AN ENHANCED MUTUAL AUTHENTICATION SCHEME TO DETECT AND ISOLATE ZOMBIE ATTACK

A Dissertation Proposal

Submitted

By

Harneet Kaur Bhinder

(11309942)

to

Department of Science & Technology

In partial fulfillment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science Engineering

Under the guidance of

Mr Krishan Bansal

(April 2015)

PAC APPROVAL

INDIA'S LARGEST UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education, Transforming India

School of Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Harneet Kaur	Registration No:11309942.
Batch: 2014	Roll No.K2306A28
Session: 2014-15	Parent Section: K2306
Details of Supervisor:	Designation: AP
Name: Krishan Bansal	Qualification: MS
U.ID: 16348	Research Experience: 2 Years

SPECIALIZATION AREA: Network and Security **(pick from list of provided specialization areas by DAA)**

PROPOSED TOPICS

1. Security issues in Cloud Computing
2. Performance of Cloud
3. Cloud Computing reliability

Signature of Supervisor 16348

PAC Remarks:

Topic 1/ is approved.

APPROVAL OF PAC CHAIRPERSON: **Signature:** 1/10/11 25/9/14 **Date:**

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

Cloud computing is a novel technology and a kind of distributed network which concatenate different concepts and technologies and creates a platform for cost-effective business applications and IT infrastructure. Though its adoption is rapidly rising in the market of technology for cost effective benefits. Different kinds of services like OS, API, storage and many more are being provided to user as service and these resources are provided as service because user has to pay for it according to its usage requirements. Cloud computing is now become most popular technology because of its availability, low cost and some other factors. But there are some issues in cloud computing, the main one is security. The problem of verifying accuracy of data storage in the cloud becomes even more demanding as virtual machines are considered the trust able party of the user which can encrypt data on the behalf of user and provide to cloud service provider which upload the data to virtual server but if the virtual machines are malicious then zombie attack will be triggered in the network which is a DoS (denial of service) attack and it reduces the efficiency of the cloud architecture. In this work, zombie attack will be isolated by detecting malicious virtual machines from the cloud architecture. The proposed technique will be based on the mutual authentication mechanism which will detect malicious VM machines which are responsible to trigger zombie attack and enhanced mutual authentication technique will prevent this zombie attack by identifying server before the establishment of communication between user and server.

ACKNOWLEDGEMENT

I would like to place on record my deep sense of gratitude of Assistant Professor Mr. Krishan Bansal School of Computer Science, Lovely Professional University, Phagwara, India for his generous guidance, help and useful suggestions.

I wish to extend my thanks to Head of Department Mr Dalwinder Singh, School of Computer Science for his constructive suggestions to improve the quality of this research work.

I am extremely thankful to Head of School Rajiv Sobti, School of Computer Science, Lovely Professional University for providing me infrastructural facilities to work within, without which this work would not have been possible.

DECLARATION

I hereby state that the dissertation proposal entitled, "An enhanced mutual authentication scheme to detect and isolate zombie attack" submitted for the M.Tech Degree is wholly my novel work and all facts and references have been fittingly acknowledged. It does not contain any work for the reward of any other degree or diploma.

Date: 30-04-2015

Investigator: Harneet Kaur Bhinder

Registration No: 11309942

CERTIFICATE

This is to certified that Harneet Kaur Bhinder has completed M.TECH Dissertation proposal titled **"**An enhanced mutual authentication scheme to detect and isolate zombie attack**"** under my guidance and supervision. To the best of my acquaintance, at hand work is the outcome of her inventive exploration and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the obedience and the partial fulfilment of the conditions for the award of M.Tech Computer Science & Engg.

Date: 30-04-2015

Signature of Advisor

Name: Mr. Krishan Bansal

UID: 16348

TABLE OF CONTENTS

Chapter 1 INTRODUCTION

1.1. INTRODUCTION ……..…...……1

1.1.1. ARCHITECTURAL CONSIDERATION……...……...…2

1.1.2. CLOUD SERVICE LAYERS OR MODELS ….....3

1.1.3 CHARACTERISTICS OF CLOUD COMPUTING 4

1.2 SECURITY ISSUES IN CLOUD COMPUTING…….....…….…..….5

1.3 CLOUD COMPUTING ATTACKS.....6

1.4 MUTUAL AUTHENTICATION……..….....7

1.4.1 ZOMBIE ATTACK …….....….8

Chapter 2 LITERATURE REVIEW…….……..…9-16

Chapter 3 PRESENT WORKS

3.1 PROBLEM FORMULATION…….....…….……..……...17

3.2 SCOPE OF STUDY…….....…….……...…...18

3.3 OBJECTIVE…….....…….....……..…19

3.4 RESEARCH METHODOLOGY ……....…...…….…….20-22

Chapter 4 RESULTS AND DISCUSSION…….....……..23

4.1 TOOL …….....…….....……23

4.2 IMPLEMENTATION …….……..... .....…23-33

4.3 OUTCOME …….....……34

4.4 GRAPHS ……....…….....…35-37

Chapter 5 SUMMARY AND CONCLUSION ……38

Chapter 6 REFRENCES …….…..39-40

LIST OF FIGURES

Figure-1: Types of clouds .....…… 4

Figure-2 Services models.....…….....5

Figure-3 DDOS attack.....7

Figure-4 Man in the middle attack.....8

Figure-5 Mutual Authentication.....10

LIST OF ABBREVIATIONS

IAAS …….....Infrastructure as service

PAAS…….....……..... Platform as service

SAAS……..….....Software as service

FTM ……..... Fault tolerance manager

SLA.....Service level agreement

OTP.....One Time Password

CSP……....Cloud service

VM…… ……Virtual machine

Chapter 1
INTRODUCTION

1.1 CLOUD COMPUTING:

Cloud computing is a novel technology and a kind of distributed network which concatenate different concepts and technologies for providing cost-effective business applications, platform and IT infrastructure. Though its adoption is rapidly rising in the market of technology for cost effective benefits. Due to more availability of services with less cost of cloud infrastructure and its maintenance, information technology industries got benefited from it. Cloud computing; thus, may be distinct as a multitenant environment that supplies users with a shared pool of different kinds of resources which are being abstracted from the primary infrastructure. Users can access resources "on demand "and "at scale" in cloud environment. Different kinds of services like OS, API, storage and many more are being provided to user as service and these resources are provided as service because users have to pay for it according to its usage requirements. These terms used in definition of cloud could be further elaborated as:-

•**Multi Tenant Environment:-** In a multi tenant environment provided by cloud, multiple tenants can access and being served with resources from a single implemented pool of services for providing a cost effective environment.

•**On Demand: -** On demand means user is served with resources on its demand and requirement and get released from those resources when not required and estimated when only used.

•**At Scale: -** In order to meet able to meet all the desires demanded by customers,infinite service are available at large scale.

1.1.1 ARCHITECTURAL CONSIDERATION:

In architectural consideration, we define the how cloud infrastructure can be deployed in different modes. It consists of diverse models that are entailing to estimate the cloud computing architectures. Architecture considers several deployment models are being differentiated on the basis of physical locations and infrastructure's provider. They are four types of deployment models:

i. Public cloud – Public cloud is that cloud deployment in which cloud resources are made available to the wide-ranging public by the provider itself. They are basically handled by any third party or organization due to their stand alone feature and are present off premises. To support general public with resources at scale, a service provider designs such infrastructure. Third parties and companies mainly use public cloud and their example is Amazon, Microsoft and Google App Engine.

ii. Private cloud –Cloud computing resources which are only presented to restricted faction of clients, to a single organization comes in category of private cloud. Usually organizations have their own private cloud and resources are limited to the users and runs in physical data centre of that particular organization. Cloud is deployed as private to internally serve resources to an organization. They may be implemented in an existing data centre of third party. This demonstration acquires a high level of manage over the cloud infrastructure and the cloud services.

iii. Hybrid – Hybrid cloud is defined as that cloud encompass the characteristics of both public and private cloud infrastructure. If we want to scale the services, then it will deem as public and for taking out day to day operations it may regard as private cloud. Hybrid itself means it's a permutation so here it combines private and public cloud.

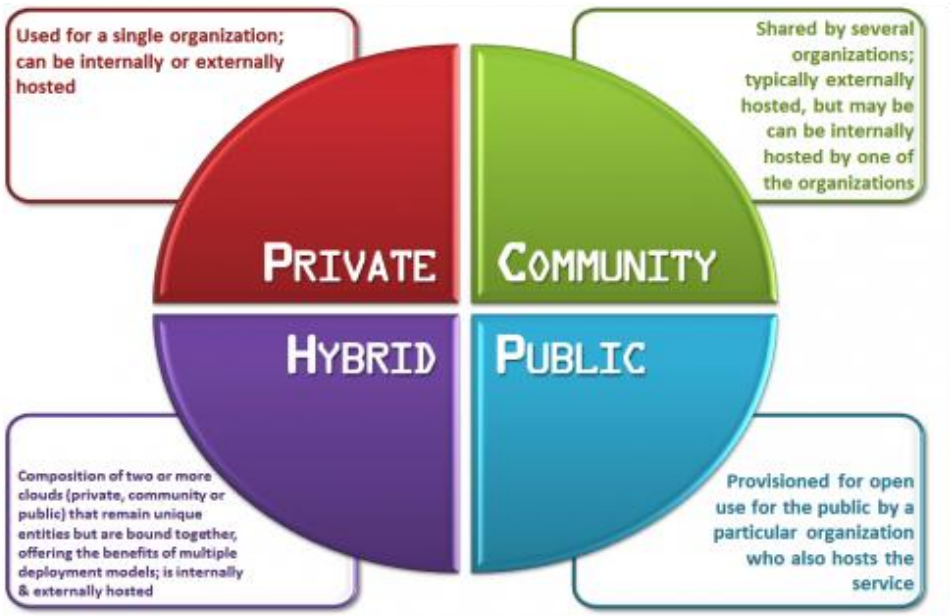


Figure 1 TYPES OF CLOUD: [9]

1.1.2 CLOUD SERVICE LAYERS OR DELIVERY MODELS

Cloud service layers or delivery models are differentiated on the basis of services provider by then on cloud environment. Cloud service models are mainly divided into three types, which are as follow:

i. Infrastructure as service (IaaS): IaaS stands for infrastructure as a service in which it serves cloud user's with hardware resources such as storage capacity, CPU and network components as a service. Cloud resources are supplied by cloud provider on virtualization platform and user can access them all the way through internet. In order to handle workloads all the services like storage systems, networking equipment, data centre space are collected and made available from a single pool. For example Amazon (Amazon web services), Google Compute Engine (GCE).

ii. Platform as service (PaaS): PaaS provides platform as a service i.e a framework for the development of software's and provides a run time environments over the network. Software platform and development environment which is combined and later it is offered as package to the customers for building their application. PaaS providers manages the requirements of applicants by offering them a predefined permutation of operating system OS and servers, such as LAMP (Linux, apache, MySql, PHP). Example Google App Engine, Amazon web services.

iii. Software as service (SaaS): Software as a service by the name itself reflects that complete software is delivered as a service to the customer over internet. A single occurrence of the service runs on the cloud. On the basis of subscription and demand of

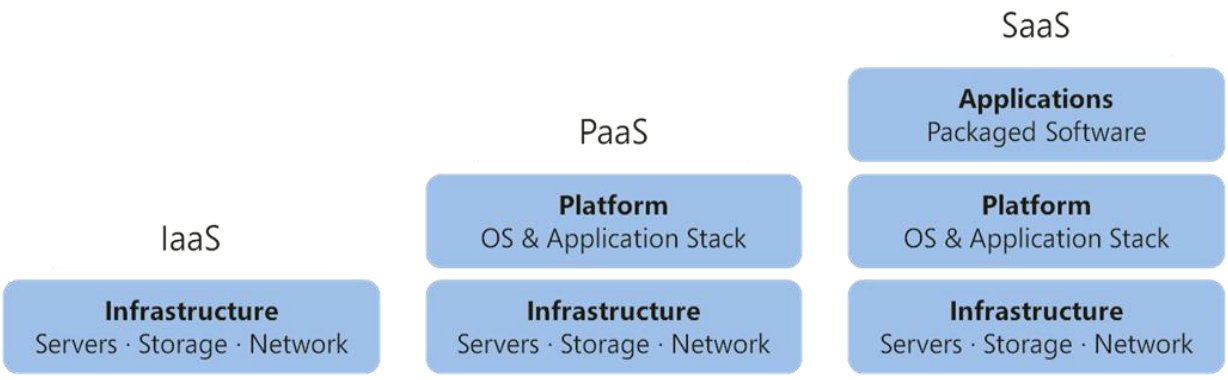


Figure 2 SERVICE MODELS:[10]

Customers, software service of cloud is being delivered over the network. Google and Microsoft are the providers of software as service in cloud. Example Gmail etc.

1.1.3 CHARACTERISTICS OF CLOUD COMPUTING

i.Broad network access: It refers to the right to use of resources from a ample range of devices such as tablets, PCs, Macs and smart phones and different locations anywhere and anytime. But there are some sorts of security loop holes while proving a wide range of access to number of devices.

ii.Shared resource pool: Services of cloud computing provide on demand access to shared pool of wide variety of resources in the form of services like platform, infrastructure and software as a service which consists of OS, API, storage etc. Cloud service provider supplies all these resources to user upon request and demand. Headache and time consuming activity of installing software's ,buying extra hard disk for the requirement of more storage and all other a replaced by cloud computing services to whom user can access with the help of internet anytime and anywhere.

iii.Metered services: Resources are provided to customers in the form of services because user have to pay for the usage. They pay according to their demand and access. Limited numbers of services are provided freely but if the company requirement exceeds the available service they can gain access by paying for it.

iv.Elasticity: Cloud computing provides suppleness of cloud network. We can extend out network, network resources, service providers, virtual servers upon our requirement. Cloud computing is not a static network which is fixed with limited and fixed additions.

v.Flexibility: It is quite flexible i.e it easily adopts all the changes used to make in any component of cloud network. It also provides flexibility in the process of accessing resources.

