Computing Evolution," [online] Available: www. computerweekly.com/feature/A-history-of-Cloud-computing. [Feb. 20, 2014].

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A view of cloud computing", Communications of the ACM, vol.53, no.4, pp. 50-58, 2010.

[3] M. Creeger, "Cloud computing: an overview," *ACM Queue*, vol.7, no.5, pp. 2, 2009.

[4] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation computer systems*, vol. 25, no. 6, pp. 599-616, 2009.

[5] I. Foster and C. Kesselman, "The grid 2: blueprint for a future computing infrastructure," *Waltham: Morgan Kaufmann Publishers*, 2004.

[6] M. A. Rappa, "The utility business model and the future of computing services," *IBM Systems Journal*, vol. 43, no. 1, pp. 32-42, 2004.

[7] L. Kleinrock, "A vision for the internet," *ST Journal of Research*, vol. 2, no. 1, pp. 4-5, 2005.

[8] M. Turner, D. Budgen and P. Brereton, "Turning software into a service," *Computer*, IEEE, vol. 36, no.10, pp. 38-44, 2003.

[9] "Evolution of Cloud computing," [online] Available: www.tech.gaeatimes.com/index.php/archive/top-10-Cloud-computing-service-providers-in-2010. [Feb. 20, 2014]

[10] "Cloud Watch Hub," [online] Available at: http://www.cloudwatchhub.eu/glossary. [Oct. 4, 2013].

[11] "Seeding the Clouds: Key Infrastructure Elements for Cloud Computing," [online] Available: http://www-935.ibm.com/services/in/cio/pdf/oiw03022usen.pdf. [Feb. 20, 2014]

[12] Vaquero, M. Louis, R. Merino, Luis and Maik, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50-55, 2008.

[13] "Gartner says contrasting views on Cloud computing are creating confusion," [online] Available: www. gartner.com/newsroom/id/766215. [Feb. 20, 2014]

[14] M. Brown, "White paper: Cloud computing," *Maximum PC*, Jan. 12, 2009.

[15] R. Buyya, C. Yeo, and S. Venugopal, "Market-oriented cloud computing: vision, hype and reality for delivering it services as computing utilities", *Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications*, HPCC-OB, IEEE CS Press, Los Alamitos, CA, USA,pp. 5-13, 2008.

[16] P. Mell and T. Grance, "The NIST Definition of Cloud computing," *National Institute of Standards and Technology*, vol. 53, no. 6, 2009.

[17] "The open Cloud manifesto: A call to action for the worldwide Cloud community (Draft 1.0.9)," [online] Available:

www.openCloudmanifesto.org/openCloudmanifesto1 [Mar. 5, 2014].

[18] K. Jeffery, B. Neidecker-Lutz, "The future of cloud computing: opportunities for european cloud computing beyond 2010," *Expert Group Report*, European Commission, Jan. 2010.

[19] V. R. Srinivasa, N. K. R. Nageswara and E. K. Kumari, "Cloud computing: an overview," *Journal of Theoretical and Applied Information Technology*, vol. 9, no. 1, pp. 71-76, 2009.

[20] M. Ahmed, A. Chowdhury and M. H. Rafee, "An advanced survey on cloud computing and state-of-the-art research issues", *International Journal of Computer Science Issues*, IJCSI, vol. 9, issue 1, no. 1, Jan. 2012.

[21] *Oracle JD Edwards Cloud Computing: choosing a deployment strategy that fits*, white paper, Oracle Corp., Oct. 2012.

[22] "Cloud Computing: Acronyms (IaaS,PaaS,SaaS)," [online] Available: www. mahameeditpro.blogspot.in/2012/03/saas-software-as-service-essentially.html. [Mar. 5, 2014].

[23] D. C. Wyld, "Moving to the cloud: An introduction to cloud computing in government," *IBM Center for the Business of Government*, 2009.

[24] "Cloud Computing Technology- the study of its model," [online] Available: www. websiteglobe.blogspot.in/2012/05/Cloud-computing-technology-study-of-its.html. [Mar. 5, 2014].

[25] Q. Zhang, L. Cheng and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of internet services and applications*, vol. 1, no. 1, pp. 7-18, 2010.

[26] R. P. Padhy, M. R.Patra and S. C. Satapathy, "Cloud computing: security issues and research challenges", *International Journal of Computer Science and Information Technology & Security*, vol. 1, no. 2, Dec. 2011.

