LOVELY PROFESSIONAL UNIVERSITY

TO ISOLATE THE VIRTUAL SIDE CHANNEL ATTACK IN CLOUD ENVIRONMENT

A Dissertation submitted

By

Hardeep Kaur

11304806

To

Department of Computer Science

In partial fulfillment of the Requirement for the
Award of the Degree of

Master of Technology in Computer Science & Engineering

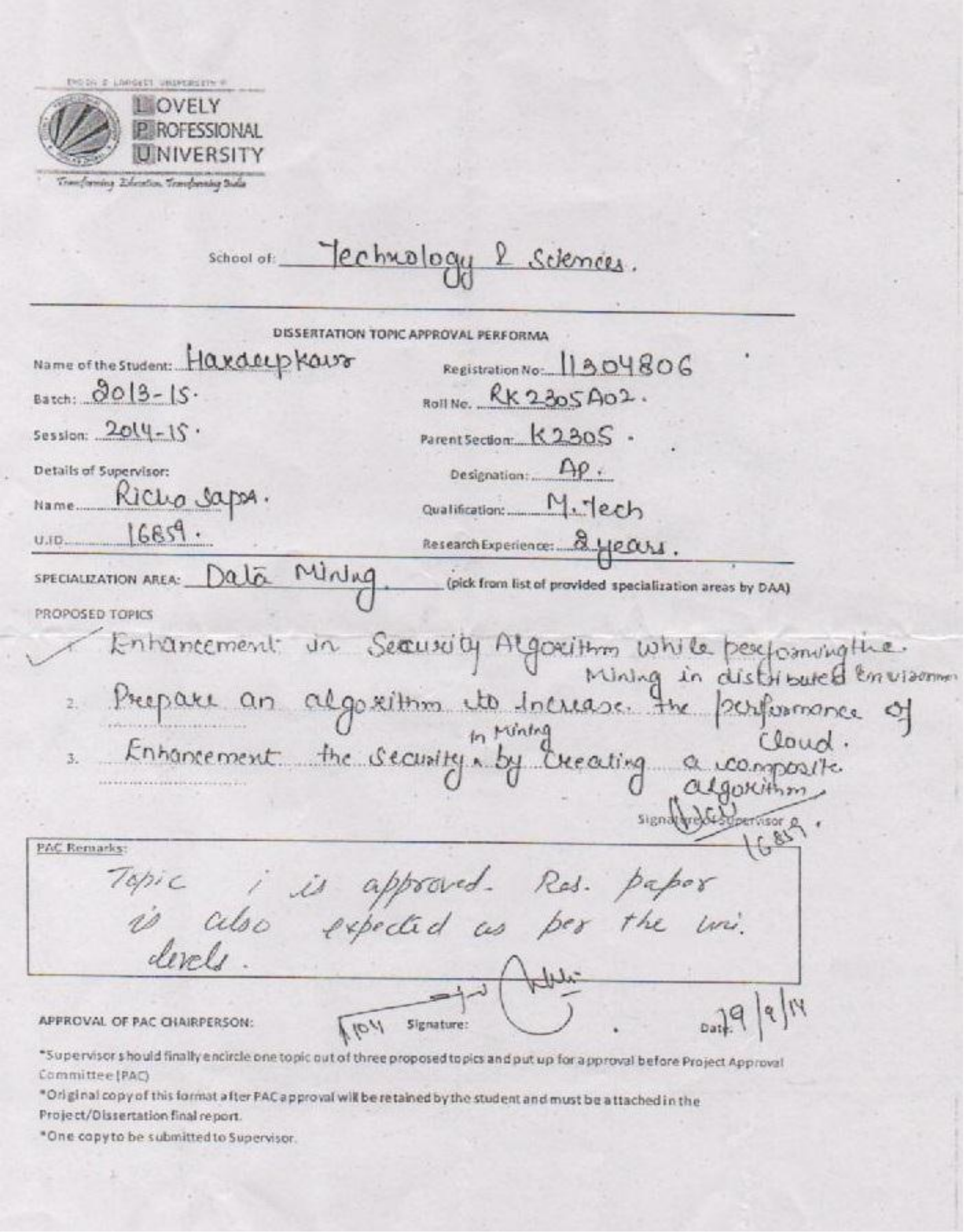
Under the guidance of

Manjit Kaur

(Assistant Professor, Lovely Professional University)

(April 2015)

PAC FORM



LOVELY
PROFESSIONAL
UNIVERSITY
Transforming Education Transforming India

School of: Technology & Sciences.

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Hardeep Kaur
Registration No: 11304806

Batch: 2013-15.
Roll No. RK2305A02.

Session: 2014-15.
Parent Section: K2305.

Details of Supervisor:
Designation: AP.

Name: Richa Sapra.
Qualification: M.Tech

U.ID: 16859.
Research Experience: 2 years.

SPECIALIZATION AREA: Data Mining. (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Enhancement in Security Algorithm while performing the Mining in distributed Environment ✓
2. Prepare an algorithm to increase the performance of Cloud.
3. Enhancement the security in Mining by creating a composite algorithm.

Signature of Supervisor
16859.

PAC Remarks:

Topic 1 is approved. Res. paper is also expected as per the uni. levels.

APPROVAL OF PAC CHAIRPERSON: Signature: Date: 29/9/14

*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

When data mining is used with cloud computing, security and privacy of user's data and information is very important. Though Cloud Computing has many advantages, it still faces many security and privacy issues. A user may loss his data due to malware attack or network outage. Cloud gives provider an opportunity to analyze user data for a long period. Also the outside attacker can analyze and access the data and violate the user privacy by managing to get access to the cloud. As cloud computing allows virtual resource sharing, and sharing of resources among potential tenants can increase the risk of information leakage due to vulnerability of virtual resources, causing side channel attacks. An access control policy such as RBAC can be used to control the data sharing among cloud customers. But, an unintelligent cloud resources management mechanism can significantly increase the risk of data leakage among roles. An attacker place a virtual machine and all the traffic of the legitimate user will directed to the attackers virtual machine. A novel technique is proposed to isolate the side channel attack in Role-Based Multi-Tenancy Access Control Scheme. The proposed technique gives better result than the previous technique in the form of network performance.

CERTIFICATE BY ADVISOR

This is to certify that she has completed M. Tech dissertation proposal titled ' To isolate the virtual side channel attack in cloud environment' under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any degree or diploma.

The Dissertation is fit for the submission and the partial fulfillment of the conditions for the award of M. Tech Computer Science & Engineering.

Date: _______________ Signature of Advisor

Name:

UID:

ACKNOWLEDGMENT

I take this opportunity to express a deep sense of gratitude towards my guide Asst. Prof. Manjit Kaur, for providing excellent guidance, encouragement and inspiration throughout the work. I would like to thank her for his constant assistance and overwhelming interest in the research that has made it successful. I express my deep sense of gratitude and appreciation towards her. Without his invaluable guidance, this work would never have been a successful one.

I would also like to thank my family and friends who have been a source of encouragement and inspiration throughout the duration of this research.

HARDEEP KAUR
(11304806)

DECLARATION

I hereby declare that the dissertation proposal entitled **'To isolate the virtual side channel attack in cloud environment',** submitted for the M.Tech(Computer Science and Engineering) degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: Investigator

Registration no. 11304806

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF GRAPHS

CHAPTER 1

INTRODUCTION

1.1 DATA MINING

One of major problem today is that we are data rich but information poor. A large amount of data is collected on daily basis and analyzing such data is important to gain knowledge. Data Mining turns a huge amount of data into valuable information.

The Data mining is known as knowledge discovery in Database i.e. KDD, knowledge extraction, mining knowledge from data, data archaeology, data dredging, business intelligence etc. Data mining discover the useful patterns through large volume of data. Data Mining is defined as a "type of database analysis that attempts to discover the useful patterns, trends or hidden relationships in a group of data.

KDD is a process of obtaining information. Data Mining is not a synonym of KDD; it is only one of stage of it. Data Mining is very useful in different areas such medical and science, finances, commerce, marketing, telecommunications, metrology, agriculture, bioinformatics etc.

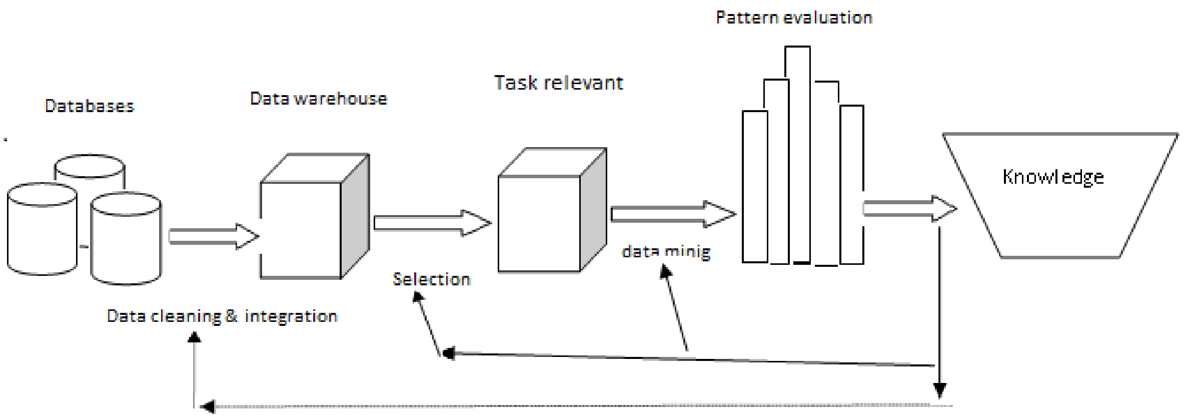


Fig.1.1 KDD Process

1) **Data selection:** data is retrieved from database which is relevant for analysis.
2) **Data preprocessing:** data cleaning, data integration and selection are done.
3) **Data transformation:** performing summary and aggregation operations, data is transformed into appropriate form.

4) **Data mining:** data is extracted by applying some methods.
5) **Evaluation:** identify the patterns representing knowledge and mined knowledge is provided to user.
6) **Knowledge presentation:** virtualization and knowledge representing methods and techniques are applied to represent a mined knowledge.

1.1.1 DATA MINING IN CLOUD COMPUTING

In Cloud Computing Data Mining applications and techniques are very useful in these days. Cloud Computing is a great area in which data mining can works as it is very much desirable. It needs to be concentrated by data mining as it becoming more powerful in all fields of business and scientific computing.

Cloud computing depends on cloud servers for handling the various tasks. Data mining can be used in cloud computing to extract the structured and valuable information from unstructured or semi-structured data sources obtaining from the web. In Cloud Computing, data mining permits the enterprises to integrate the management of software and data storage resources, with guarantee of efficient, trustworthy and secure services for the consumers. Data mining techniques are implemented over cloud computing. It allows consumers to get valuable information from the virtually integrated data warehouse.

1.2 CLOUD COMPUTING

Cloud computing is a biggest-scale computing paradigm which is focused by economies of scale. It is a pool of managed computing power, dynamically scalable, virtualized, abstracted, platforms, pool of storage and services are delivered on request of customers through internet. Cloud computing is internet-based computing, where different services as servers, storage and applications are provided to an organization or individual customers.

Cloud computing provides on demand and convenient access of the network to the computing resources like storage, servers, applications, network and other services in efficient way. User, client or organization which is using the cloud service has to pay for what he is using. For example, Drop box is cloud service which can be used by free account or premium account users.

Cloud computing allow their customers to put and get their information and data into cloud. The customer got different types of services from cloud through internet. When users use a

cloud service, they saw virtual view. In cloud data and services are distributed at different locations. As the cloud is based on the web service and web service is based on the internet.
Internet has its own security weakness. As it is open and it has many attacks and threats. Thus cloud services faces big range of security problems but there are also many security technologies available to resolve security issues.

Cloud Computing can be described as "a type of Internet-based computing," where different services such as servers, storage and applications are delivered to an organization's computers and devices through the Internet".