1.2 SECURITY ISSUES IN CLOUD COMPUTING

Security is the major anxiety for any network terminologies available over internet because of many reasons like secret and confidential data in an organization which must be protected from third party or unauthorized access and attacks. The main problem cloud

computing faces today is to preserve confidentiality and integrity of data. Some of the security issues are described as following:

Trust- Trust between cloud service provider CSP and customers is one of the main issue facing by many companies. SLA (service level agreement) is the only legal document which is the solution to resolve this problem which contains information of what providers is doing and willing to do.

Confidentiality- Information of user should always be kept confidential because of information storage at the remote locations and every cloud user uses the shared storage and while sharing those resources, work done on them is confidential. So it is necessary to prevent the offensive exposé of information. Encryption is one of the best way to prevent data from being disclosure.

Identity and access management- Authentication, authorization and auditing of the users accessing cloud services are some of the key concepts to be surely considered for security purpose. There is trust boundary between organization which can be controlled and monitored for the applications deployed on the cloud.

Authenticity (Integrity and Completeness) - Like confidentiality, preventing integrity is also one of the main concern that needs to be handled through encryption. One way to this is to use digital signatures for successful encryption. But there is a problem because not all users have access to supersets and they cannot verify the subset of data even if they are provided with digital signature.

Key Management- Key management issue of major issue in cloud computing. In the traditional encryption techniques single is used for both encryption and decryption. Customer must control and manage their key management systems because encryption keys cannot be stored on cloud.

1.3 CLOUD COMPUTING ATTACKS:

In cloud computing there are many types of security issues as we discussed and due these issues, several attacks are possible in cloud. There are various potential attacks vector criminals may attempt such as:

a. Denial of Service (DoS) attacks - Dos attack is defined as security attack in which services are unavailable for authenticated users also. Cloud is more vulnerable to

DoS/Distributed DOS attacks because it is shared by larger number of users which can makes DoS attacks much more hazardous .

b. Side Channel attacks – Malicious virtual machine are placed in close proximity to a target where attacker could challenge to negotiation the cloud and then exploit a side channel attack.

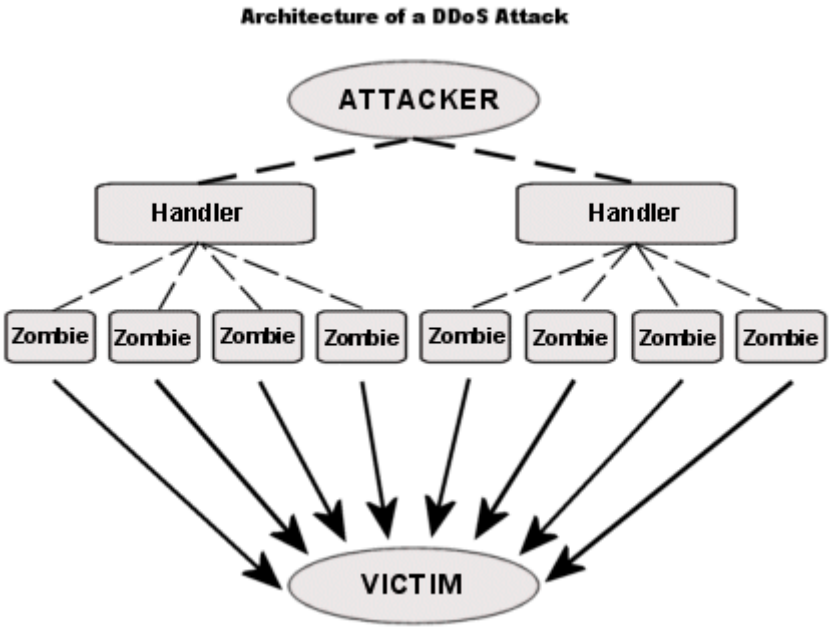


Fig. 3 of DDOS attack [Sanjoli Singla, 2009]

c. Authentication attacks – One of the weakest points in virtual services is authentication and is commonly under fire. We can authenticate users in many different ways but can be attacked during authentication because during authentication process user and server exchange keys and if keys are hacked by attacker ,then There are many different kind of ways to authenticate users for example based on what a person knows, has, or is. Attackers frequently target technology used to secure the authentication process for authentication attack.

d. Man-in-the-middle cryptographic attacks – When attacker places himself between two communication parties i.e sender and receiver in order to carry out man in the middle attack. Attacker can intercept and modify communications message taking place between two parties. Man in the middle attack is used to sniffs any data being sent. Attacker receives original data from both parties and responds then with fake data.

In the below diagram is an example of how a man-in-the-middle attack works. The attacker intercepts some or all traffics coming from the client, collects the information and then precede it to the destination the user was originally intending to visit.

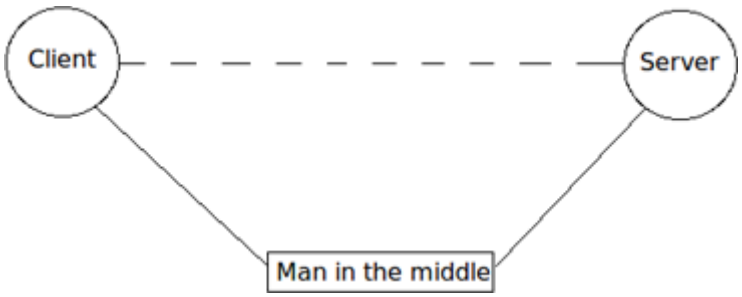


Fig4 Man in the middle attack (Young-Gi Min,2012)

1.4 MUTUAL AUTHENTICATION:

Mutual authentication is an authentication scheme in which both user side and server side authentication is carried out for the establishment of communication. The scheme consists of various phases like

- Registration phase,
- Login Verification phase,
- Mutual authentication phase
- Password change phase.

Both user and server are verified to start communication if they will be proved authorized, they can proceed further with their process otherwise they will be halt. Mutual authentication is vulnerable to denial of services but it provides some solution like password checking during identification and login phases to allow only valid user to access services and block unauthorized users by preventing them from requesting to overload the cloud server.

Mutual authentication also called as 2-way authentication where both sender and receiver authenticate each other at the same time. In order to ensure each other identity user authenticating themselves to a server and server authenticating itself to user. Mutual authentication provides the same things as Secure Socket Layer, with the addition of authentication and non-repudiation of the client authentication, using digital signatures. During mutual authentication process, certificate is being provided to server by client to prove its legitimacy. Mutual authentication requires an extra round trip time as client sends its certificate then server sends it back after authenticating it.

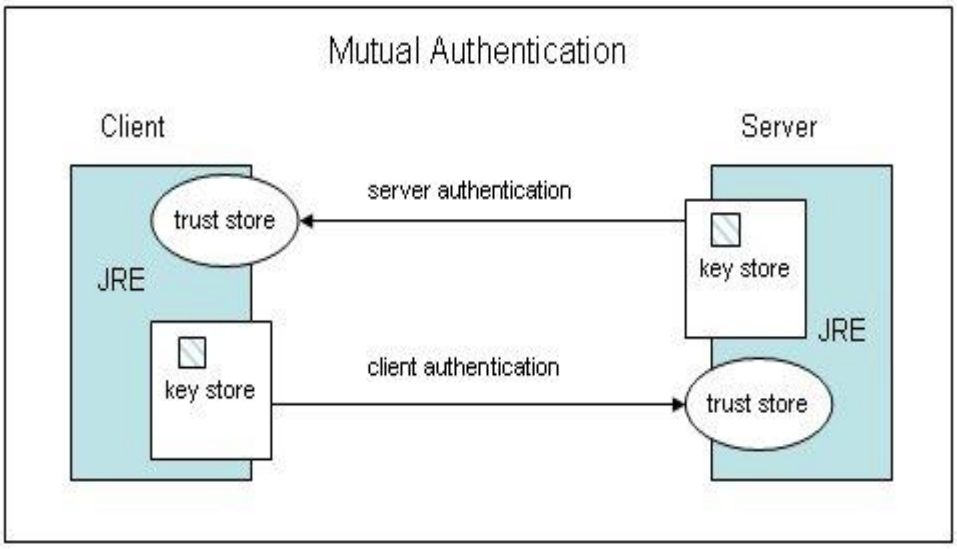


Fig 5. Mutual authentication

1.4.1 ZOMBIE ATTACK: In computer science, a zombie is a computer linked to the Internet that has been compromised by a hacker, computer virus or Trojan horse. Zombie computers are often used to spread e-mail spam and initiate denial-of-service attacks in which services are unavailable for authorized users. User of zombie computers will be uninformed that their system is being used in a wrong way. Attacker tries to overflow the victim by sending large number of requests from unaware hosts in network through interne. These unaware hosts are called as zombies. We access virtual machine through internet but if service to access that virtual machine is denied by attacker for legitimate user, then they won't be able to access it though and cloud server won't be able to respond to user request. Performance and availability of Cloud services is interrupts due to non availability of resources. The zombie attack will degrades the network performance and reduce reliability to large extend. This behaviour of cloud will not accomplish user's requirements.

Chapter 2
LITERATURE REVIEW

Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013) [1] Proposed the analysis of security issues of cloud computing. They worked up upon SPI model i.e SaaS, PaaS, IaaS vulnerabilities and threats. We need to ensure the security factors and provide confirmation of security to organization while data travels through internet or there is an involvement of third party. Relationship between different vulnerabilities and different threats then is also discussed by listing them. Different types of virtualization technologies approach security mechanisms in different ways. Biggest security concerns in cloud computing are storage, virtualization, and networks. Survey of security issues about clouds is conducted .They have determined dissimilarity, where it's important to understand these security issues. Relationship between vulnerabilities and threats is made in order to recognize what vulnerabilities add on to the implementation of these threats and make the system more robust, this thing was done because relation among security issues was not enough. While communicating with remote virtual machines, virtual networks also get targeted for some attacks. A new security techniques and equipments avoid those problems due to some complexities in previous security technique. They have discussed some vulnerabilities which virtual network faces while communicating with remote virtual machines.

Jian Yu, Quan Z. Sheng, Yanbo Han (2013) [2]: Proposed special issues and computing services on the basis of reliability. Cloud services include reliability model, service virtualization, and user-centric services. Cloud service reliability model, service virtualization, and user-centric services. A reliability model of atomic Web services is proposes with few fault tolerance techniques to improve the quality of service using recovery block adaptation. Fuzzy requirements and a two-level ranking algorithm are discussed and evaluated.

One of them have proposes a spreadsheet-like encoding environment called mashroom to support data integration by non skilled users at particular locations. This paper focus on key directions in which active and hastily expanding area of research and

development are involved. For satisfying the on-demand needs of users, large-scale data centers must offer reliable and secure services with high quality standards.

V.Nirmala, R.K. Sivanandhan, Dr. Shanmuga laskmi (2013) [3] proposed the encryption for the statistics that they have classified as inactive data and alive data. There is enhancement in the security issues with the services provided under infrastructure as service. Less security is required for inactive data as classified by which does not show much changes and is mostly used for storage but in case of alive data that often changes we need to rise the security levels so that they are not much prone to risks. All the security issues that can occur are being surveyed and have proposed a solution in case of alive data. The associated effort of this paper is voted out in the area of integrity. The method that they have chosen for this issue is they have wrapped up the data double so that no leakage occurs on server sides and have improved the encryption levels with the integrity mechanism.

Virendra Singh kushwah and Aradhana Saxena (2013) [4] proposed security approaches while migrating the data. As purchaser gaze to shift their data and applications to the cloud so that's why security is the most imperative question that is at all times raised from the purchaser perspective. The consequence of security in the migration of inheritance systems have been justified and have carried out an approach that aims at ruling the needs, concerns, requirements, aspects, opportunities and benefits of security in the migration process of legacy systems . They must accomplish the objectives, confidentiality and audit ability for improving the security in the procedure of migration. Secure data access and transfer is provided under confidentiality and in case of audit ability for attesting whether the security surroundings of applications have been changed or not.

N.S.Sudharshan, Dr. K Latha 2013[5] proposed a new approach which is used for preventing phishing attacks in Dropbox and is integrated in the system for the prevention of such attacks. Loads of social sites like facebook, Gmail, Dropbox are most popular these days. Some security issues are related with this because dropbox reached the hike these days. These services are used for accommodating storage of large amount of images, videos and audios. Data includes both the private and business sectors which is accumulated in the drop box. In online systems like banking systems phishing attack is the prime crisis. The attacker sends the counterfeit link to the user which appears as if

comes from authorized site which will temp the user to send sensitive information like user name, password, credit card number etc. The proposed system combines the two approaches for identifying phishing attack.

(I) Using abnormal keyword feature

(II) Identification of fake link (URL obfuscation) using the relationship facto between suspected link and its associated link in drop box cloud environment.