[27] M. Nazir, "Cloud computing: overview & current research challenges," *Journal of Computer* Engineering, IOSR-JCE, vol. 8, issue 1, pp. 14-22, Dec. 2012.

[28] M. A. Vouk, "Cloud computing–issues, research and implementations," *Journal of Computing and Information Technology*, CIT, vol. 16, no. 4, pp. 235-246, 2008.

[29] V. K. Reddy, B. T. Rao and L. S. S. Reddy, "Research issues in cloud computing," *Global Journal of Computer Science and* Technology, vol. 11, no. 11, 2011.

[30] T. Dillon, C. Wu and E. Chang, "Cloud computing: issues and challenges," *24th IEEE International Conference on Advanced Information Networking and Applications*, AINA, pp. 27-33, Apr. 2010.

[31] B. Schroeder and G. A. Gibson, "A large-scale study of failures in high performance computing systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 4, pp. 337-351, Oct. 2010.

[32] D.Zissis and D.Lekkas, "Addressing cloud computing security issues", *FGCS ELSEVIER*, Vol. 28, Issue 3, Pages 583–592, March 2012.

[33] C. Rong, S. T. Nguyen and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computers and Electrical Engineering*, vol. 39, no. 1, pp. 47-54, 2013.

[34] "New IDC IT Cloud Services Survey: Top Benefits and Challenges," [online] Available: http://www.blogs.idc.com/ie/?p=730. [Mar.5, 2014].

[35] "The Notorious Nine Cloud Computing Top Threats in 2013," [online] Available: www.Cloudsecurityalliance.org/topthreats. [Feb. 20, 2014].

[36] 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, issue 1, pp. 1-11, Jan. 2011.

[37] W. E. Burr, D. F. Dodson and W. T. Polk, "Electronic authentication guideline," *NIST Special Publication*, US Department of Commerce, Technology Administration, National Institute of Standards and Technology, Apr. 2004.

[38] V. Sulochana and R. Parimelazhagan, "A puzzle based authentication scheme for cloud computing," *International Journal of Computer Trends and* Technology, IJCTT, vol. 6, no. 4, pp. 210-213, Dec. 2013

[39] P. Rewagad and Y. Pawar, "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing," *International Conference on Communication Systems and Network Technologies*, CSNT, IEEE, pp. 437-439, 2013.

[40] S. E. Arasu, B. Gowri and S. Ananthi, "Privacy-preserving public auditing in cloud using HMAC algorithm," *International Journal of Recent Technology and Engineering*, IJRTE, vol. 2, issue 1, Mar. 2013.

[41] N. Tirthani and R. Ganesan, "Data security in cloud architecture based on diffie hellman and elliptical curve cryptography," *IACR Cryptology*, ePrint Archive, vol. 49, 2014.

[42] K. Govinda, V. Gurunathaprasad and H. Sathishkumar, "Third party auditing for secure data storage in cloud through digital signature using RSA," *International Journal of Advanced Scientific and Technical Research*, vol. 4, issue 2, Aug. 2012.

[43] M. Singh and S. Singh, "Design and implementation of multi-tier authentication scheme in cloud," *International Journal of Computer Science Issues*, IJCSI, vol. 9, issue 5, no. 2, Sep. 2012.

[44] S. Kumar and A. Ganpati, "Multi-authentication for cloud security: A framework," *International Journal of Computer Science & Engineering Technology*, vol. 5, no. 4, pp. 295-303, Apr. 2014.

[45] P. Kalpana and S. Singaraju,, "Data security in cloud computing using RSA algorithm," *International Journal of Research in Computer and Communication technology*, IJRCCT, vol. 1, no. 4, pp. 143-146, Sep. 2012.

[46] "Authentication, Authorization and Contextualization in FermiCloud," [online] Available: www.cd-docdb.fnal.gov/cgi-bin. [Mar. 5, 2014].

[47] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," *International Conference on Computer Science and Electronics Engineering*, ICCSEE 2012, IEEE, vol. 1, 2012.

[48] "MATLAB" [online] Available: www.mathworks.in/products/parallel-computing. [Mar. 5, 2014]

[49] "MATLAB" [online] Available: www.cba.neu.edu/~mmeyer/courses/platforms/mathworks.pdf. [Mar. 5, 2014].

[50] B. Sridevi and S. Rajaram, "Deploying modified hash based message authentication code HMAC in MATLAB using GUI controls," *International Conference on Information and Network Technology,* ICINT 2011, vol.4, 2011.