Cloud computing focuses on sharing the information and computations over network of nodes which are scalable. E.g. the nodes include end user and Web Service, data centers. Theses network of nodes forms as a cloud. The main idea is to use the infrastructure in order to bring all feasible services to the cloud and to make it possible to access those services irrespective of time and location [9].

1.2.1 SERVICE MODEL

The three service models of cloud computing are:

1) **Software as a Service:** applications are developed and hosted on clouds. Without the need of installing any program or software on user's computer, it supports user interaction with the applications. On the demand of user, an application is offered to a user as a service by cloud service provider. Multiple users are serviced by running a single instance of a service. User also does not need any software license. User also has not need to spend money on software. On the other hand, for provider it costs very less because single application is needed to be managed and it hosts many users. E.g. salesforce.com.
2) **Platform as a Service:** It allows the users to build applications by delivering the services like development tools, platforms where user can also run their applications. User can deploy and run software over cloud computing infrastructure via programming languages, libraries, services and with the tool that are supported by provider. The expenses on this model are lowered. It does not need to manage any software or hardware which needs for building an application. E.g. Google app engine, windows Azure.
3) **Infrastructure as a Service:** It provides storage and computing capabilities as standardized services. In IaaS storage systems and servers are integrated or pooled

together. To handle the workload these resources are managed properly and made available to customers. In this customer can deploy his software. E.g. amazon web services [10].

1.2.2 CLOUD DEPLOYMENT MODEL

The main deployment model of cloud computing are:

1) **Public Cloud:** infrastructure and services are provided off-site over the internet. It can be access by anyone and can access the cloud storage.it is more vulnerable to security attacks. It is executed and managed by a third party. Cloud service provider owns the infrastructure. It based on pay per use and has a low cost.

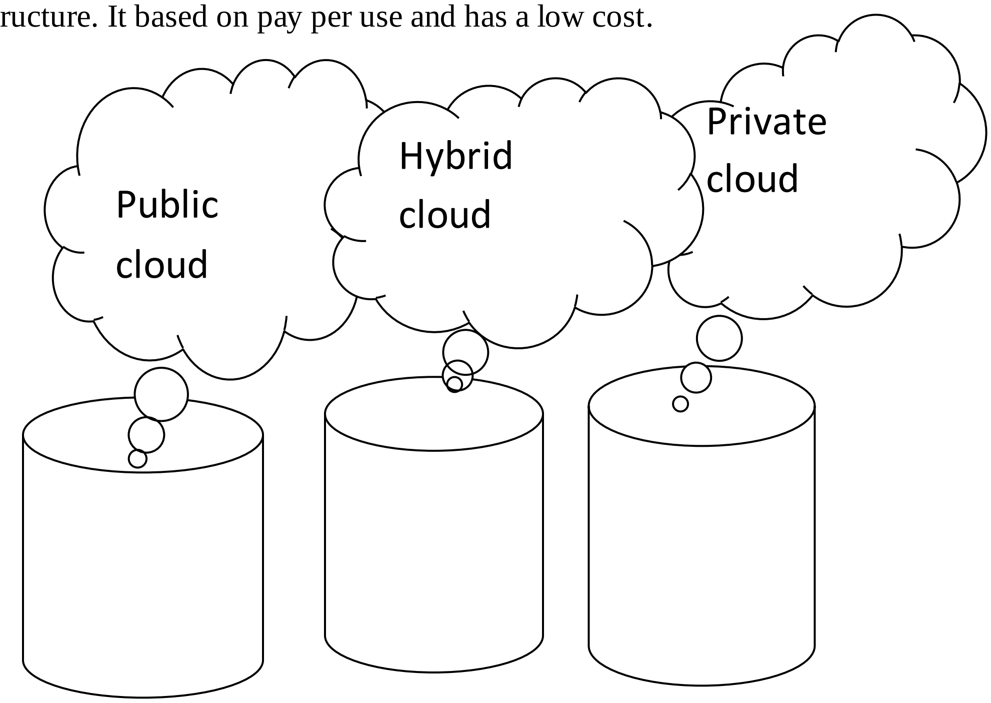


Fig. 1.2 Cloud Deployment Model

2) **Private Cloud:** it is also known as internal or enterprise cloud. In this infrastructure and services are handled by the private networks. It offers a high level of security. An organization or company purchase and maintains software and infrastructure and has more control over infrastructure. It also requires an expertise employee to manage it.

3) **Hybrid Cloud:** it is the combination of more than two deployment models e.g. public and private clouds. It can be managed by a third party or by the organization. It can be placed both an on-site or off-site locations. It helps to achieve high level of efficiency and scalability.

4) **Community Cloud:** Multiple organizations share and control this as it supports the users, who have a similar interest of area or work. A third party or the committee of owners can managed this deployment cloud [6].

1.2.3 CHARACTERISTICS OF CLOUD COMPUTING

1) **On-demand self-service:** user can request and manage the services from cloud whenever they need.
2) **Broad network access:** the services that are provided by the cloud and the data present at cloud must be accessible to the user over networks like internet from devices likes PC, laptops, tablets.
3) **Rapid elasticity:** the resources should be scaled as per user's demands.
4) **Resource pooling:** resources are shared by pooling in a multitenant environment among different customers.
5) **Virtualization:** cloud computing enhance the utilization by sharing of storage media and servers.
6) **Pay-per-use:** user pay for only what they are using. Users can see their usage and can also check how much they used and how much they have to pay.

1.2.4 SYSTEM MODEL

Three different types of network entities are:

1) **User:** users store the data on clouds. They use the clouds for data computations. It may be individual user or an organization.

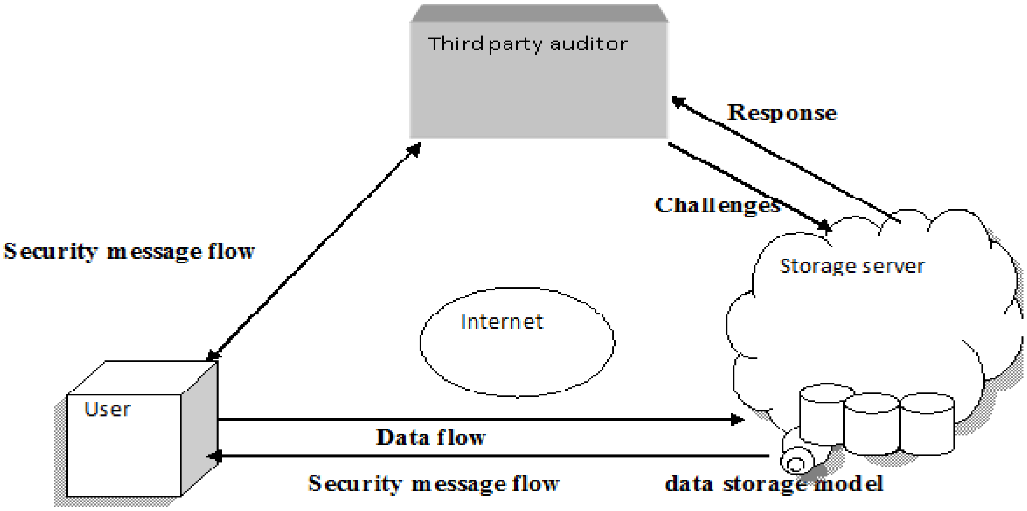


Fig. 1.3 Cloud Data Storage Model [21]

2) **Cloud service provider:** it has its own resources, infrastructure and expertise. It can build and manage the cloud storage.
3) **Third party auditor:** it is a trusted third party. User can request it to assess and expose the risk of cloud storage services. It has capabilities and expertise which a user might not have.

1.3 CLOUD COMPUTING SECURITY

Security is the main concern to every service. Security ensures the privacy and integrity of the data. The cloud security comprises the network security, information security and other security types like the computer security. Cloud security has set of technologies, policies and controls which are used to secure the application or data exist with the cloud environment. Cloud vendor may implement their own security policies. In any service there may be security loopholes and the security issues exist [13].

1.3.1 CLOUD THREATS

The main threats to data or information in cloud are:

Confidentiality

- Insider User Threats
- External Attacker Threats
- Data Leakage

Integrity

- Data Segregation
- User Access
- Data Quality

Availability

- Denial of Service Threat
- Physical Disruption

1.3.2 TYPES OF ATTACKER

An attacker can be divided into two groups:

Internal attacker: an internal attacker is employed by cloud service provider, user or third party organization. These attackers intentionally corrupt the user's information inside the cloud by deleting or modifying the information. It has authorized access to cloud services, user’s data and application. They are able to obtain all the data and may leak it to outsiders

External attacker: these are unauthorized parties from outside of the cloud. External attacker has the capabilities of compromising the cloud server and can modify and delete the user’s information and may disclose user private information.

1.4 CLOUD COMPUTING CHALLENGES

The major challenges in Cloud Computing are:

Security: security issues have main role in hindering the acceptance of cloud computing. Security issues like botnets, phishing poses serious threats to organization’s data. The features of cloud computing like multi-tenancy resource pooling also introduces new security challenges. E.g. use of cloud computing to organize botnets as it provides reliable infrastructure service at low cost to start an attack.

Data Privacy and Integrity: Cloud computing ensures cost economy and relieves users from managing infrastructure. The data in cloud is more vulnerable to risk in terms of confidentiality, integrity and availability.

Costing Model: Though cloud computing reduces the cost of infrastructure but the cost of communication is high as it includes the cost of transferring data to and from public or community cloud and cost of using resources.

Charging Model: pool of resources made the analysis of cost complicated as compared to regular data centers. Virtual machine also becomes the unit of cost analysis.

Service Level Agreement: SLA is vital to guarantee the cloud user for service delivery from provider. It covers user’s expectations and is simple to evaluated and verified. It is enforced by resource allocation on cloud. Different service defines different SLA Meta specification which increases the implementation problems for provider [15].

1.5 CLOUD COMPUTING ATTACKS

There are various potential attacks such as:

1) **Denial of Service (DoS) attacks:** Attacker send very large amount of packets from exploited information resources, called Zombie. It affects the availability of service for authorized users. DoS attack is possible in cloud as large no of users share it.

2) **Side channel attacks:** attacker can compromise the cloud through placing his virtual machine to the target cloud. Attacker forces a user to put his password and id to access information and thus security and information of users compromised.
3) **Authentication attacks:** it is a weakest point in virtual services and hosted. This attack is frequently used through different king of authentications. E.g. users can be authenticated based on what a person know, has, and is.
4) **Man in middle attacks:** it is a cryptographic attack. An attacker places himself between the two parties which are communicating. Attacker can capture the message and can modify it. If the communication is in unencrypted form then attacker can obtain any information from parties without letting them to know about it.

1.6 VIRTAUL SIDE CHANNEL ATTACKS

VIRTUAL MACHINE

It is a logical entity and behaves like the physical machines. Virtual machines execute programs like physical machine and shared the same hardware infrastructure. It is an operating system or software that runs application likes on a separate computer.

VIRTUAL SIDE CHANNEL ATTACK

In cloud computing, IaaS service model contains collection of infrastructure like virtual machines, computers, storage servers etc. it is possible to map the cloud infrastructure and where the target virtual machines are resides in network. An attacker compromised the cloud system through placing his malicious virtual machine to target system server. Attacker first map where the virtual machine is resides on the cloud and then attack by placing his virtual machine on target machine. Then attacker extracts the information from targeted virtual machine known as virtual side channel attacks [1, 14]. An attacker takes the advantages of physically shared components in order to steal information from victim. It has two steps:

1) Placement: placing malicious virtual machine on the same physical machine.
2) Extraction: getting information of user's data on targeted virtual machine.

As shown in figure1.4, cloud service provider is associated with the virtual servers bi-directionally for the purpose of storing user's information. It is also associated with the virtual machines. A no. of users are presented in the cloud network and associated with the virtual machine bi-directionally to exchange the information and data. A third party is also attached to virtual machines, users and cloud service provider for security purpose.