Pradnyesh Bhisikar, Prof Amit Sahu 2013[6] proposed a problem in transmission and storage of data in prospective with security. In networking high speed is the most significant issue. In contrast to conventional methods where data and services are under suitable control of physical, logical and personnel where in cloud computing data and resources are dispersed to various data centers where the management and security of data may not be trustworthy. This research paper provides information about security of data without affecting networking and also protecting the data from unauthorized attacks. They proposed a model where the transferred data is encrypted on the top of transport layer instead of IPSEC or SSL. Thus this is effective and flexible distributed scheme which provides secure communication by pre-processing of encryption in the upper layer.

Joel Gibson, Darren Eveleigh, Robin Rondeau, Qling Tan (2012) [7]: Proposed the challenges that are faced by the service models in cloud. Three architectural models mainly infrastructure as service, platform as service and software as service that are present in the cloud computing are discussed. Servers, storage and virtualization, hardware etc are provided under Infrastructure as a service to facilitate convenience services to user. As all other cloud services run on the apex of this service, so that's why security have become major confront in the infrastructure as a service in cloud delivery model.

In software as service and platform as service the main defy that arises is that, sometimes it became very complicated to understand appropriate business solution provided by cloud service model. This paper clearly states that that availability of services won't be decreased if users will be able to access services which are available at anytime

and anywhere to users. Main concern is lack of services and resource availability which leads to inadequacy in cloud environment.

Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom (2012) [8]: Proposed the research related to security of single cloud and due to uniqueness of "multi-cloud", "intercloud", "cloud of cloud", usage of single cloud is not that populated like before. Various security factors have different impacts on different services. As its being described that multi-cloud infrastructure requires less security attention as compare to single cloud. Recently several users faced many problems due to data intrusion, availability. Security techniques such as encrypting data using cryptographic hash function for maintaining data integrity and storing data on different servers to overcome the limitation of availability of data. For virtual storage Depsky data model which deals with different cloud provider is a being used with depsky library.
In multi-cloud bottom layer is the inner cloud i.e Byzantine protocol which deals with hardware and software faults called as byzantine faults.Limitation of encryption is that encrypted data can't be manipulated. However user involved in cloud computing environment can be affected with the use of multi-cloud.

Anas BOUA Y AD, Asmae BLILA T, Nour el houda MEJHED, MohammedEL GHAZI (2012) [9]: Proposed the security challenges of cloud computing. We believe the major impact of security issues while adopting the model for cloud computing. As due to model related problems such as architecture of cloud model, multi-tenancy, elasticity, it became more complicated to handle out security problems.Virtualization and SOA (service oriented architecture) are used for some of the security problems and on contrary multi-tenancy and isolation is being done for security of SaaS. They investigated the problem from different standpoint such as cloud architecture, cloud services, characteristics and derive a detailed specification of the cloud security problem from this analysis. Who so ever wants to access any object of cloud platform, should firstly pass through several security components. Elasticity engines and APIs (Application program interface) are some interfaces which provide flexible security interfaces.It delivers integrated security to support integration and organize security controls.

Users will not take full advantage of technology until and unless security models are not in place, so current way out provided by them also have some loop holes. Future work will focus on implementation of proper security model.

Ravi jhawar, Vincenzo Piuri, Fellow and Macro santanbrogio (2012) [10]: Proposed a approach which describes the implementation techniques of fault tolerance for application developers and customers. However there are reliability, availability and security concern to obtain fault tolerance properties from third party.

They have adopted redundancy mechanism to generate replicas of different resources for providing better fault tolerance .Long term fault tolerance is being provided to client application by service provider.Working of FTM (fault tolerance manager) is done, however work is not described well defined framework is designed in which system is integrated with existing cloud infrastructure and fault tolerance is being provided as a cloud service.This framework also provides elasticity of measuring the strength of fault tolerance and can consider cost analysis as future work.

Mohamed Hamdi (2012) [11]: Proposed research of security, storage and networking of cloud computing. Due to involvement of third party there are security vulnerabilities while services are delivered through network.Cloud computing is cost efficient but lack of protection is quite challenging, so some features such as confidentiality, privacy authentication, anonymity, survivability, dependability, and fault tolerance are in some extent, contradictory. Security requirements, security principles, testing mechanism are some of fundamental concepts of cloud discussed in this paper.Different security requirements such as confidentiality, availability are described in the basis of several services i.e Iaas, Paas, Saas.

Some attacks like HTTP acquire with flood attacks with number of requests which effect essentially resources of web application and then attach URL of that TCP connection flood on port 80 same as HTTP attack .Moreover study of several values and produce dealing with cloud security is still in process. Basis of cloud security techniques, tools, and countermeasures are discussed. The security challenges faced by cloud used and providers have been first highlighted. Attacks that can be conducted against cloud-based services are also reviewed. Other aspects which also affect the protection of cloud

computing are left for future work. Homomorphic encryption for cloud architectures, protection of cloud-based multimedia streaming, digital investigation in cloud computing will get investigated in future.

Huaglory Tianfield (2012) [12]: He proposed different issues regarding security of cloud computing i.e., confidentiality, integrity, availability, trust, and audit and compliance.Responsibilty of cloud security by multi-stakeholder according to services is described in detail. Security related factors of cloud are explained having characteristics like multi-tenancy, multiple stakeholders, third party control which deals with .Data integrity, trust, reliability are general requirements of cloud security. Loop holes of public cloud are discussed, as in public-cloud computing, we have multiple security issues that need to be addressed in comparison to a private cloud computing scenario. For providing a better shared resources environment, virtualization and multi-tenancy are the big issues using cloud computing. A complete security architecture depicting how to manage the security in cloud computing interface. Summarization of the security issues in cloud computing by a cloud security architecture and taxonomy for security issues in cloud computing are reviewed in this paper.

Wentao Liu(2012) [13]: Proposed a paper which illustrates cloud concepts and demonstrates the cloud features such as scalability, elasticity, platform independent, low-cost and reliability. The security problems in the cloud system are discussed. Cloud computing has a very fast rate of knots of development and shows good prospects and great potential. The cloud computing is related to many areas of information management and services. Data in the cloud computing environment is greatly dependent on the network and server, so data privacy issue becomes more outstanding than the traditional network. There are many customers who mistrust the security and privacy of cloud computing customers and they do not want to move the data into the cloud platform from the company or private system. The development of cloud computing and the security issue are the core problems. In order to effectively solve these problems the cloud computing provider must variety measures to protect the security.

Jaidhar C. D (2012) [14]: Proposed time-bound ticket-based mutual authentication scheme for cloud computing. This paper shows that the mutual authentication scheme is vulnerable to Denial-of-Service attack and insecure password change phase during the authentication process. An enhanced scheme is proposed to overcome these security pitfalls is a time based ticket bound scheme. Enhanced scheme is proved an efficient one on the basis of performance judgment. Hao et al's scheme is reviewed in this research paper but it has some disadvantages like Denial-of-Service attack due incompetent password change phase and wrong password recognition prior to login request phase of authorized user identification .To overcome these security loop holes, enhanced version of time bound ticket based mutual authentication scheme is proposed in this paper which verifies whether the password and identifier entered by user are correct or not .During mutual authentication, session key is used for smart card and cloud server agreement. In addition to it, user can select and change the password at the smart card side without taking any assistance from the cloud authentication server.

Alexandru Iosup, Simon Ostermann,Nezih Yigitbasi, Radu Prodan, Thomas Fahringer, and Dick Epema (2010) [15]: Proposed an analysis conducted by on cloud services for multi-task scientific computing and on some clouds such as Amazon(EC2),GoGrid(GG)etc. Virtualization, abstraction, resource level parallelism are factors describes impact on cloud infrastructure.E-scientific and big data centers are provided with new platform options on the basis of different parameters, performance of different clouds is evaluated

In this paper they have checked the sufficiency of cloud performance that to Multi- Task Computing.They find out the performace for scientific solutions is not good but it provides instant resources and temporarily needed for scientific purpose.

Clouds which are being used for commercial purposes carry out more workload. Due to low utilization of clouds clusters, there will be threatens to cancel out the commercial benefits provided by cloud to customers.

Balachandra Reddy Kandukuri,Ramakrishna Paturi V,Dr. Atanu Rakshit(2009) [16]: Proposed a service level agreement(SLA) a swot which is a security assurance scheme for customers by service providers .As there are many security concerns arises.

When data travels through internet and order to incite them for relying on security issues service level agreement is being conducted. For the assurance and understanding of security policies for customers which are not much aware SLA is used and it also describes the complexity, security based on the services a customer ask for. Current SLA's of cloud computing is reviewed and consistency of SLA's followed by the proposed data security issues is also discussed.

There is a consistent way to organize SLA taking in consideration, several security risks privileged user access, regulatory compliance, and will facilitates in using cloud computing services for enterprise. If services provided won't met SLA agreement, then waivers are given but sometimes waivers don't really help the customers fulfilling their losses. Security policies and implementation of SLA is also discussed in this conducted research. However, there is legal action, if any customer will any cloud service.

Chapter 3
PRESENT WORK

3.1. PROBLEM FORMULATION

Cloud computing predictably poses novel challenging security threats for number of reasons. Firstly, due to loss of control of data under Cloud Computing environment we can't just adopt traditional cryptographic primitives for the purpose of data security and protection and for the explicit information of the entire data verification of correct data storage in the cloud must be conducted to check whether data is getting stored at right place or not. The problem faces during the confirmation of correct storage becomes even more challenging due taking in consideration of various kinds of data for each user stored in the cloud would be stored safely and the stipulate of long term continuous guarantee of data safety.

Secondly, Cloud Computing is not just a third party data warehouse. Frequent updating like modification, insertion, deletion, appending and reordering, etc are being done by cloud users in order to ensure storage accuracy .New solution are provided by dynamic feature of data assurance and all traditional integrity insurance techniques like distributed techniques are considered as unsuccessful over dynamic data support of cloud environment. In order to provide redundancies and guarantee in data reliability facility in file distribution scheme used to avoid making any kind of data updating once data has been stored. New dynamic invent reduces the communication and storage overhead as like obsolete redundancy based file distribution mechanism .To assure accurate coded data , guarantee of data correctness and reassurance of simultaneous localization of data errors, i.e., by using similar kinds of token are user on both server and user side with distributed verification method for detecting the misbehaving server(s). With latest method we get supports for performing secure and efficient dynamic operations on data blocks like: deletion of data, update and append. This proposed technique provides high resistance against malicious data altering attack and even server colliding attacks with their security analysis and widespread. In this work, we will augment the proposed technique to isolate zombie attack in cloud computing architecture.

3.2. SCOPE OF STUDY

Cloud computing is a novel technology and a distributed environment which incorporates on-demand consumption to shared pool of resources, virtualization, open source software, and internet delivery of wide range services for users. The deployed architecture Cloud consists of on-premise and cloud different resources, middleware, services, and software components, reallocation etc by defining relationship between then and properties of those are also refers as proving credentials of a virtual system in cloud computing architecture. Due to this mobility will be increases and users can access the information from anywhere. This facility of cloud computing had liberated-up IT giants who may have been occupied for performing factions like, installing, updates and patches or involving in application support for too long. Cloud users can take benefit of as many resources they want in the form of services by paying for them in order to use but there are some security issues which make users unbalanced regarding the efficiency, safety and reliability in cloud computing. In this work, we will work on to isolate zombie attack in cloud architecture. The zombie attack will degrades the network performance to large extend. In this work, new technique will proposed which isolate zombie attack and detect malicious VM machines are responsible to trigger zombie attack.

3.3 OBJECTIVE

The main objective of this research is to propose an enhanced mutual authentication in which firstly user will authenticate virtual server to get connect with it by asking for some credentials which will authenticate server. This authentication mechanism will be based upon unique identification number which will be assigned to both user and server, before the start of communication with the user. If the virtual machine will able to hand over its credentials to users then only massage exchanges will be developed in that case, if user will not be served with those credentials then in that case virtual machines would be malicious i.e attacked by zombie attack will be detected and will be isolated by separating that particular victim virtual server from whole cloud network.

1. To study and analyze various security vulnerabilities in cloud architecture.

2. To analyze various schemes proposed to isolate zombie attack in cloud architecture.

3. To propose enhancement in mutual authentication based scheme to isolate zombie architecture in cloud computing.

4. To implement proposed and existing mutual authentication scheme in simulated environment.

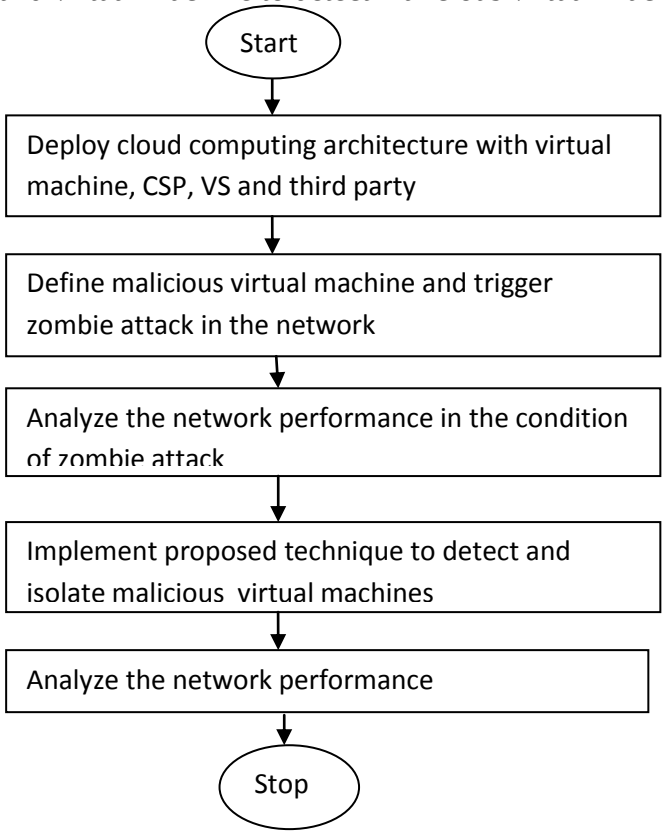
5. To analysis the results graphically of proposed and existing scheme.

3.5. RESEARCH METHODOLOGY

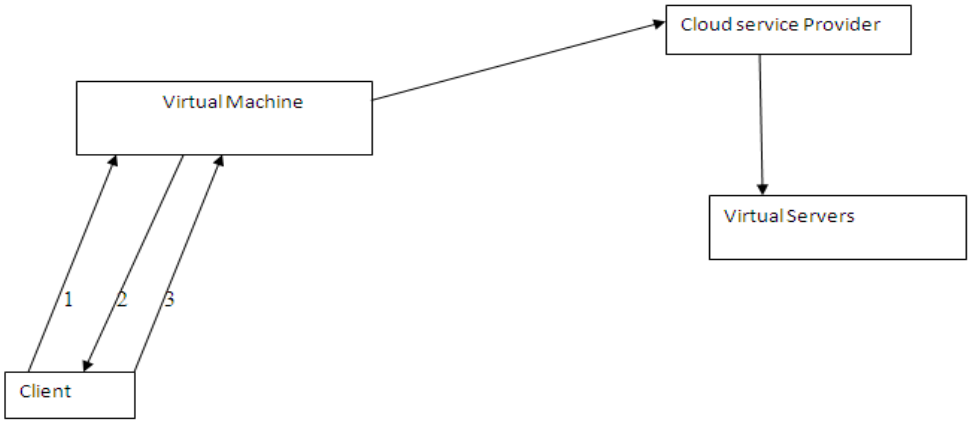
The software architecture contains various components like virtual servers, cloud services providers, virtual machines and third party. In order to encrypt data on the behalf of user and provide to cloud service provider which uploads the data to virtual server is responsibility of virtual machines which are considered as the trust able parties of the user. If virtual machines are malicious then zombie attack will be triggered in the network in that particular virtual machine. The zombie is the denial of service attack and it reduces the efficiency of the cloud architecture by not forwarding authentication user's request to access resources. In this work, zombie attack will be isolated and malicious virtual machines are detected from the cloud architecture. The proposed technique will be based on the **mutual authentication mechanism**. In this technique

- Unique number
- OTP (one time password)

will be assigned, before start of communication with the user. The machine will able to present it credentials to users. The massage exchanges are also developed in this work, between third party and virtual machine to detect malicious virtual machines.



Firstly we will deploy cloud architecture with all its components like virtual machine, cloud service provider, trusted third party and virtual servers. Malicious virtual machine i.e victim of zombie attack would be defined to trigger the zombie attack .A virtual machine will be a malicious if ifs not fulfilling use's authentication requirements ,that user will ask to server before the start of communication. Then we analysis would be



done to check the network performance in the condition of zombie attack where victim virtual machine is not able to forward user's request to cloud service provider. Afterwards proposed technique will be implemented to detect and isolate malicious virtual machines and again analyze the network performance after implementing new technique solutions.

Step 1: To verify the identity of the server there message exchanges are required. The procedure of message exchange is defined in the algorithm.

While designing this algorithm, let us take some assumptions.

1. The client presents its virtual ID's to the virtual machine.

2. The clients original ID is stored on the virtual machine and virtual machine knows both virtual, MAC address and clients original id.

Step 2: Message exchange between client and virtual machine, if the virtual machine is legitimate then the followings steps are followed in the algorithm:

1. Client sends its Mac address and its virtual id to virtual machine, with the nonce value.
2. When virtual machine receives, the message it will verify the credentials, if the credentials are verified.

3. Virtual machine send it's ID, clients original ID and nonce timestamp , its MAC address
4. If the client verified its originals ID and virtual machines ID
5. Then communication will start between client and virtual machine

Step 3. If the virtual machine is illegitimate, then following steps are following:

1. Client send its Mac address and its virtual id to virtual machine, with the nonce value
2. When virtual machine receives, the message it will verify the credentials ,if the credentials are verified
3. The virtual machine send, its ID, clients original Id and nonce stamp, MAC address
4. The client will not verify its original Id and virtual machines id
5. The communication will halt and fake virtual machine will be detected on its MAC address.

Chapter 4

RESULTS AND DISCUSSION

4.1 TOOL:

The proposed technique will be implemented in MATLAB. Matlab (short for Matrix Laboratory) is a idiom for technological computing which was developed by the The Math works, Inc. It provides a single platform for computation, visualization, programming and software development. All problems and solutions in Matlab are articulated in notation used in linear algebra and essentially involve operations using matrices and vectors.

4.2 PROBLEM IMPLEMENTATION:

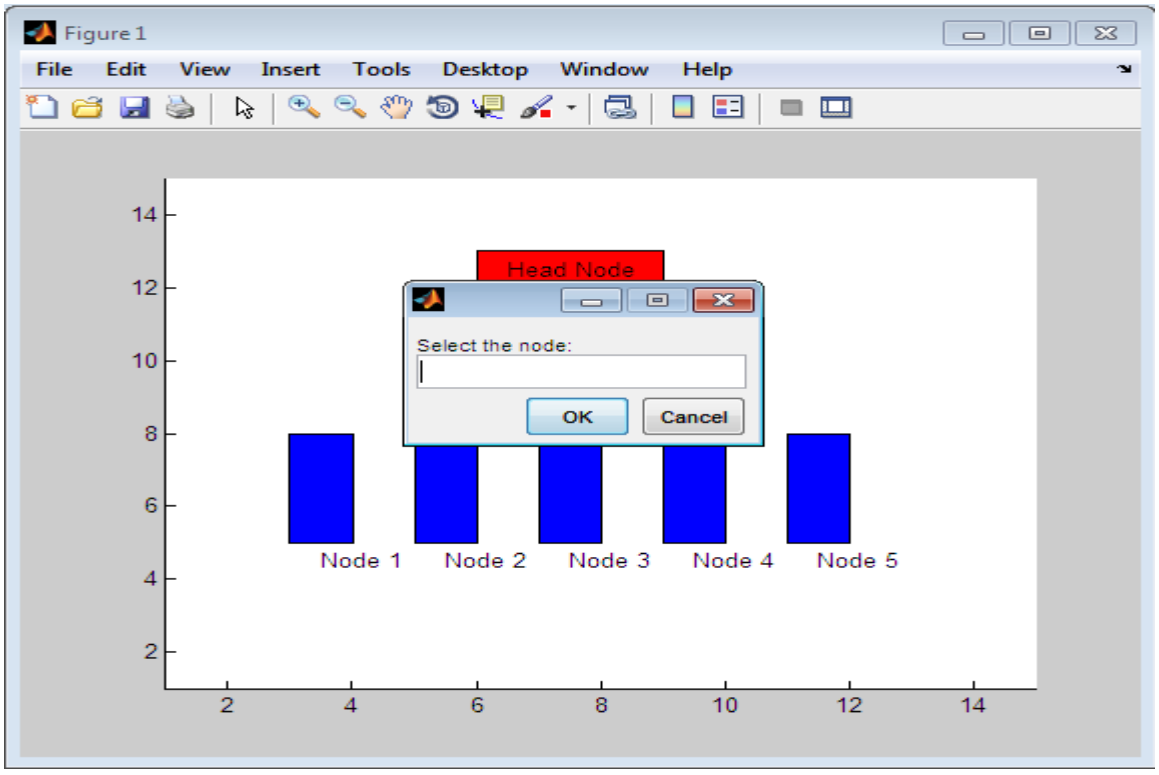


Fig 1. The cloud network is deployed with the fixed number of user and cloud service provider. In this figure the user will enter the user with whose it wants to communicate

using mutual authentication scheme where both cloud service provider and user authenticate each other before the start of communication.

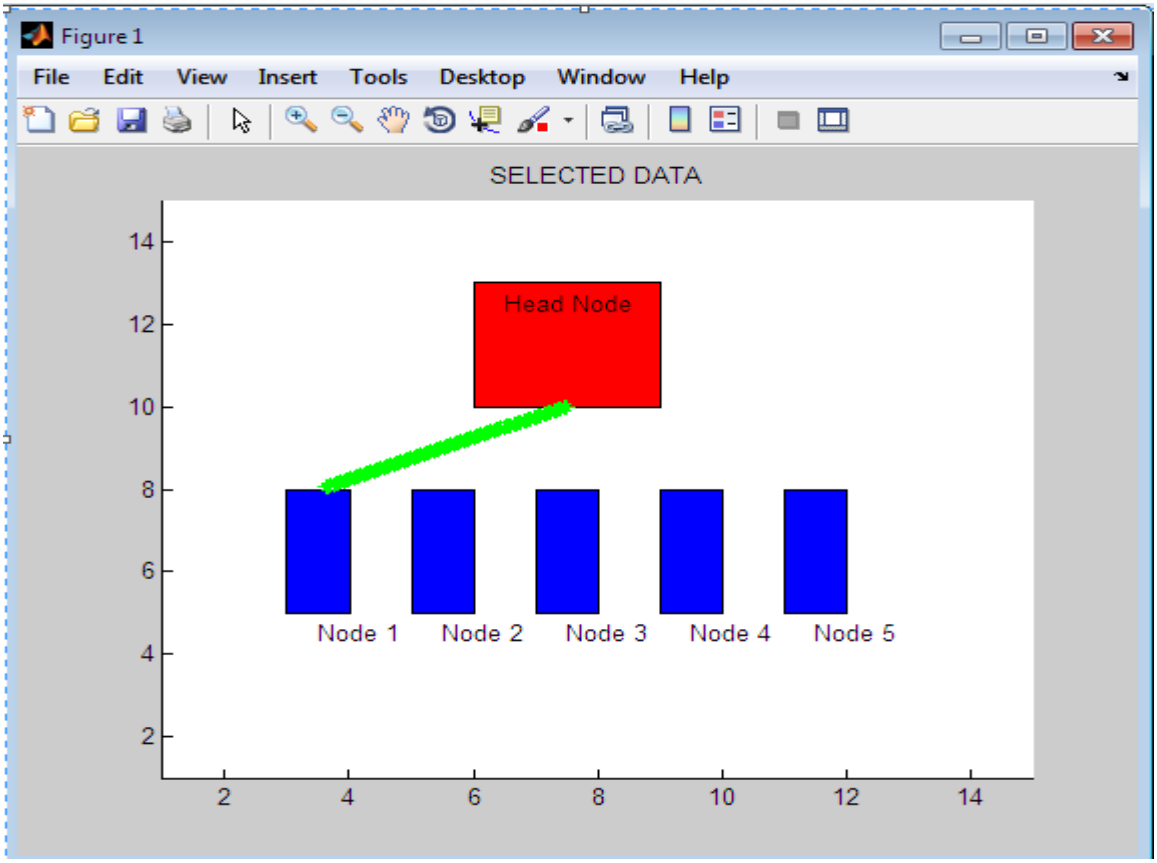


Fig 2: Keys are exchanged between cloud service provide and user for authentication. These keys should be same otherwise no communication will take place and whole process of authentication will start over. If keys are same, user and cloud service provider starts communicating.

Problem: If keys exchanged during mutual authentication will be detected by attacker then zombie attack can take place where multiple duplicate nodes will be created by attacker which will act as legitimate users and reinstate the data transfer between authenticated user and cloud service provider .When a user want to communicate,

attacker replace its identity and itself act as legitimate user. Now data transfer by node will go to attacker's account instead of cloud service provider.

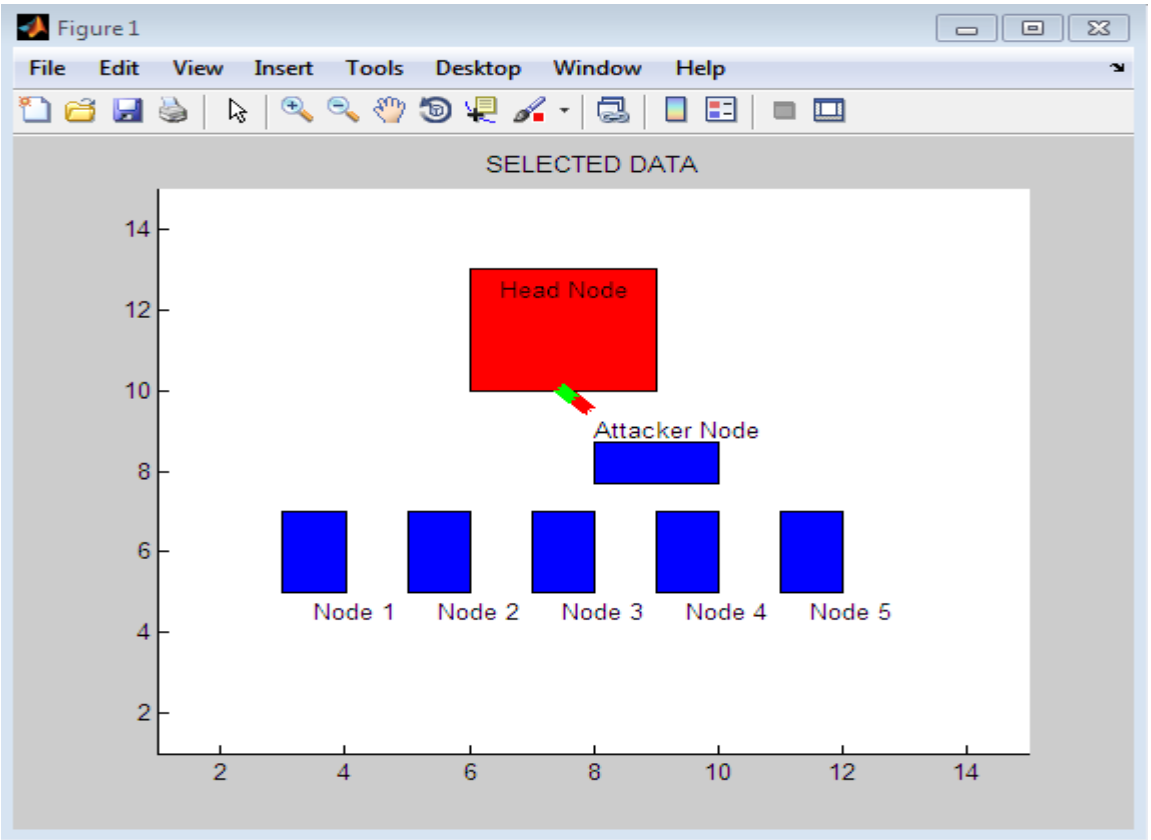


Fig 3. Here zombie attack take place and a duplicate node is created which is acting like a authenticated like other nodes and whenever a user want to communicate ,this attacker replace user's identity and itself act as that user .Now communicate will take place between attacker and cloud service provider. Cloud thinks that it's communicating with legitimate user but data goes to attacker's account instead of users.