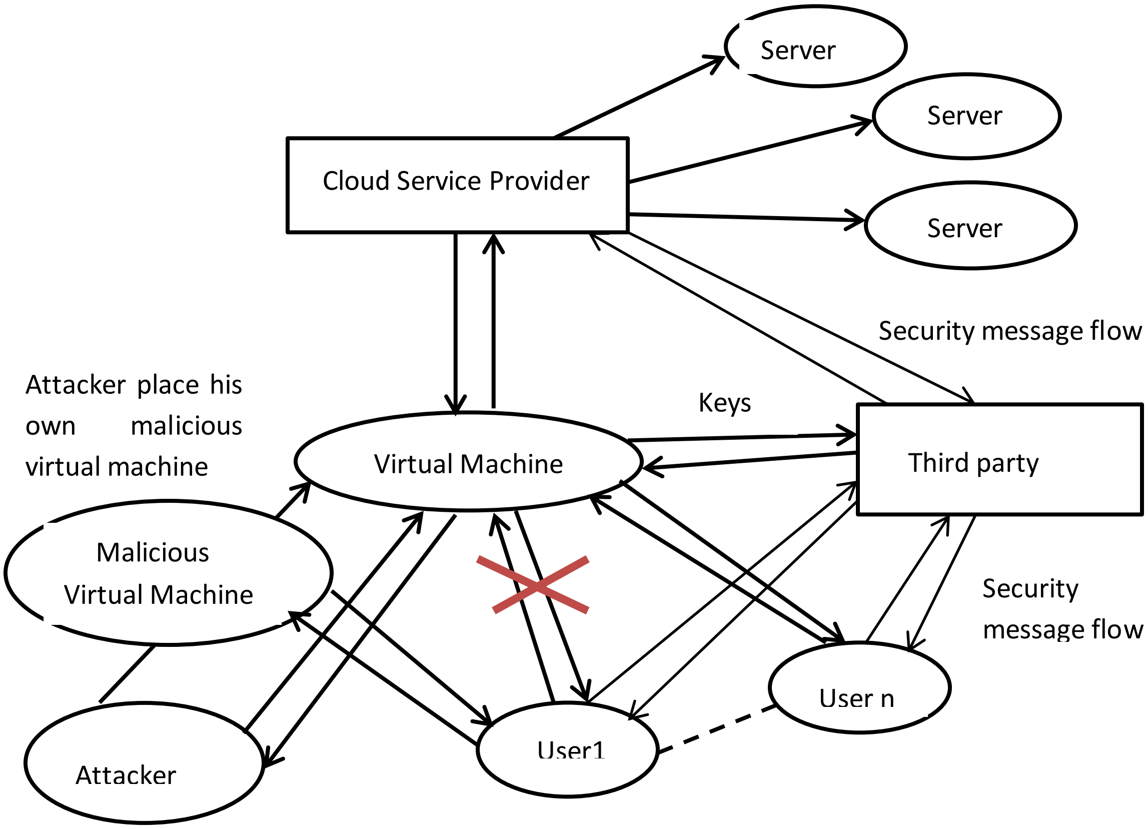


Fig. 1.4 Virtual Side Channel Attack

But there is also a user 3 which is attacker. This attacker first of all associated with legitimate virtual machine and as a response this virtual machine gives credential to the attacker or we can say attacker steal credential from legitimate virtual machine. Now user 3 force user 1 to link up new virtual machine which is similar to legitimate user. When User1 associates with legitimate virtual machine, its information goes to attacker i.e. user 3. This is called virtual side channel attack.

1.6.1 CLASSIFICATION OF SIDE CHANNEL ATTACKS

It is of two types:

INVASIVE vs. NON-INVASIVE: Invasive attacks require de-packaging the chip to get direct access to its inside components. E.g. the connection of a wire on the data bus to see the data transfers. A non-invasive attacks only exploit the information like running information time and power consumption. Non-invasive attacks are undetectable. These attacks are usually of low cost to set up on large scale from economical point of view.

ACTIVE vs. PASSIVE: active attacks try to tamper with the devices' proper functioning. While passive attacks will observe the device behavior during their processing without disturbing it.

1.7 MULTI-TENANCY IN CLOUD COMPUTING

Multi-tenancy is the very important feature of the cloud computing in which, multiple tenants are served through a single instance of software application runs on sever. As the same application is shared by multiple users but users can't see and access the data of other users. It is required to decrease the cost, to improved security and providing privacy to users by isolating their data.

TENANT

Tenant is a group of users who share the same deployment model. Tenant can use the same computing resources and applications which are provided by the cloud service provider.

MULTI-TENANT DATA

In multi-tenancy, multiple-tenant's data can be stored in independent databases which provide complete isolation with high cost, in one database with separately schema or with identical schema.

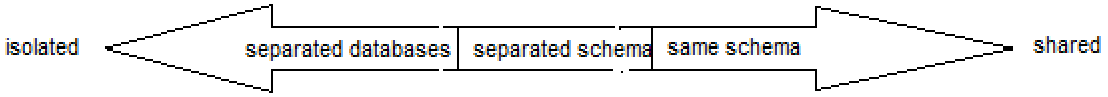


Fig. 1.5 Managing Multi-tenant Data

1.7.1 MULTITENANT DEPLOYMENT MODES FOR APPLICATION SERVER

1) Tenants accessing application running on dedicated server.
2) Tenants accessing application running on different virtual machines.
3) Tenants accessing application running on same virtual machines.

1.8 MANAGEMENT ACESS CONTROL, AUTHENTICATION AND ID MANAGEMENT

The many techniques have been proposed for access control. . Cloud needs user based access control method, where every customer can request to any service provider. User is bounded with the user id and entitlement data information.

Role based access control is the efficient and reliable technique for Access Control methods. In the Role Based Access Control method, the user can prove its identity to cloud service provider through the secure authentication procedure. User id will have attributes or identifiers that find and define the user. There should be a strong Identity Management and authentications for the client and the cloud provider [25].

1.8.1 ACCESS CONTROL CHARACTERISTICS IN CLOUD

The main four layers of conceptual categorization [8]:

1) **Entropy layer:** applications are providing to the users as a set of services. This is done through SaaS service model. The hybrid and public deployment models needs to collaborate the services among the companies which are participating. The entropy level of the application can be relative high, is depends on the deployment model. When hybrid or public deployment model is used, host is characterizes as high dispersion and low when private model is used.

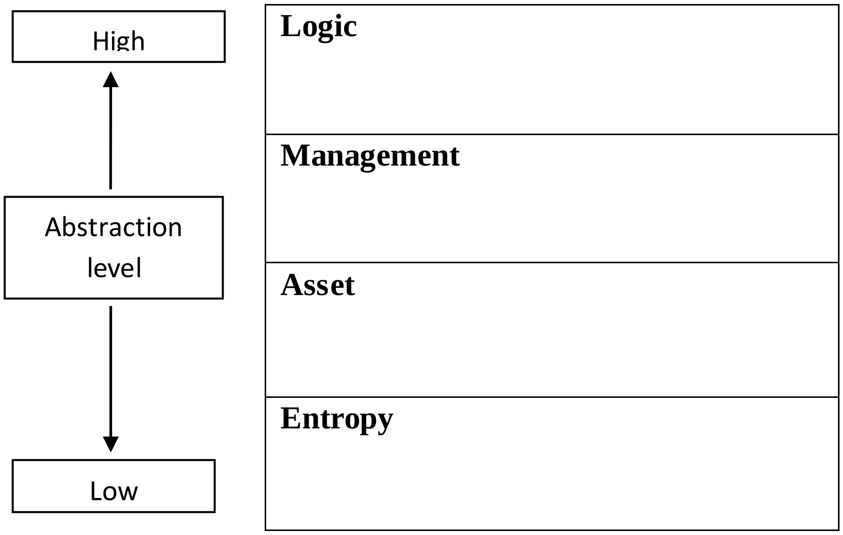


Fig. 1.6 Conceptual Categorization Layer

2) **Assets layer:** in cloud computing two types of assets i.e. hardware and software are there. Software defines as a set of services. Hardware resources include network

bandwidth, CPU, storage space and so on. If a user send request to access an asset, access must be approved only if the requestor is a valid user and also authorized to access the specified asset. Multi-tenancy must be supported.

3) **Management layer:** in cloud computing management of policies is required to be centralized in some cases. If there is collaboration between two companies management of policies needs to be distributed.
4) **Logic layer:** To provide and ensure the agreed level of quality to the customers, quality of service policies and service level agreements are made.

1.9 ROLE BASED ACCESS CONTROL

Role Based Access Control Model has two phases, which are used to assign privileges to users. In the first part, many-to-many user-role assignments are provided. In second part, many-to-many permission to role assignment is given. Roles can have role hierarchies which affect the authority and responsibilities of an organization [7].

Users are the members of roles and all authorizations to users are given through roles. Users get the roles authorization to access objects. The access to an object is controlled by roles.

According to allocated roles, a user can perform certain operations through permissions. Role based access control contain some authority constraints like separation of duty, data abstraction and least privileges.

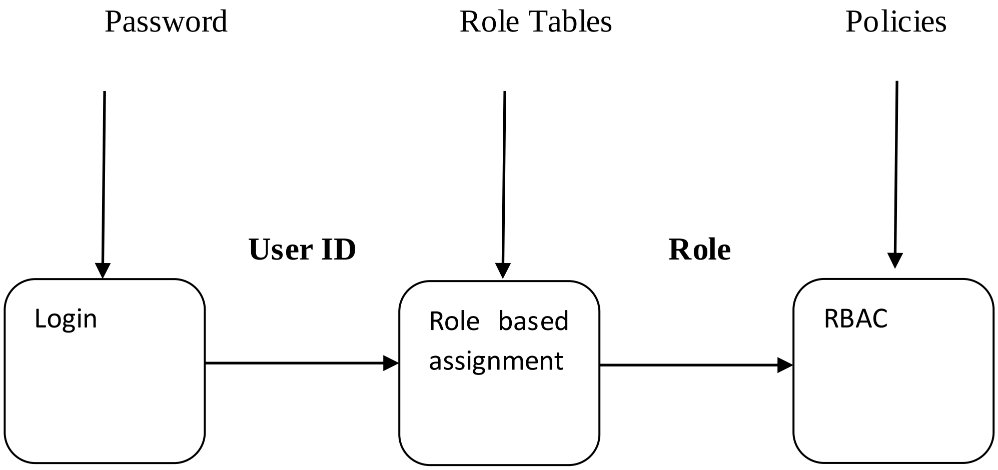


Fig. 1.7 Role Based Access Control Model

When a user want to perform some actions, certain type of authority is required. For this authority of proper role has to be granted to a user to perform some actions.

RBAC comprises a family of four references models:

RBAC0: In this User permissions (P), user (U) and roles (R) are the entities are minimum set of requirements. Permission-role assignment and user-role assignment defines a relation between these set of entities. Many roles can be assigned to one user and a role may contain more than one user. Similarly, permission can be assigned to many roles and a role can have more than one permission. A can have multiple sessions. User can invoke many roles within a session. Each session should relate to only one user.

RBAC1: it includes a role hierarchy with RBAC0. Role hierarchy is used to manage the roles, which represents an organization. It includes responsibility and degree of authority.

RBAC2: it defines the concept of constraints. These constraints are applicable on sessions, permission-role and user-role assignments.

RBAC3: it includes RBAC0, RBAC1 and RBAC2. It is known as a united model of RBAC. In this Constraints can also be applied to role hierarchy.

1.9.1 THE AUTHORIZATION CHALLENGES

1) As it is not possible to know the identities of all users in advance. Classical RBAC Model is not capable for supporting systems that provide services to unknown users. This is because RBAC needs users to be authenticated for access control. When users are dynamic and their identities are unknown, determining users' authorization is challenging.
2) Users can give all or part of their authority to another user. This needs support for delegation as well as revocation of delegation neither of which are provided by traditional RBAC (Role Based Access Control Model) [16].

1.10 KAMAN PROTOCOL

Kaman- Kerberos Assistant Mobile Ad-hoc Network (KAMAN) protocol is an extension of the Kerberos protocol. Kaman protocol is used to authenticate the Nodes in the Ad-hoc Network by secure server. Nodes are mutually authenticated. It is symmetric, key based authentication mechanism which involves both direct and indirect authentications. The main points in Kaman protocol are:

- Password of user is hashed and store on server. Each user has his own password and only known to him.