Outcome: Communicating should be between legitimate user and cloud service provider but due to zombie attack, communication is broke and started with attacker. This is how

zombie attack is detected when user's data reaches to attacker instead of cloud service provider.

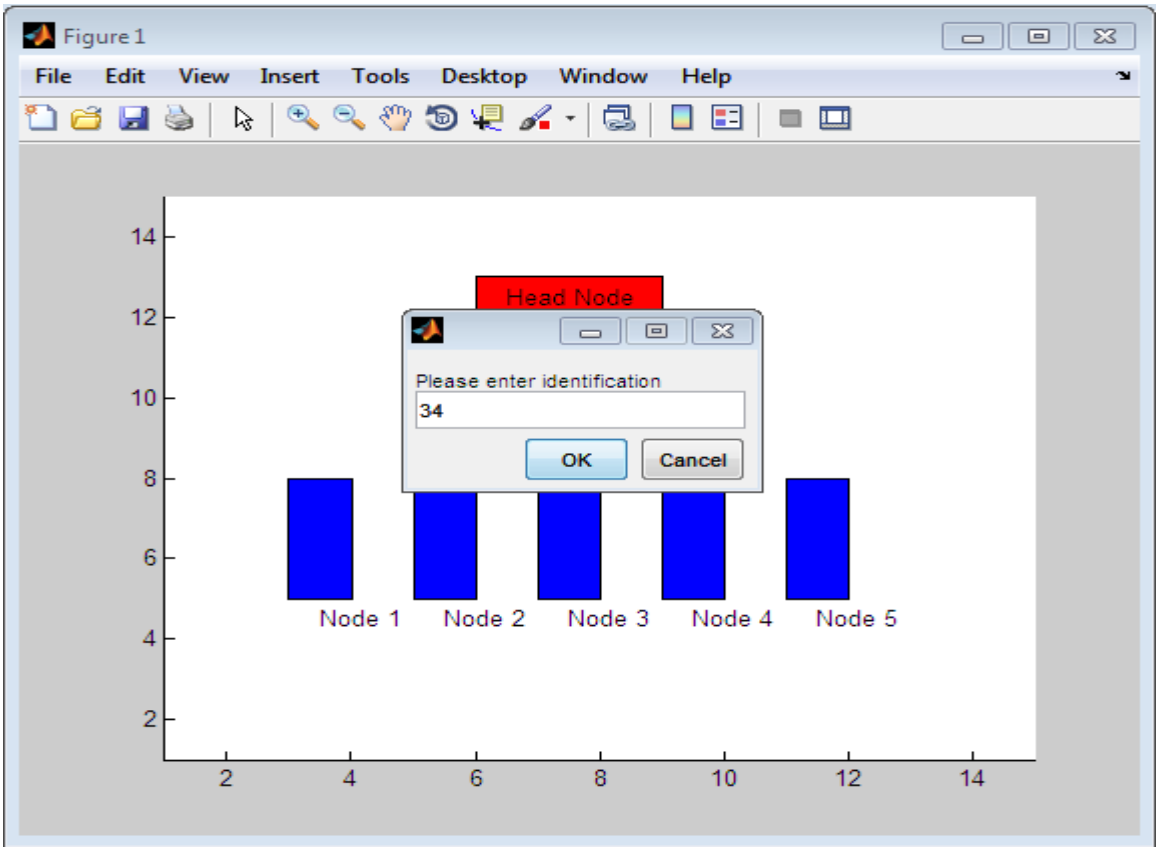


Fig 4.In order to isolate zombie attack for cloud, mutual authentication is enhanced in which some more authentications requirements such as

- Identification
- MAC address
- IP address

Firstly key is exchanged then identification, MAC address and IP address is asked from user and being sent to cloud service provider which encrypt these things using its private key and generate an identification id and send to user. Then user decrypts its identification id using its own private key and sender's public key.

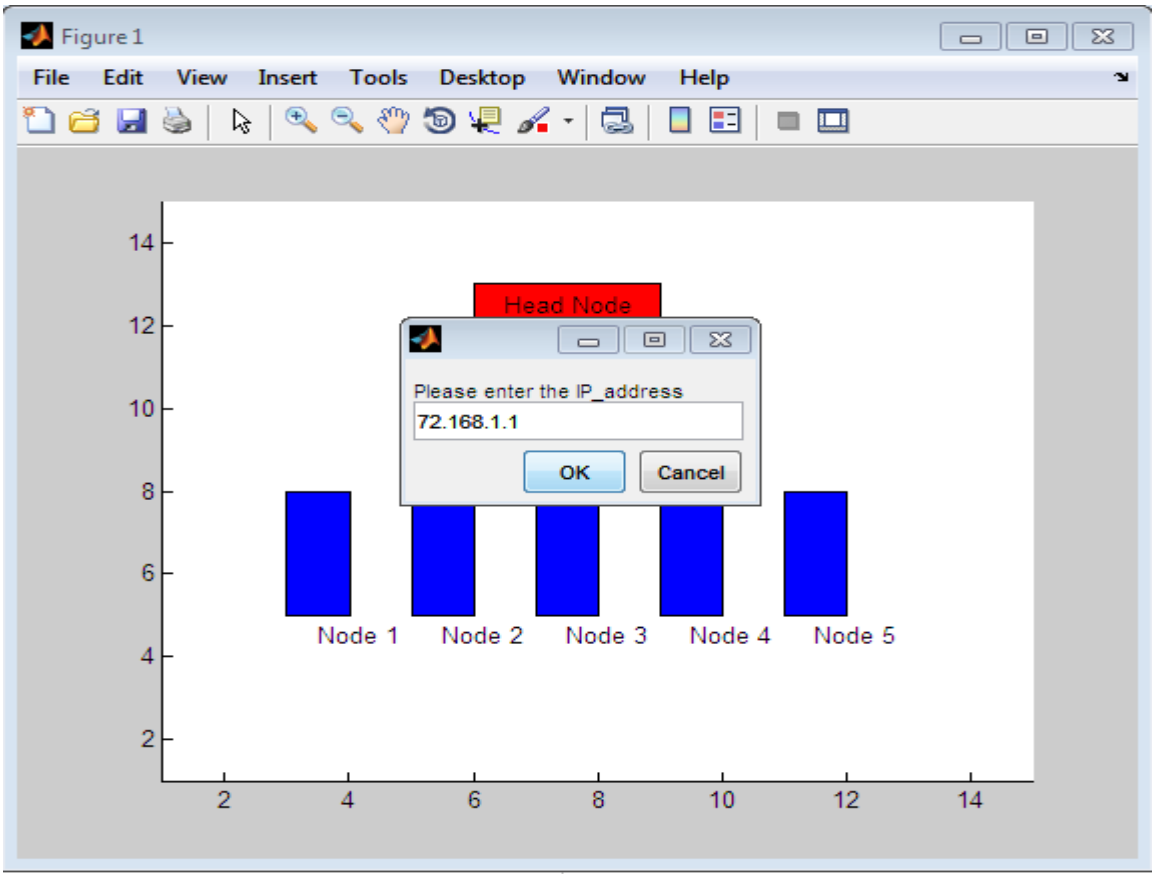


Figure 1
File Edit View Insert Tools Desktop Window Help
Head Node
Please enter the IP_address
72.168.1.1
OK
Cancel
Node 1
Node 2
Node 3
Node 4
Node 5

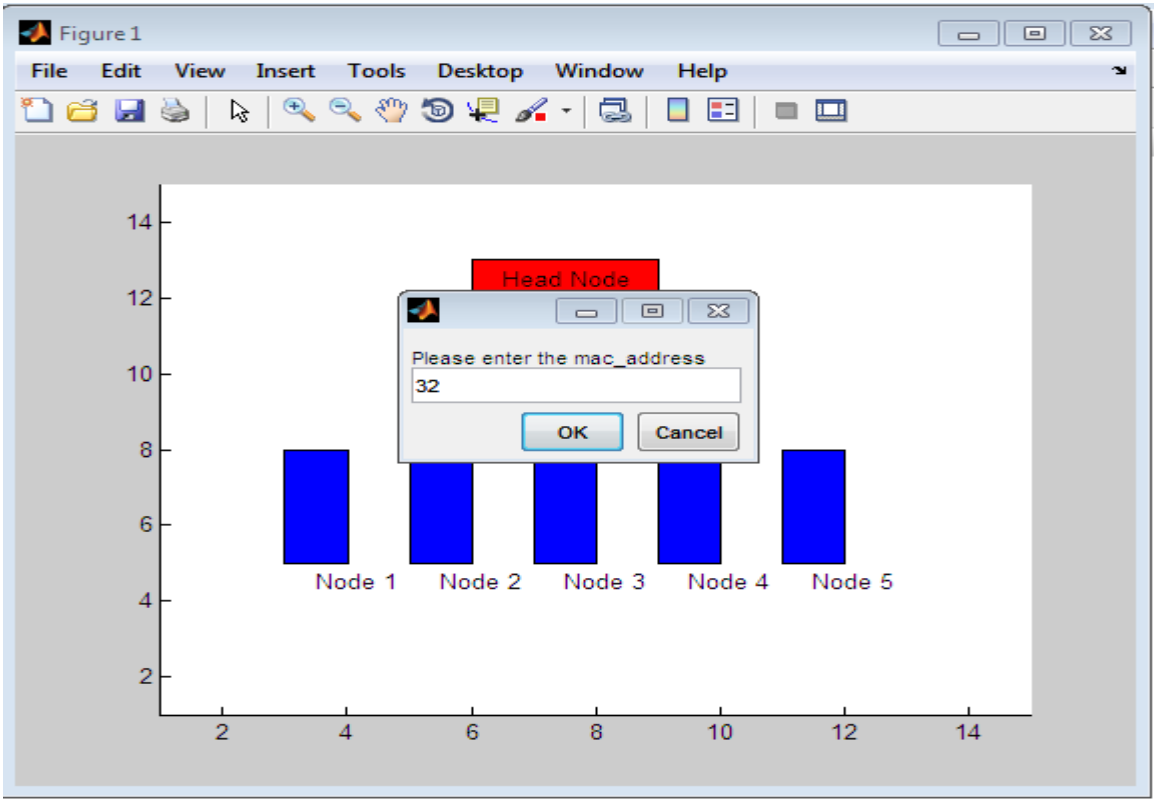


Figure 1
File Edit View Insert Tools Desktop Window Help
Head Node
Please enter the mac_address
32
OK
Cancel
Node 1
Node 2
Node 3
Node 4
Node 5

Fig 5 and Fig 6: In these figures IP address and identification number and MAC address is provides and then general identification id is generated by cloud service provider and encrypt it using own private key and user's public key and transfer it to user.