- Mutual authentication should be their between the servers. Servers share a Secret Key with each other for mutual authentication.
- Servers shared a secret key. Repository is encrypted with secret key.

In Kerberos protocol three parties are involved: user, authenticated server and ticket granting server. A large no of messages are required to exchange for authentication and getting service from server. But in KAMAN protocol, two parties are involved: one is the client node and the other one is the authentication server thus lesser number of messages are required to transfer between node and server for authentication and starting service.

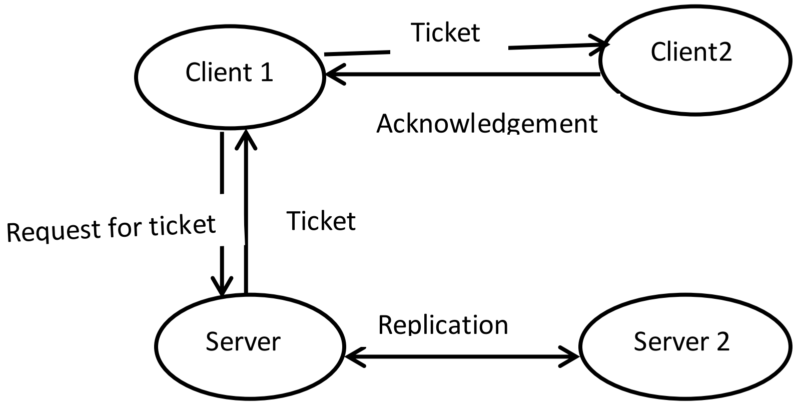


Fig. 1.8 Working of KAMAN Protocol

When a client wants to communicate with other client, then mutual authentication is required for both the client and server. Client send request to the server, client get authenticated and server send ticket to the client. Then client send that ticket to the another client and get acknowledged. Ticket has shared key which is created by server. By using this shared key data is encrypted and shared between two clients.

There is also a replicated server and replica is produced from time to time to avoid single point of failure. Authentication server and replicated servers are also mutually authenticated. Election mechanism is used to select the secure server. When nodes are authenticated with the server, a session is established between the node and the server.

1.10.1KAMAN Client-Server-Client Communication

Client1 → Server Options, ID_{C1}, ID_{C2}, Times, Nonce
Server → Client1 ID_{C1}, $Ticket_{C2}$,{$K_{C1,C2}$, Times, Nonce, ID_{C2}} K_{C1}
Client1 → Client2 Options, $Ticket_{C2}$, $Authenticator_{C1}$
Client2 → Client1 {TS, Subkey, Seq#} K_{C1}, K_{C2} $Ticket_{C2}$={Flags, $K_{C1, C2}$, ID_{C1}, AD_{C1}, Times} K_{C2} $Authenticatior_{C1}$={ID_{C1}, TS}$K_{C1,C2}$

Table1. Client-Server-Client Authentication

Options- used to request that certain flags be set in the returned ticket.

Times - specify the start, end renew time setting in ticket.

Flags - ticket status.

Nonce -random value as identifier to avoid replay attacks.

Subkey - instead of using Kc1, c2 other encryption key for the session.

Seq# - starting seq. no. to detect replays attacks.

ID_{C1} – Client1 identity

ID_{C2} – Client2 identity

AD_{C1} - Client1‘s network address.

K_{C1}- Encryption key of client1 based on the hashed value of the password

$K_{C1, C2}$ - Session key between client1 and client2.

TS - Time when authentication generated.

CHAPTER 2
LITERATURE REVIEW

Abdulrahman Almutairi, *et.al* (2014), present a risk aware cloud virtual resources assignment for big datacenters and proposed two heuristics algorithms PBH partition based heuristic and SBH sharing based heuristic for scheduling to solve the assignment problem. Develop efficient risk aware virtual resources assignment mechanism for cloud multitenant environment [2].

Shin-Jer Yang, *et.al* (2013), proposed a cloud service model ,using identity management and Role-Based Access Control, under a multi –tenant architecture (MTA), to propose and design a Role-Based Multi-Tenancy Access Control (RB-MTAC). In RB-MTAC a user can be assigned to many roles and each role is assigned to many permissions. This model combines identity management and role based access control method in multi tenancy cloud environment ,to manage privileges for providing protect of the security of application and data privacy .This model also block a non- tenant user accessing using identity management and access control prevent tenant users to viewing and accessing application and database without specific privilege .This method use a mechanism to manage user privilege using role based view point , and administrator only need to modify role privileges to change user privileges and thus reduce the potential errors from constant modifications. Each tenant can build an independent database or multi-tenants can share the same database .Data of different tenants could be stored in same place and that can prevents other tenants using data and system of that tenant . User login with an account no and system authenticates the user accounts through identity management. For valid users, a role assignment capture roles corresponding to user from database and assign the role and access right which belong to the user [20].

Kanupriyya, *et.al* (2013), proposed improvement in Role Based Access Model using Reference Ontology. It is used to control the no. of users per role, no. of transaction per user. The backup and restoration can also be done through this. These features are add to provide more security and if there is any crash in cloud data can be restore [11].

Shikha Singh, *et.al* (2013), discussed the different attacks and their respective corresponding solutions. In cloud Denial-of-service attack (DoS) is penetrable as in cloud many users uses the services and resources of cloud. Attacker send very large amount of packets from exploited information resources, called Zombie. It affects the availability of service for authorized users. To avoid theses DoS attacks some solutions are like intrusion prevention system, black holing, sink holing etc. are suggested. In malware injection, an attacker created his own malicious service implementation modules like SaaS or PaaS or virtual machine instance and adds it to the cloud. Through virtual side channel attack, attacker can place the virtual machine to get into cloud is described. The two techniques virtual firewall appliance and randomly encryption decryption are proposed to avert side channel attack as a solution [18].

Vijay Varadharajan, *et.al* (2013), proposed a security model for cloud service that helps to detect and prevent the security attacks in cloud environment based on trusted attestation techniques. A multitenant cloud architecture with provides different services on virtualized sources, an attacker model and attack scenarios are considered. This model allows the cloud service provider to certify some security properties of tenant virtual machine and services which are provided. These properties are used to detect and minimizes these attacks. If there are any changes in the behavior of the virtual machine with the certified properties, it dynamically isolates the virtual machine [22].

Bibin K Onankunju (2013), proposed a technique for providing cloud storage a secured access. A hierarchical structure is implemented to offer a more secure access. Using this, a file can be easily deleted, download from and to the cloud. It is a highly efficient model for provide access control in cloud computing. A clock is used for decryption key which is based on time [5].

Wei-Tek Tsai, *et.al* (2011), proposed a role based access control method by using role ontology for multi-tenant Architecture in clouds. Ontology can build a role hierarchy for a particular domain. A security mechanism is provided for multi-tenant architecture. Ontology information is used in RBAC access control as a heuristic for providing role hierarchies. The proposed system reduced the complexity of system design. Ontology transformation algorithm and operations are given [23].

Xiao-Yong Li, *et.al* (2010), proposed a multi tenancy based access control model to implant the duty of separation in cloud. This model has a two grain level access control method, i.e. a tenant granule level access and application granule control. Tenant granule is for the cloud service provider to compartmentalize different users and other is for customers to manage the access to their own application. At application perimeter, MTACM based system can be used. It defines different management domains for CSP and customers. At granule levels, different security management function interface is provided. The author described model in public cloud for the security of applications. The basic rule related to tenant and application i.e. tenant rule and application rule are defined. A prototype of MTACM is also implemented for high performance and compatibility [24].

Kirsten Sohr, *et.al* (2008), Discuss non-temporal and history-based authorization constraints in the Object Constraint Language and first-order linear temporal logic. With the help of a theorem prover author verified the role based access control policies and also validate policies with the help of USE system tool, which is a tool for validating OCL constraints. UML/OCL system is used in use case to formulate RBAC policies. To validate the authorization constraints, USE tool is employed. Various conflicts b/w authorization constraints and missing conflicts detected with the help of USE. RBAC policy is a hierarchical RBAC. A set of constraints are defined for organization. An authorization engine is also described for enforcement of authorization constraints. Authorizations constraints are used to design architect polices and express higher level organization rules [12].

Shin-Jer Yang, *et.al* (2007), authors proposed a new technique ISPWAP, for web based applications to incorporate security and performance features. ISPWAP combines role based access control and SWAP framework. While designing the web applications to fix the security and performance related issues ISPWAP approach is proposed. Authors proposed ISPWAP framework through algorithm and describe the implementation of the secure web based application with improved performance. The approach provides a method for reducing security related risk and improved system throughput in designing web applications. Various design issue for security like access control, SQL injection, session hijacking, information disclosure and performance related issues like time for get into web pages and handling database are defined [19].

Asad Amir Pirzada, *et.al* (2004), describes Kaman protocol as authentication service for mobile and ad-hoc network. Kaman migrate a no. of features of Kerberos authenticated protocol. The main features includes preventing the forgery of node identity, detection of replay attacks, establishment of secure network, mutual authentication distribution of session keys among servers[3].

Ravi S. Sandhu, *et.al* (1996), discuss about the family of models for role based access method. In this model permissions are associates with roles and user is a member of role. The role carries a set of objects on one side and set of subjects other side. Author describes a framework of reference models to address the components of RBAC, and their interactions. The author defined four reference models: base model (RBAC0), advanced models (RBAC1 and RBAC2), consolidate model (RBAC3). The base model, defines the minimum requirements for any system that support RBAC. RBAC1 add concept of role hierarchy. RBAC2 add constraints and consolidated model, RBAC3, includes RBAC1 and RBAC2 and RBAC0. A management model is also specified to manage the RBAC itself [17].

B. Clifford Neuman, *et.al* (1994), describes an authentication protocol which is used to authenticate users in distributed environment. Through Kerberos a user can authenticate itself to multiple servers using password. In this there is a KDC (key distribution Centre) which contains authentication server (AS) and ticket granting server (TGS), application server (V) and a number of clients. Client receives ticket granting ticket (TGT) from AS, send this ticket to TGS to get service ticket and then send service ticket to V to get service [4].

CHAPTER 3
PRESENT WORK

3.1 PROBLEM FORMULATION

In cloud computing processing is performed by a standard browser through internet. As cloud computing offers many good services, security and privacy issues makes users worried to migrating to cloud computing. Security is the most important aspect which is consider when moving to cloud. Data which is stored on cloud can be access by legitimate user. In large organization, the data as well as software's are installed on the cloud which is accessed by the organization's different level of employee's. The employee's on the different level can have different access rights. It means that every employee can access different data according to their designation. In the cloud computing, it is difficult to maintain the access control lists. The many techniques have been proposed for the access control. For access control RBAC technique is effective and reliable among all other techniques. In role based access control technique legitimate user can prove its identity to cloud service provider through the secure authentication procedure. According to user rights, the access is provided to the user. The main problem in such technique is security. Many security attacks are possible in role based access control technique. A new hybrid type of technique is developed which is the combination of identity management and RBAC method. In this technique the side channel attack is possible, in which attacker place the virtual machine and all the traffic of the legitimate user will directed to the attackers virtual machine. The attacker will hijack all the credentials of the legitimate user, and present it to server on the behalf of the legitimate user. Thus attacker can compromise the identity of users and can access the user's data on clouds.

3.2 SCOPE OF STUDY

The cloud computing contains the set of services that are delivered to a consumer over network. A third party provider owns the cloud infrastructure, delivered services to consumers and thus reduced the burden at consumer's side. To enhance the security of cloud architecture the access control methods are mainly concern. As the number of roles is less in RBAC model it is widely used. A user can be easily classified according to his role. The Role-based Access Control model, provide an efficient way to manage access to information and also in large networked applications it reduced the cost of security administration and complexity. A hybrid type of access control scheme is being developed by joining a RBAC and identification schemes. In RB-MTAC, identity management is used to determine the user's identity and RBAC is used for assigning roles which are appropriate according to user's related work. Role-based assignments manage user's access rights to attain application independence and data isolation for improving the processing performance of cloud multi-tenant services and hardening the security and privacy of cloud applications. The side channel attack is possible in RB-MTAC scheme. The enhancement will be done in RB-MTAC scheme to prevent the side channel attack. This will enhance security and reliability of cloud computing.