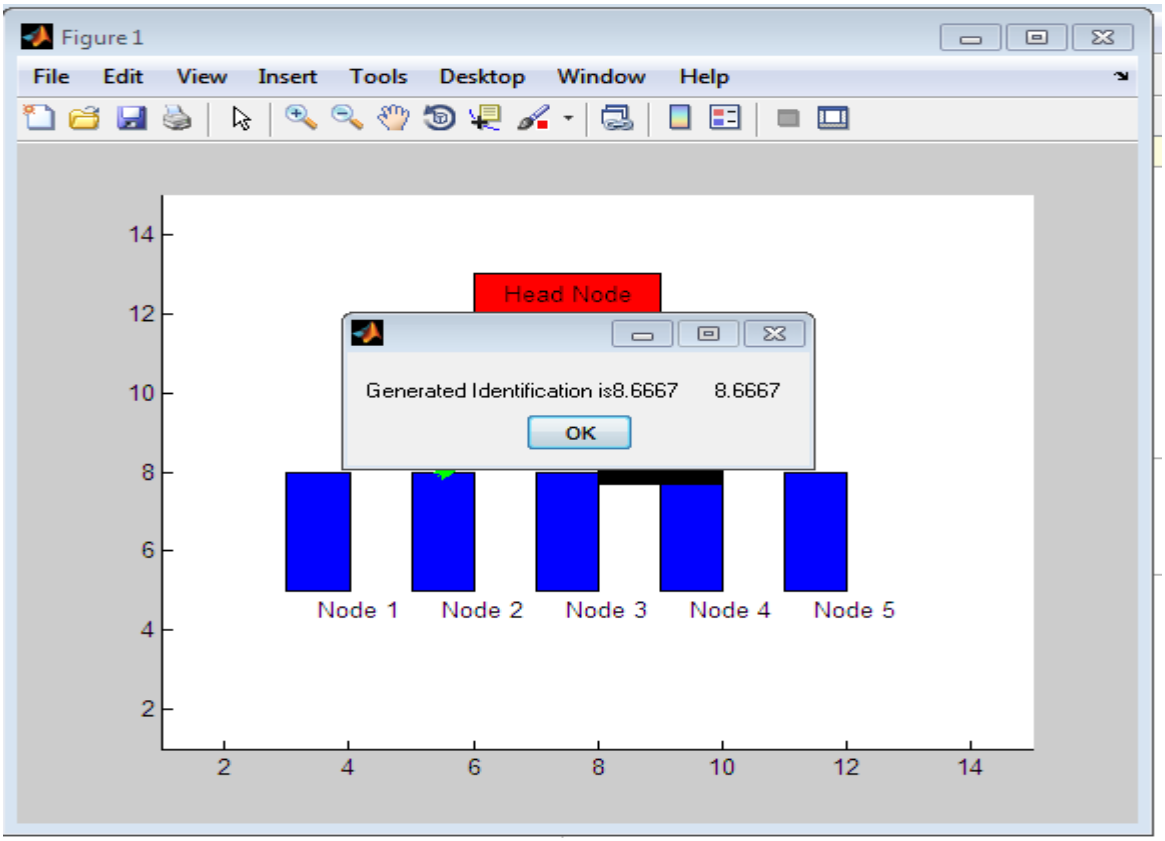


Fig 7. This general identification number is sent to user but it is received by attacker and unfortunately attacker doesn't have cloud's public and its own private key to decrypt that general identification. By this way cloud service provider will came to know that user it is communicating with is not legitimate.

Outcome: Zombie attack is detected with the use of enhanced mutual authentication scheme.

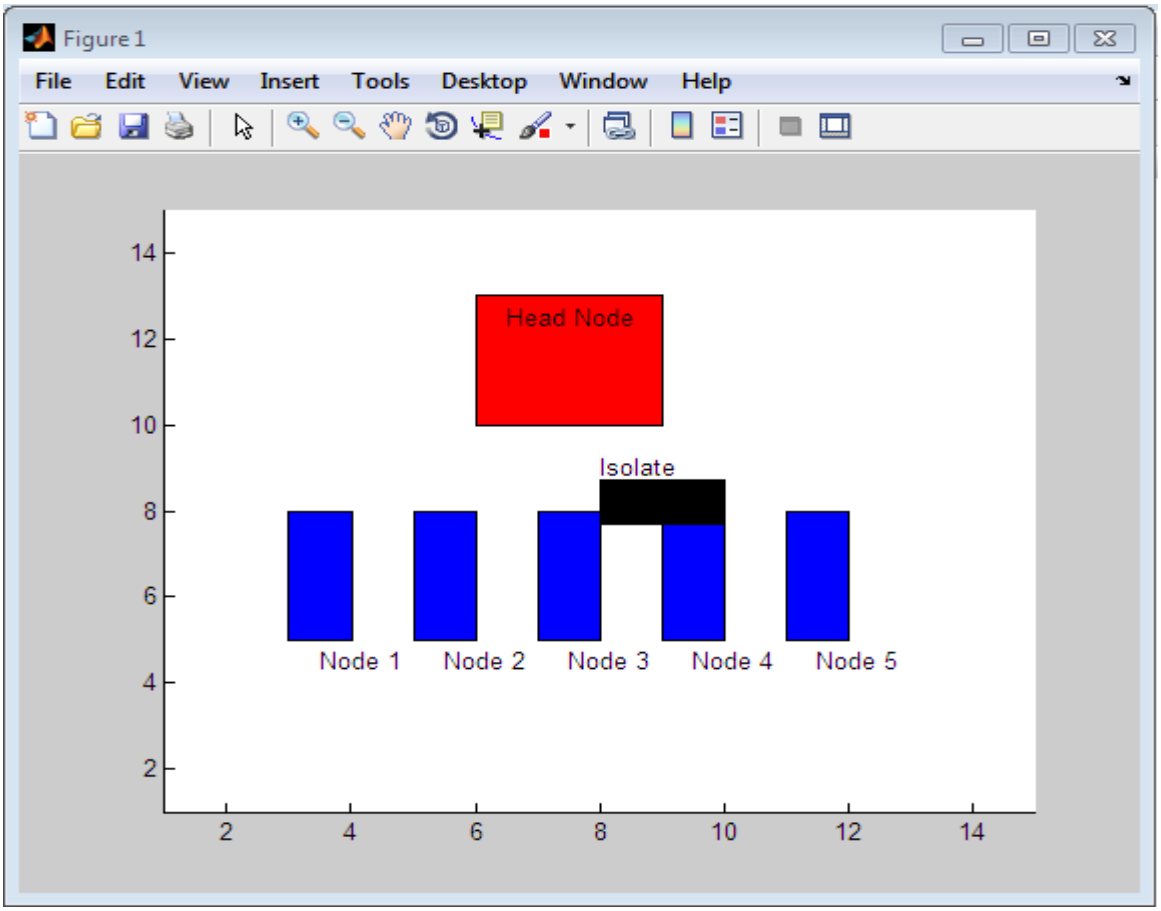


Fig 8: Zombie node is detected and isolated from cloud.

Outcome: The encrypted message is generated and it will be transferred to the user. The user will revert back the generated identification to the cloud for the verification. But attacker wouldn't revert back because it doesn't have any key to decrypt. So cloud service provider will come to know that node is not legitimate so it isolated that attacker's node from cloud environment by this way.

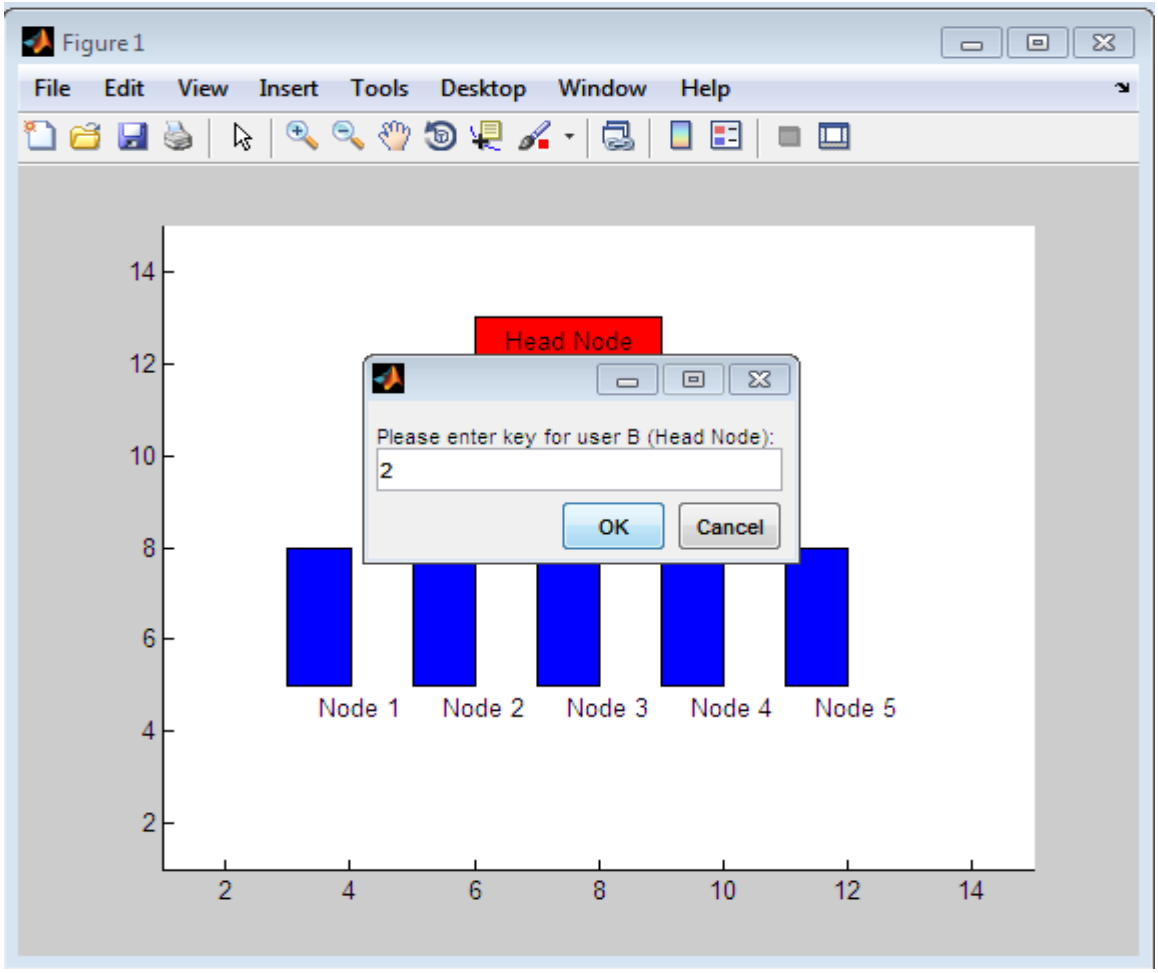


Fig 9: The encrypted message is generated and it will be transferred to the user. The user will revert back the generated identification to the cloud for the verification. After detecting and isolating zombie attack from cloud we want to run cloud with enhanced mutual authentication environment. It will again ask to select node and key for user and cloud and after matching keys , MAC address ,IP address and identification will be provided and being sent to cloud for encryption.

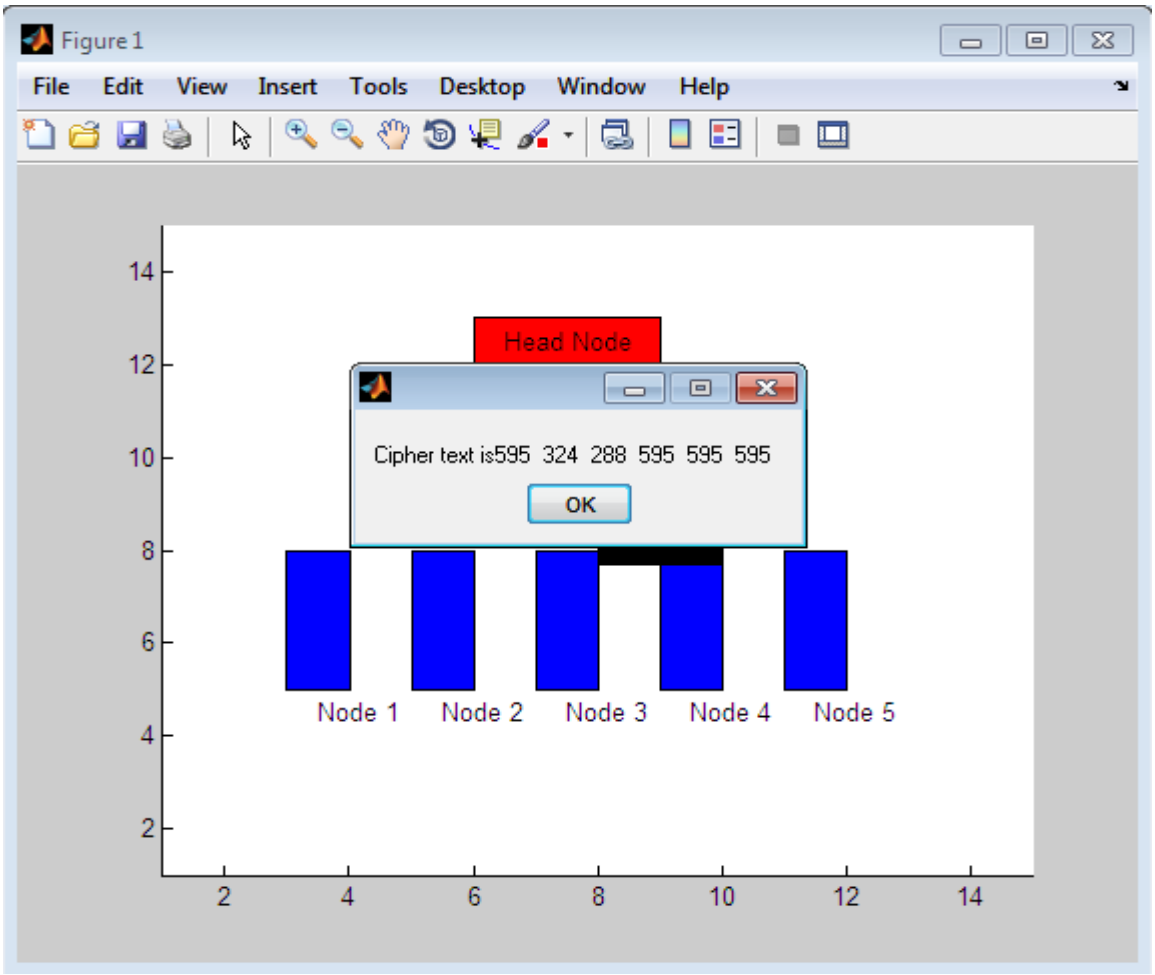


Fig 10. After detecting and isolating zombie attack from cloud we want to run cloud with enhanced mutual authentication environment. It will again ask to select node and key for user and cloud and after matching keys , MAC address ,IP address and identification will be provided and being sent to cloud for encryption. Cipher text is generated by cloud by encrypting user's credentials and send it back to user for verification.