3.3 OBJECTIVES

1) To identify the existing schemes for Access Control in Cloud Computing.
2) To analyze shortcomings of Role-Based Multi-Tenancy Access Control Scheme.
3) To prevent side channel attack in Role-Based Multi-Tenancy Access Control method in cloud environment.
4) To propose novel technique to prevent side channel attack in Role-Based Multi-Tenancy Access Control Scheme.
5) To implement the proposed technique and compare it with the existing technique.
6) To help the users to ensure the privacy of data.
7) To enhance security and reliability of cloud computing.

3.4 RESEARCH METHODOLGY

Access control methods are used for the purpose of accessing a system. It allows, denies or restricts an access to a system. Access control methods monitors and record all efforts, which are made to access a system. An unauthorized user who is attempting to access a system can be identified by access control methods.

Various Access Control models like Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC) can be used for accessing a system. These models are identity based access control models. In identity based access methods, user and resources are identified by unique names. Identification can be done directly. It may also be done through assigning roles to users. In distributed system where fixed no of users with known set of service is available; these Access Control Methods are used. The side channel attack is possible in RB-MTAC. It will reduce the network reliability and security of the network will be compromised.

3.4.1 FLOW CHART FOR PROPOSED WORK

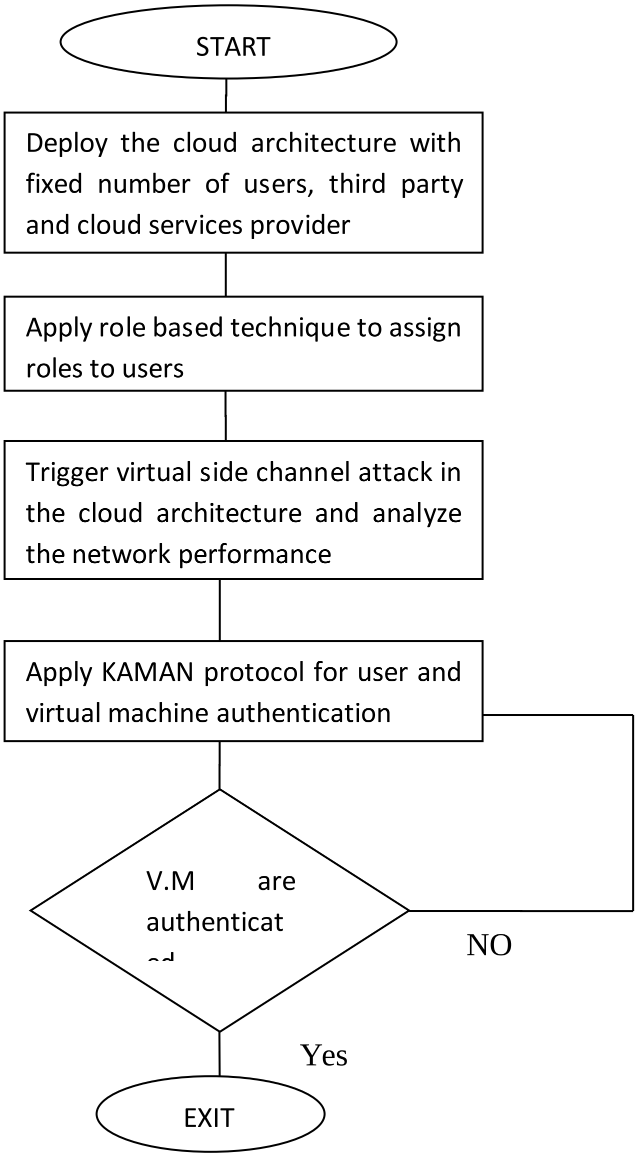

START
Deploy the cloud architecture with fixed number of users, third party and cloud services provider
Apply role based technique to assign roles to users
Trigger virtual side channel attack in the cloud architecture and analyze the network performance
Apply KAMAN protocol for user and virtual machine authentication
V.M are authenticat
NO
Yes
EXIT

Fig.3.1 Flow Chart for Proposed Work

In this work, first we deploy cloud architecture with cloud service provider, third party and fixed number of users. A role based access method is used to assign the roles to users. Then virtual side channel attack will be trigger in cloud architecture. To prevent the side channel attack, novel technique will be proposed which is based on the server identification. Before present its credentials to the server, legitimate client will ask sever for its credentials. If the sever credentials are verified by the client then further process will proceed otherwise algorithm will halt.

3.4.2 ALGORITHM FOR PROPOSED WORK

MESSAGE EXCHANGE BETWEEN CLIENT AND VIRTUAL MACHINE

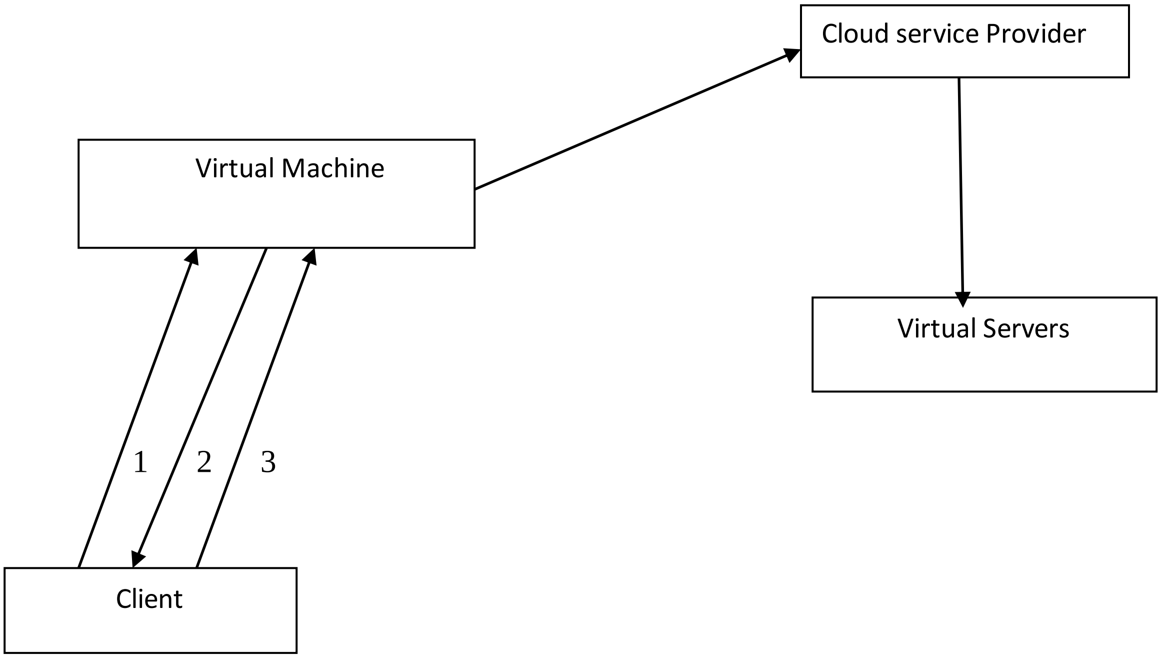


Fig.3.2 Message Exchange Diagram

To verify the identity of sever three message are required to exchange between user and VM. The procedure of message exchange is defined in the algorithm.

While designing this algorithm, let us take some assumptions:

1. A secret no is shared between user and VM.
2. The client ID stored on the VM and VM knows MAC address of Client and Client ID.

If the virtual machine is legitimate, then following steps are followed in the algorithm

1. Client send its MAC address with the nonce value and request the VM to send VM ID, Client ID and MAC address of VM.
2. When VM receives the message it will verify the credentials.
3. If the credentials are verified, VM sends VM ID, Client ID, nonce timestamp, and VM's MAC address.
4. If the client verified its Client ID and VM ID.
5. Then communication will start between Client and VM.

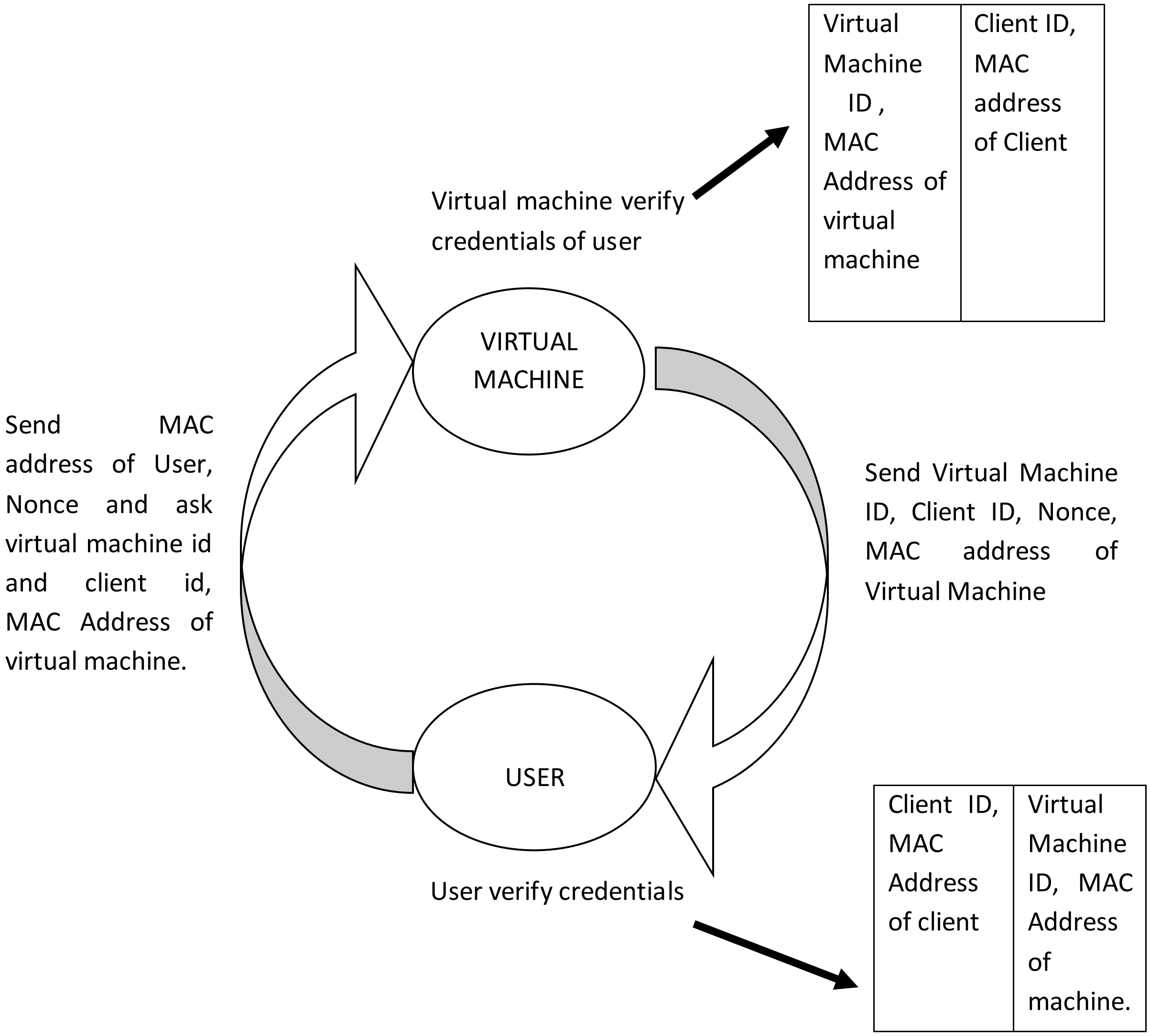
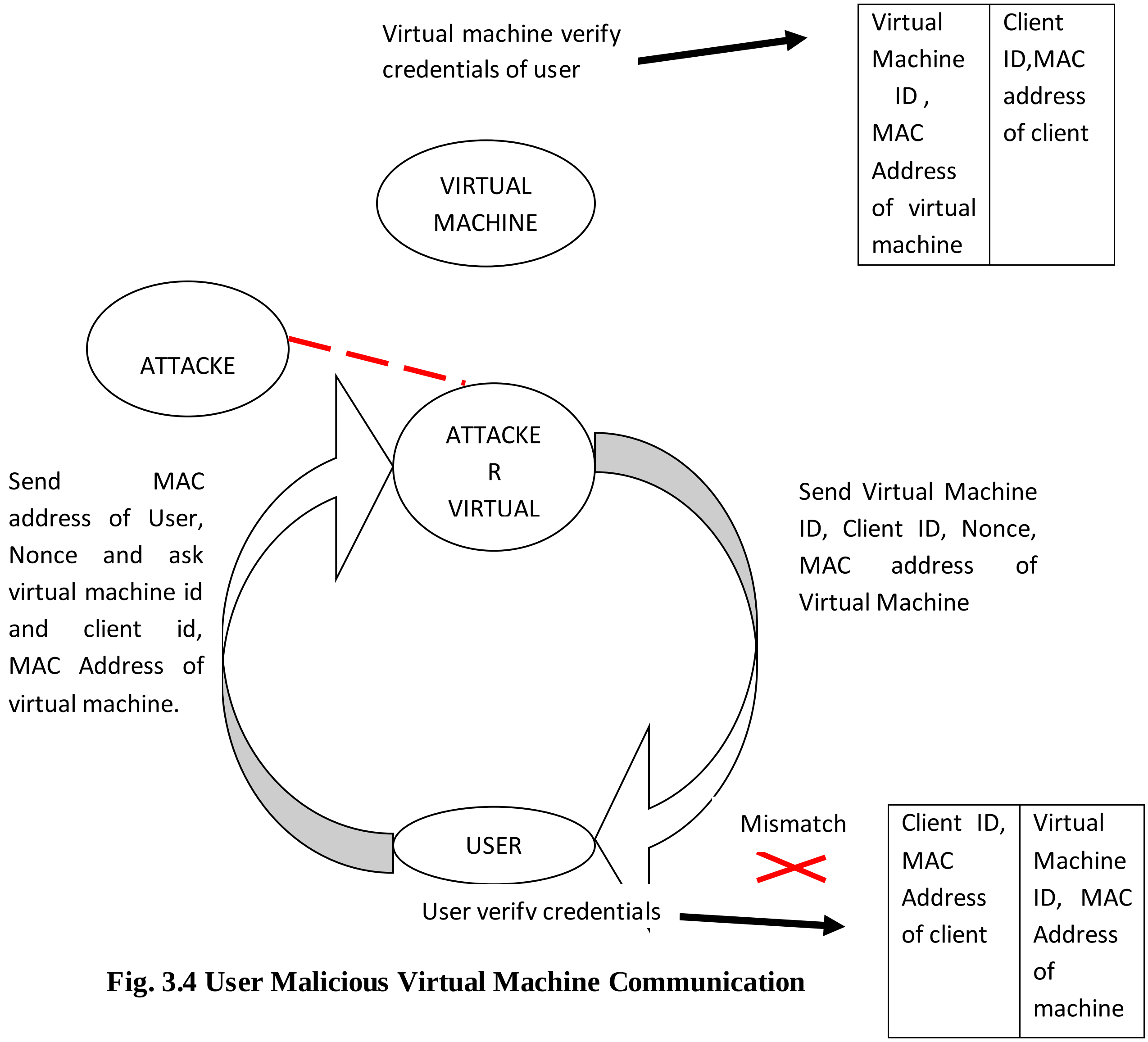

Virtual Machine ID , MAC Address of virtual machine
Client ID, MAC address of Client
Virtual machine verify credentials of user
VIRTUAL MACHINE
Send MAC address of User, Nonce and ask virtual machine id and client id, MAC Address of virtual machine.
Send Virtual Machine ID, Client ID, Nonce, MAC address of Virtual Machine
USER
User verify credentials
Client ID, MAC Address of client
Virtual Machine ID, MAC Address of machine.

Fig.3.3 User-VM Communication

If the virtual machine is illegitimate, then following steps are followed in the algorithm

1. Client send its MAC address with the nonce value and request the VM to send VM ID, Client ID and MAC address of VM.
2. When VM receives the message it will verify the credentials.
3. If the credentials are verified, VM sends virtual machine ID, Client ID, nonce timestamp, and VM's MAC address.
4. The client will not verify its original ID and VM ID
5. The communication will halt and fake VM will be detected on its MAC address.


Virtual machine verify credentials of user
VIRTUAL MACHINE
ATTACKE
ATTACKE R VIRTUAL
Send MAC address of User, Nonce and ask virtual machine id and client id, MAC Address of virtual machine.
Send Virtual Machine ID, Client ID, Nonce, MAC address of Virtual Machine
USER
Mismatch
User verifv credentials

Virtual Machine ID , MAC Address of virtual machine	Client ID,MAC address of client

Client ID, MAC Address of client	Virtual Machine ID, MAC Address of machine

Fig. 3.4 User Malicious Virtual Machine Communication

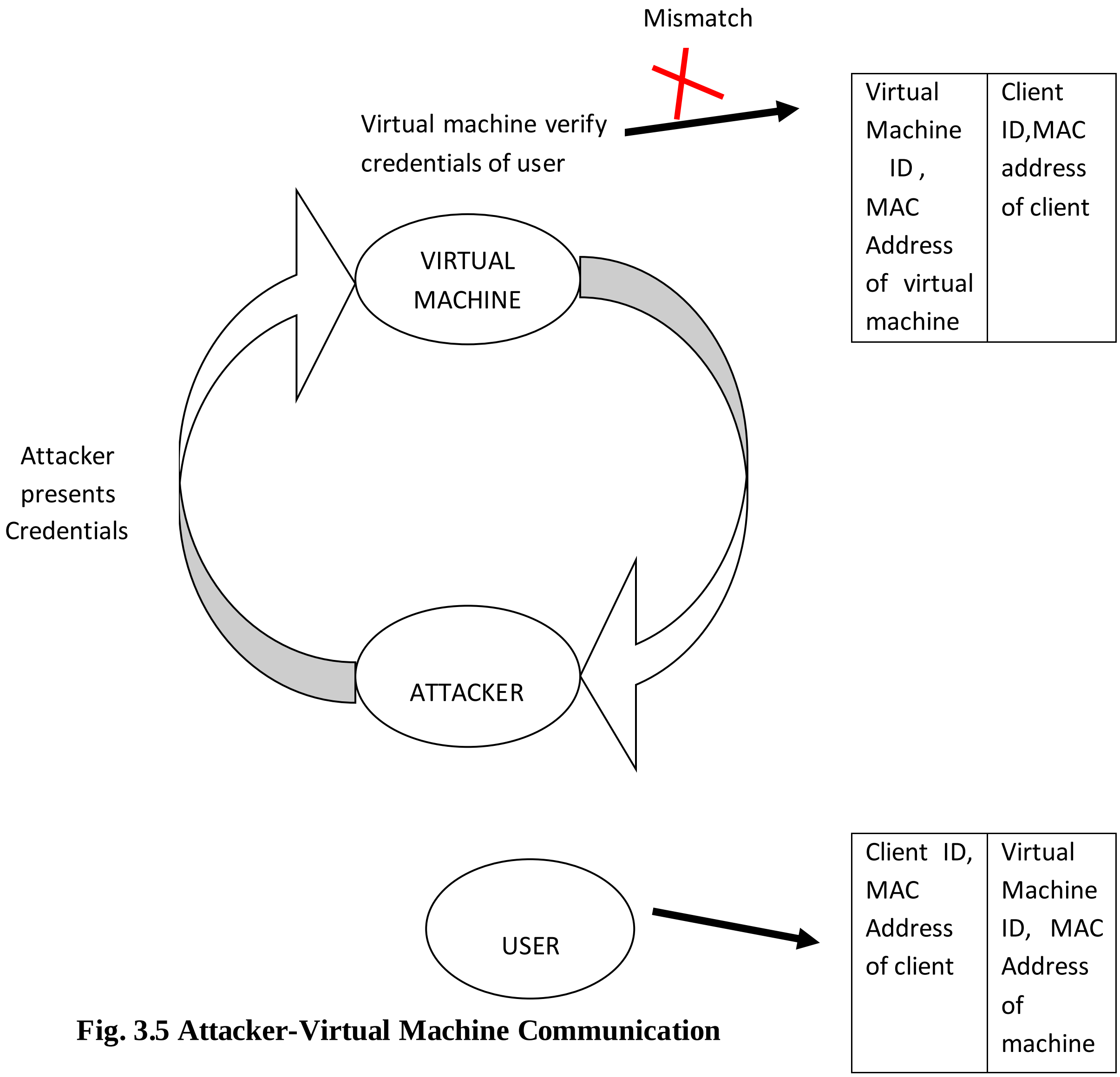

Mismatch
Virtual machine verify credentials of user
Virtual Machine ID , MAC Address of virtual machine
Client ID,MAC address of client
VIRTUAL MACHINE
Attacker presents Credentials
ATTACKER
USER
Client ID, MAC Address of client
Virtual Machine ID, MAC Address of machine

Fig. 3.5 Attacker-Virtual Machine Communication

User → Virtual Machine REQUEST TICKET: MAC ADDRESS of Client, Virtual machine ID, Client ID , Nonce
Virtual Machine → User TICKET: Virtual Machine ID, MAC address of Virtual Machine , Client ID, Nonce

Table 2 User-Virtual Machine Authentication

PSEUDOCODE

```
Deploy the network with users and ask for credentials
User input ‘user name’
User input ‘password’
Set the flag B=0;
Set the array with registered user and virtual machines
Do {
The user send Query message about the MAC ID of the virtual machine
If “mac_id” of virtual machine is equal to registered MAC ID
{
Set B=1;
Else
{
    1. Ask for the secret number of virtual machine, NONCE number and identity of
       machine

    If (Secret number of the virtual machine matched with user secret Number)
    Ask for MAC ID of the machine
    If (MAC ID Machine Matched)
    {
    User access the assigned data
    }
    Else
    Isolate the machine
}
}
}
```

CHAPTER 4

RESULTS AND DISCUSSION

4.1 TOOL

NS-2 is an open-source simulation tool which runs on UNIX like operating systems. It is an event simulator targeted at network research and support the simulation of routing protocols, multicast protocols, and IP protocols as UDP, RTP, and TCP over wired, wireless and satellite networks. As it supports multiple protocols and has the capability of detailing network traffic graphically makes it a very useful tool. It also supports different algorithms in queuing and routing. Routing algorithms includes LAN routing and broadcast and queuing algorithms includes FIFO, fair queuing etc. it is used as a variant of the REAL network simulator in 1989. REAL network simulator is used for studying the dynamic behavior of flow control and congestion control schema in packet-switched networks. NS development was supported by DARPA (defense advanced research project agency) through VINT in 1995.

NETWORK SIMULATOR-2 (NS-2) OVERVIEW

Network simulator is a discrete event simulator used for networking research. It is a simulated program developed by virtual internetwork test-bed (VINT) project group. Ns-2 supports simulation of TCP and UDP, MAC layer protocols, routing and multicast protocols over wired and wireless network etc. in this

- Physical activities are translated to events.
- Events are queued and processed in order of their schedule occurrences.
- Time progresses as event processed.

Simulations are stored in trace files as per user’s requirements. These trace files are uses as input for analysis purpose for different components.

A NAM trace file is used for ns animator which provide simulated environment. Tit is denoted as .nam.

A trace file denoted by .tr is used to generate the graphical results with the help of X graph component.

COMPONENTS OF NS-2

Ns: the simulator itself

Nam the network animator: visualize ns and other output. GUI input simple ns scenarios

Preprocessing: traffic and topology generators

Post processing: trace analysis

SOFTWARE STRUCTURE OF NS-2

Ns-2 used two languages

1) **C++**

   Used for packet processing. It is Fast to run, detailed and has complete control.