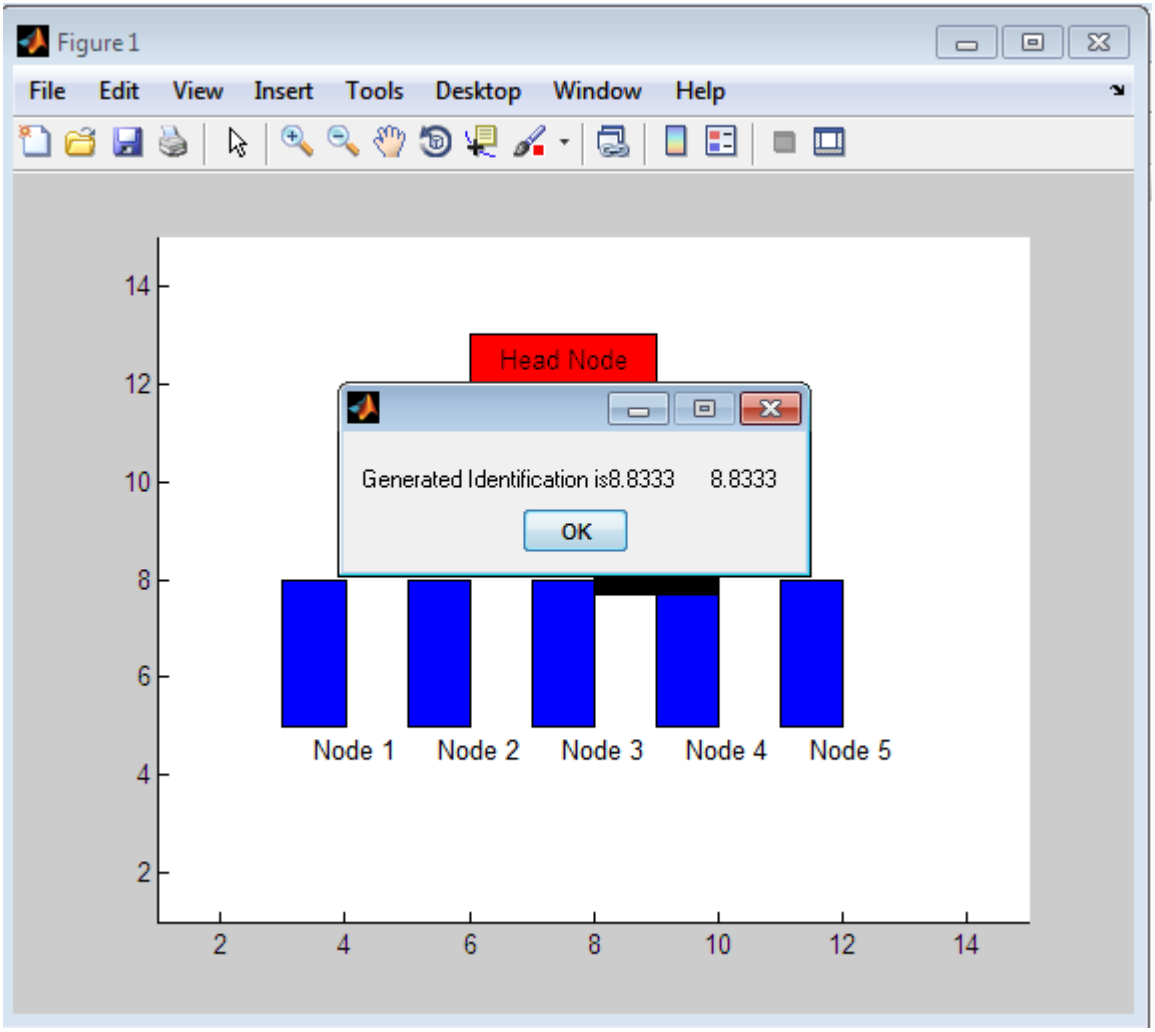


Fig 11 : General identification number will be general by cloud after encrypting MAC address , IP address and identification number with its private key and send it back to user who will decrypt its private key and cloud's public key. Only after the user decryption that data communication will start.

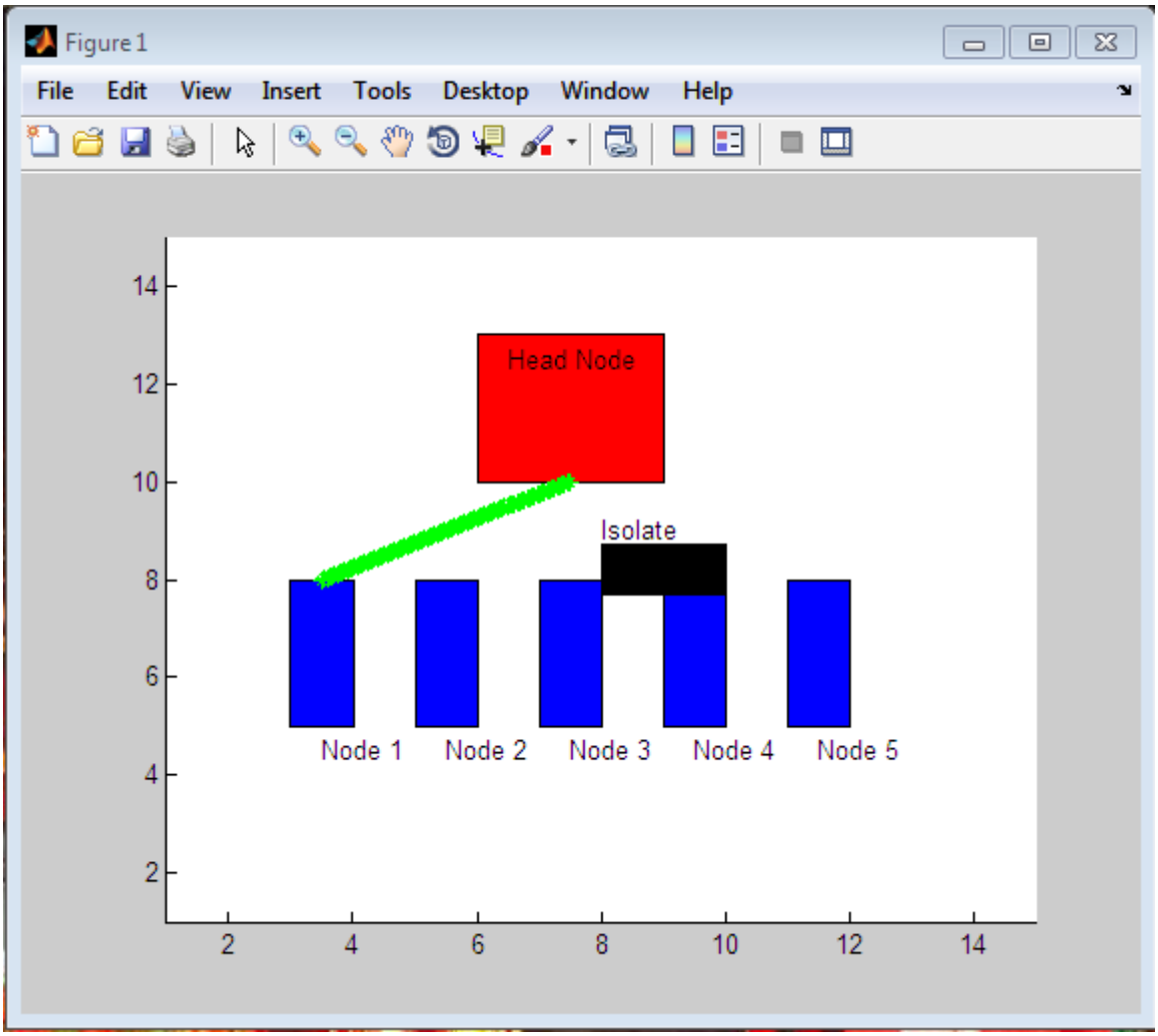


Fig 12: After detecting and then isolating the zombie attack from cloud environment, communication will take place between authenticated user and cloud service provider only.

Outcome: A secure cloud interface is provided using enhanced mutual authentication scheme which is being used to detect and isolate a zombie attack. Now there will be direct communication between user and CSP without nay intermediate duplicate node.

4.3 OUTCOME:

Mutual authentication scheme is firstly enhanced which is further used to detect the zombie attack. As simple mutual authentication was not appropriate enough to avoid zombie attack because say key is used by user and cloud and that key can be easily hacked by attacker so some more identification is added as MAC address, IP address and identification is provided by user for its identification and send it to cloud server which encrypts these identification means with user's public key and is own private key and generate a general identification and send it back to user. Then user decrypts it using its own private key and cloud server's public key. If it matches with cloud general identification only then communication will start. But attacker don't have genuine private key so when it decrypt the general identification with fake key, it won't be match with cloud general identification and from here zombie node will be detected and isolated.

- Various security attacks in cloud architecture were analyzed and then zombie attack is focused and analyzed.

- There are various schemes which were proposed to isolate zombie attack in cloud architecture and mutual authentication is one of them.

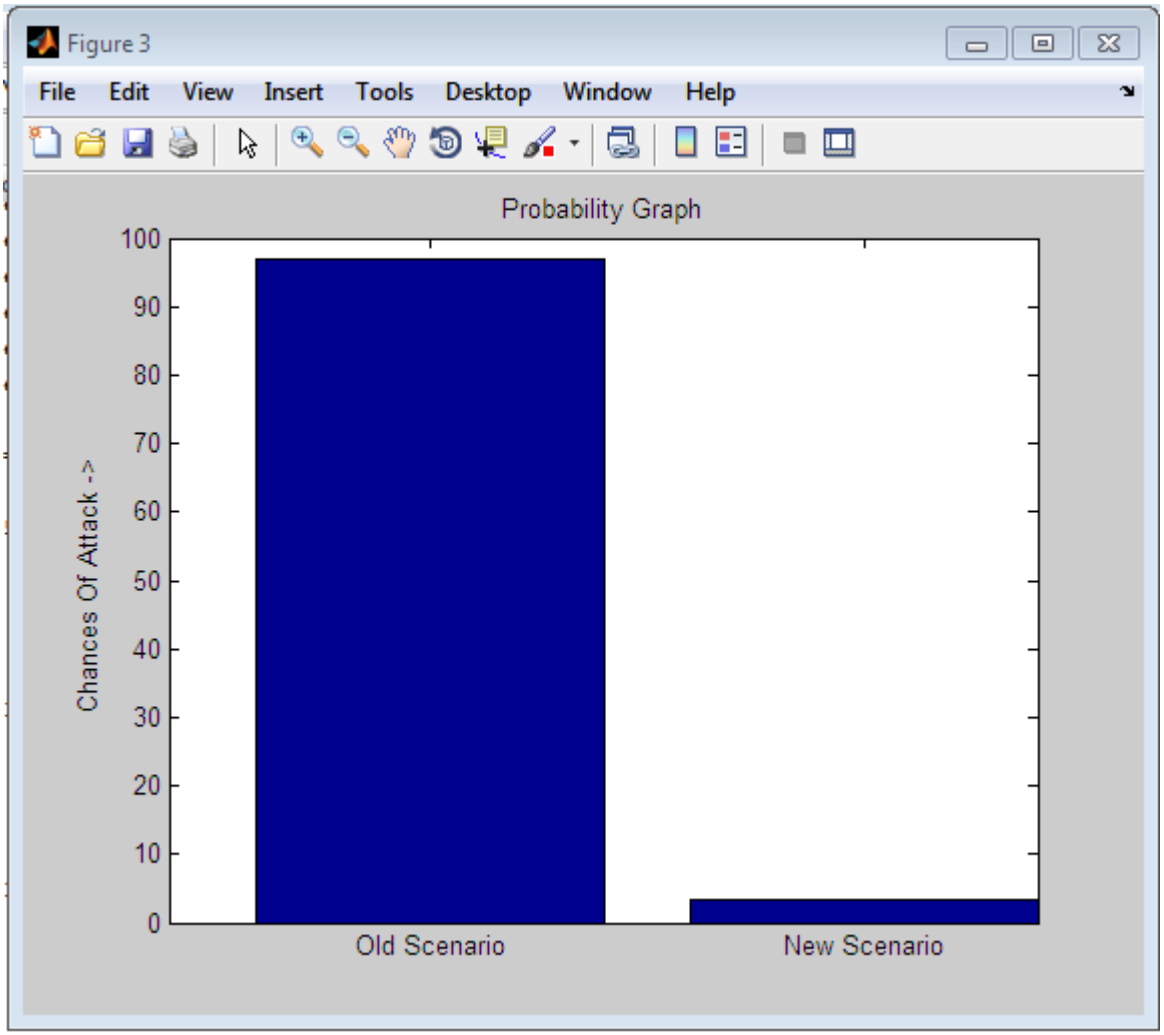
- Mutual authentication based scheme is enhanced to isolate zombie architecture in cloud computing by adding some more identification is added as MAC address, IP address and identification.

- Proposed enhanced mutual authentication and existing mutual authentication scheme are implemented in simulated environment where zombie attack was firstly triggered and then was detected using enhanced mutual authentication and isolated from cloud environment.