2) **OTCL**

   Used for control. It has Simulation setup, configuration, occasional actions. It is fast to write and change.

User's view of NS-2

NS-2 is object oriented Tcl script interpreter that has a simulator event scheduler and network component object libraries and network setup module libraries.

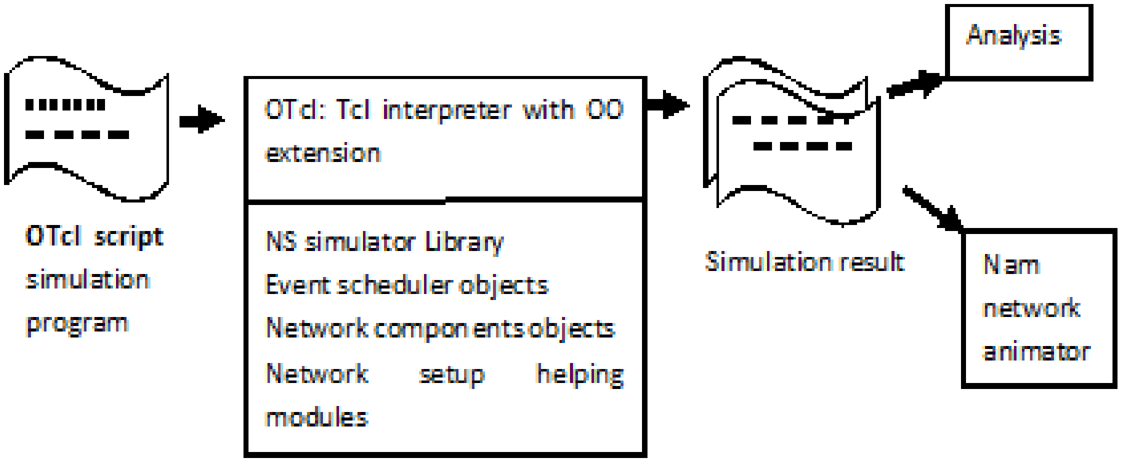


Fig.4.1 Simplified user's View of Network

In this section, two cases are shown. In the first case, problem is implementation. In problem implementation part, legitimate users authenticate to virtual machine and can store and retrieve their data through cloud service provider on virtual server. Virtual side channel attack is triggered through an attacker is also shown. In the second case, solution is implemented, in which KAMAN protocol is implemented to avert virtual side channel attack.

4.2 PROBLEM IMPLEMENTATION

First of all, network is deployed with finite numbers of node. In our case 41 network nodes are deployed as shown in Fig. 4.2.

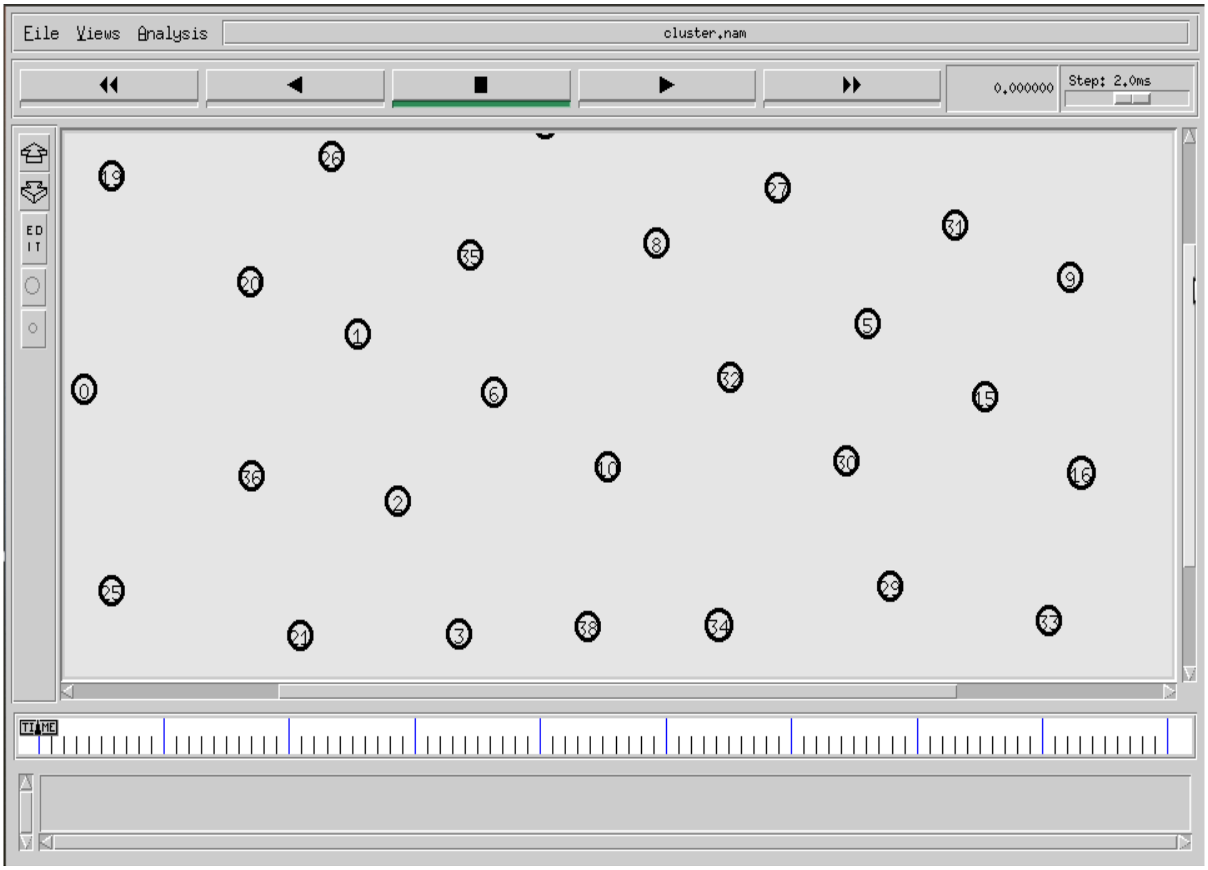
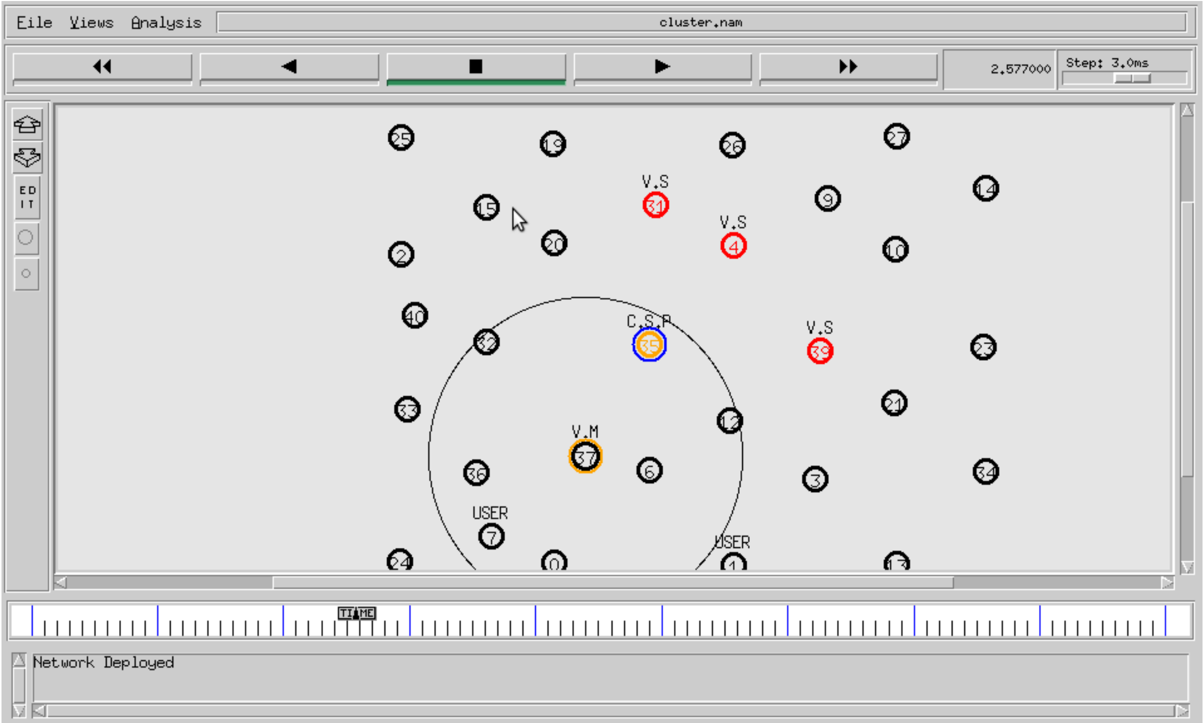


Fig.4.2 Network Deployment with fixed number of Nodes

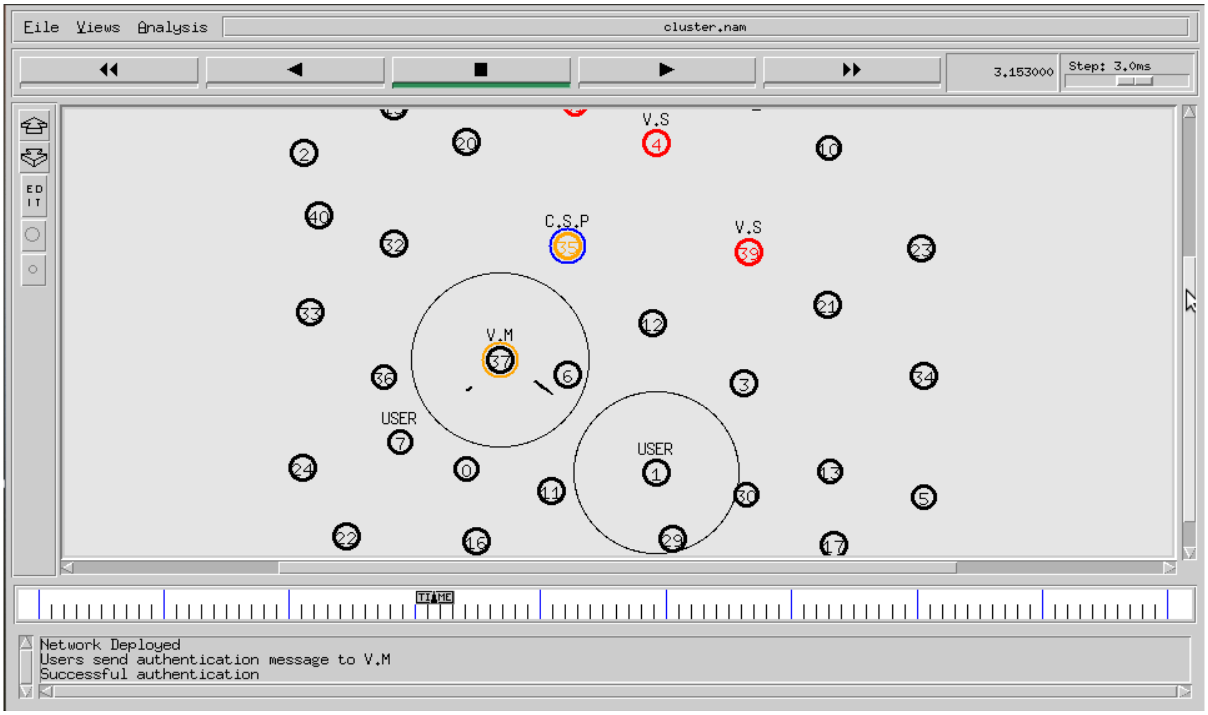
There are finite numbers of nodes in the network. Deploy the network and select source and destination. As shown in Fig.4.3, Node37 act as virtual machine. Node1 and Node7 acts as user. Node4, Node31, Node39 respectively acts as virtual servers. Node35 act as cloud service provider.



```
Network Deployed
```