- Results of proposed enhanced mutual authentication and existing mutual authentication are determined graphically to analyze the difference in performace.

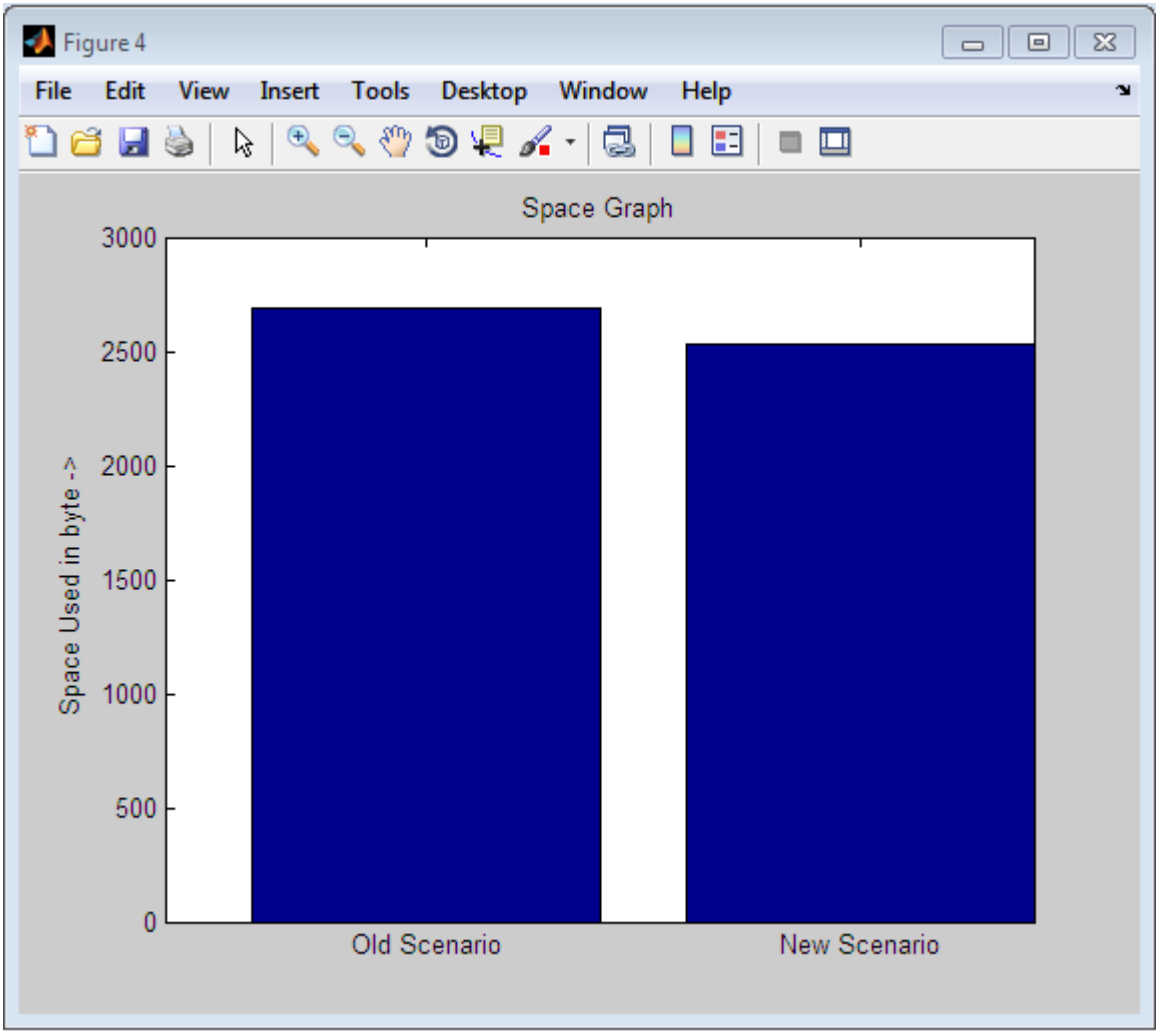
4.4 GRAPHS:

1. In this probability graph chances of attack compared between old scenario i.e mutual authentication and new scenario i.e enhance mutual authentication.



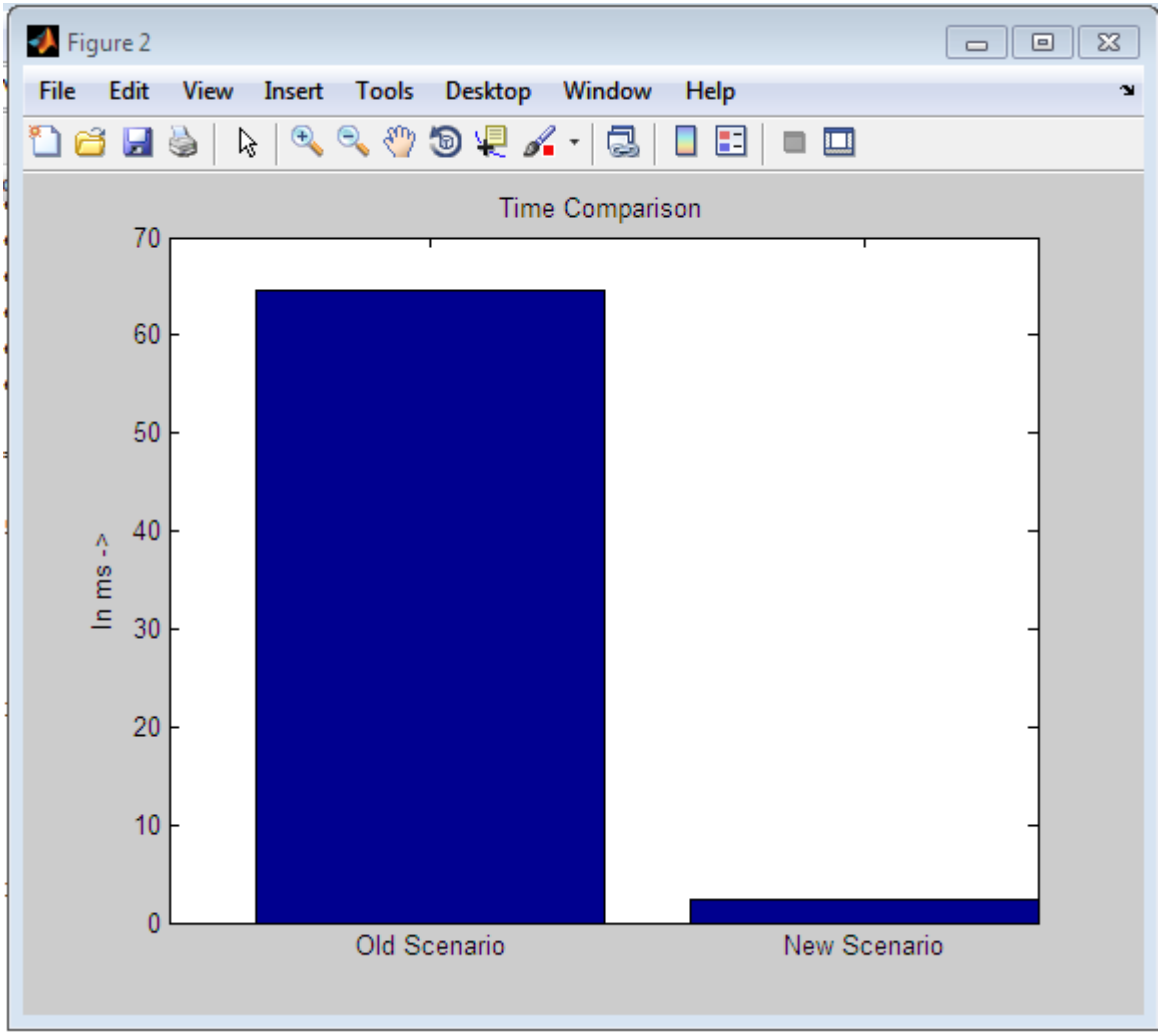
Chances of zombie attack are very less in case of enhanced mutual authentication scheme as wide variety of authentication parameters are applied ,which are being used to detect the attack at very early stages before it make a virtual machine a malicious one. On contrary chances of zombie attack are very high in old scenario because it was almost impossible to detect and isolate attack, only we can face is dealing with a malicious virtual machine without our knowledge.

2. This space graph is about the space being used in bytes during authentication process of user and cloud.



Space graph is about the space being used in bytes during authentication process of user and cloud. We can see that space used during proposed mutual authentication is little bit smaller than being used in existing authentication scheme.

3. This time graph show time in milliseconds (ms) in old as well as in new scenario of authenticating user and cloud server.



Time taken to authenticate user are cloud during enhanced mutual authentication scheme is quite less than that of existing authentication scheme, with this speed will be increased and hence performance will be.

Enhanced mutual authentication gives much better performance when we compared it with existing authentication scheme under parameters such as chances of attack, time taken during authentication process and space required. So, performace of cloud will be increased to a great extent with the use of enhanced mutual authentication scheme for the detection and isolation of zombie attack.

Chapter 5

CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION: Cloud computing is an internet based computing which provides us a shared pool of resources. Depending on physical server's storage of different service providers, multiple virtual systems are being created depending upon storage capacity of provider's system. When user request for the access of that virtual machine, then virtual machine is being provided to it by service provider, but what if that virtual machine got compromised by some attacker and it's not forwarding the user's request to access resources and finally leads to unavailability of services for authorized user's. This virtual system unavailability is vulnerable to zombie attack which will reduce the efficiency of the cloud architecture. We have detected malicious virtual machines from the cloud architecture and isolated zombie attack also. Mutual authentication mechanism is be used as existing technique which is later enhanced and used to avoid and isolate the attack if already happened. To get rid of the attack user will verify whether the server is legitimate or not before the start of communication with the user. The machine will able to present it credentials to users such as Mac address, IP address and identification number. User and virtual machine exchanged these credentials in order to detect and isolate malicious virtual machines.

5.2 FUTURE SCOPE:

This enhanced mutual authentication can also be used be side channel attack where attacker can easily gain secret information when a virtual machine fails by then placing a new VM with targeted VM and extract confidential information from targeted VM on same physical machine. Enhanced mutual authentication scheme is used to verify the authenticity of new virtual machine.

Chapter 6
REFERENCES

[1] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013) "An analysis of security issues for cloud computing"2013

[2] Jian Yu, Quan Z. Sheng, Yanbo Han (2013) "Introduction to special issue on cloud and service computing" 26 April 2013

[3]V.Nirmala, R.K.Sivanandhan, and DR. R Shanmuga Lakshmi(2013) "Data Confidentiality And Integrity Verification Using User Authentication Scheme In Cloud" Proceedings Of 2013 International Conference On Green High Performance Computing.

[4]Virendra Singh Kushwah and Aradhana Saxena(2013)"A Security Approach For Data Migration In Cloud Computing"International Journal Of Scientific And Research Publications, Volume 3, Issue 5,May 2013

[5] N.S. Sudharshan, Dr. K. Latha ,"Improvisioning Seeker Satisfaction in Cloud Community Portal:Dropbox", International conference on Communication and Signal Processing, April3-5,2013,India.

[6] Pradnyesh Bhisikar , Prof Amit Sahu ,"Security In Data Storage and Transmission In Cloud Compituing,International Journal Of Advanced Research In Cloud Science And Software Engineering,IJARCSSE,March 2013

[7] Joel Gibson, Darren Eveleigh, Robin Rondeau and Qing Tan (2012) "Benefits and Challenges of Three Cloud Computing Service Models"2012 IEEE

[8] Mohammed A. AlZain #, Eric Pardede #, Ben Soh #, James A. Thom* (2012) "Cloud Computing Security: From Single to Multi-Clouds" 2012 45th Hawaii International Conference.

[9]Anas BOUA Y AD, Asmae BLILA T, Nour el houda MEJHED, Mohammed EL GHAZI (2012) "Cloud computing : security challenges"2012 IEEE.

[10] Ravi jhawar, Vincenzo Piuri,Fellow,and Macro santanbrogio(2012)"Fault tolerance management" 2012 IEEE.

[11] Mohamed Hamdi(2012) “Security of Cloud Computing, Storage, and Networking” 7/12.2012 IEEE

[12] Huaglory Tianfield(2012) *“Security Issues In Cloud Computing”* 2012 IEEE October 14-17, 2012.

[13] *Wentao Liu*(2012) “ *Research on Cloud Computing Security Problem and Strategy”* 2012 -3/12/2012 IEEE

[14] Jaidhar C. D(2012) “Enhanced Mutual Authentication Scheme for Cloud

Architecture” 29-3/12.2012 IEEE

[15] Alexandru Iosup, Simon Ostermann,Nezih Yigitbasi,Radu Prodan,Thomas Fahringer, and Dick Epema(2010) *“Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing” 2010* IEEE TPDS, MANY-TASK COMPUTING, NOVEMBER 2010

[16] Balachandra Reddy Kandukuri,Ramakrishna Paturi V,Dr. Atanu Rakshit(2009*) “Cloud Security Issues”* 2009 IEEE International Conference on Services Computing.

[17] “Types of clouds” www.techgyd.com Fig 1

[18] “Service Models” blog.appcore.com Fig 2.

[19] “DDOS attack” Sanjoli Singla, 2009 Fig 3

[20] “Man in the middle attack” Young-Gi Min,2012 Fig 4

[21] “Mutual Authentication” support.sas.com Fig 5