Fig. 4.3 Deploying fix no. of Users, VM, CSP and VS

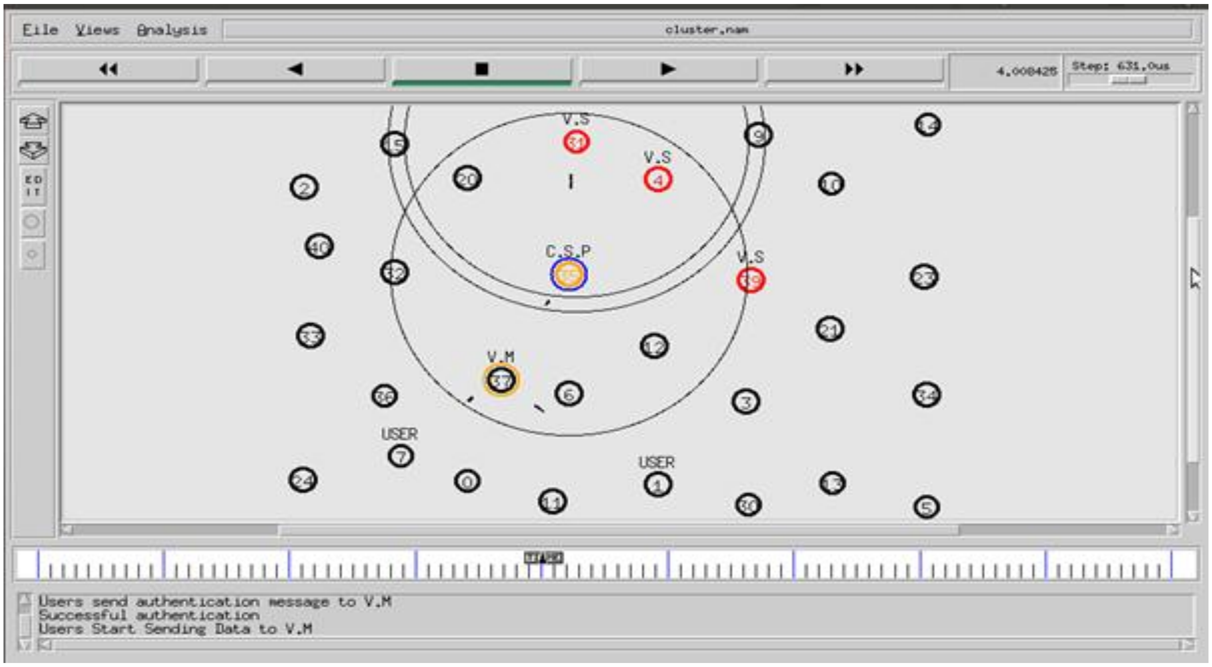
In Fig.4.4, Communication is shown between user and virtual machine. User send his user ID and password as an authentication message to virtual machine to verify their credentials. If credentials are verified successfully, then VM responds back to user with OK messages.



```
Network Deployed
Users send authentication message to V.M
Successful authentication
```

Fig. 4.4 User Authentication

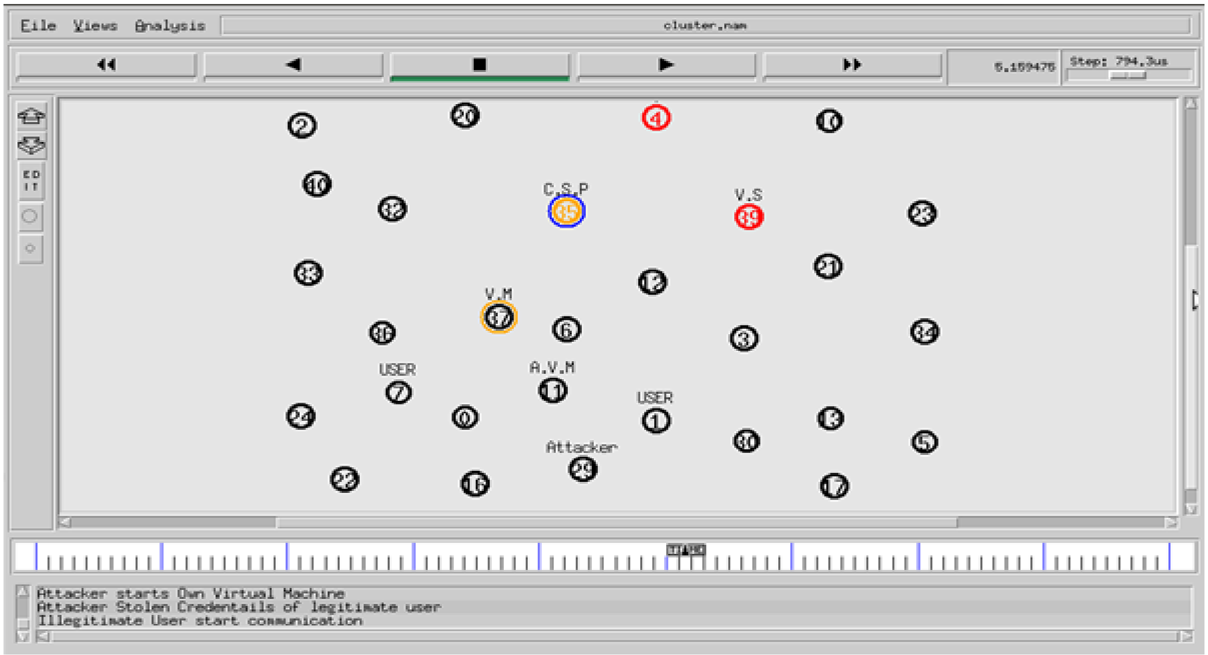
In Fig.4.5 shows, communication starts between user and VM after. After that user send his data to VM and VM sends data to CSP and upload the data to other virtual servers.



```
Users send authentication message to V.M
Successful authentication
Users Start Sending Data to V.M
```

Fig. 4.5 Communication between User and VM and Data Storing at Virtual Server

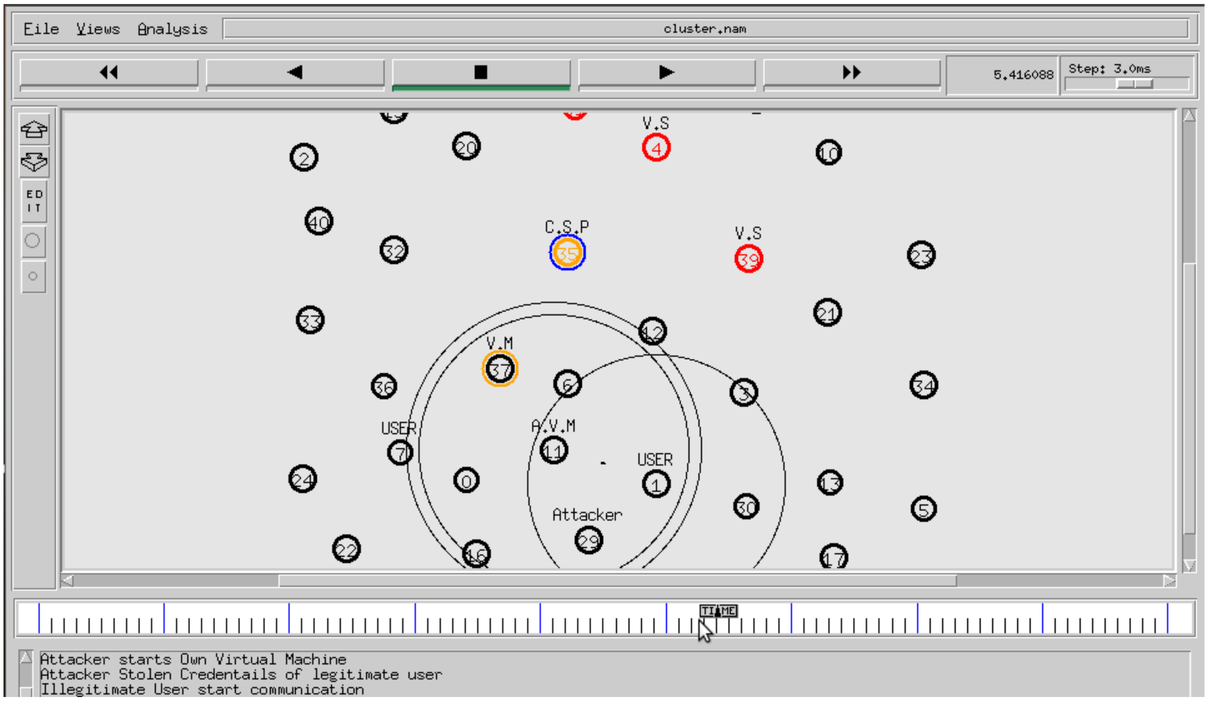
When the data transfer from source to destination. Attacker start their own illegitimate VM. Attacker tries to hack data during transfer as shown in the Fig.4.6. Node29 is attacker and Node11 is the attacker’s VM.



```
Attacker starts Own Virtual Machine
Attacker Stolen Credentails of legitimate user
Illegitimate User start communication
```

Fig. 4.6 Attacker Places his own Virtual Machine

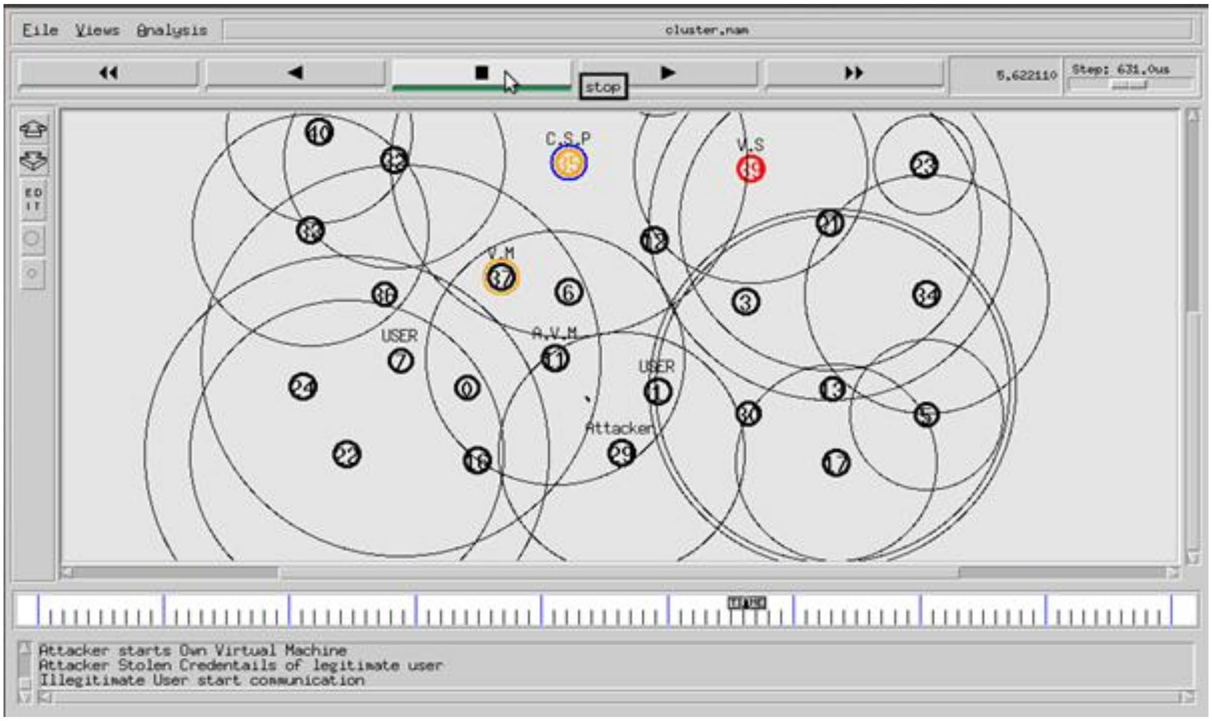
Legitimate users show their credential to the illegitimate virtual machine as shown in Fig.4.7.



```
Attacker starts Own Virtual Machine
Attacker Stolen Credentails of legitimate user
Illegitimate User start communication
```

Fig. 4.7 User presents the credentials to Attacker's Virtual Machine

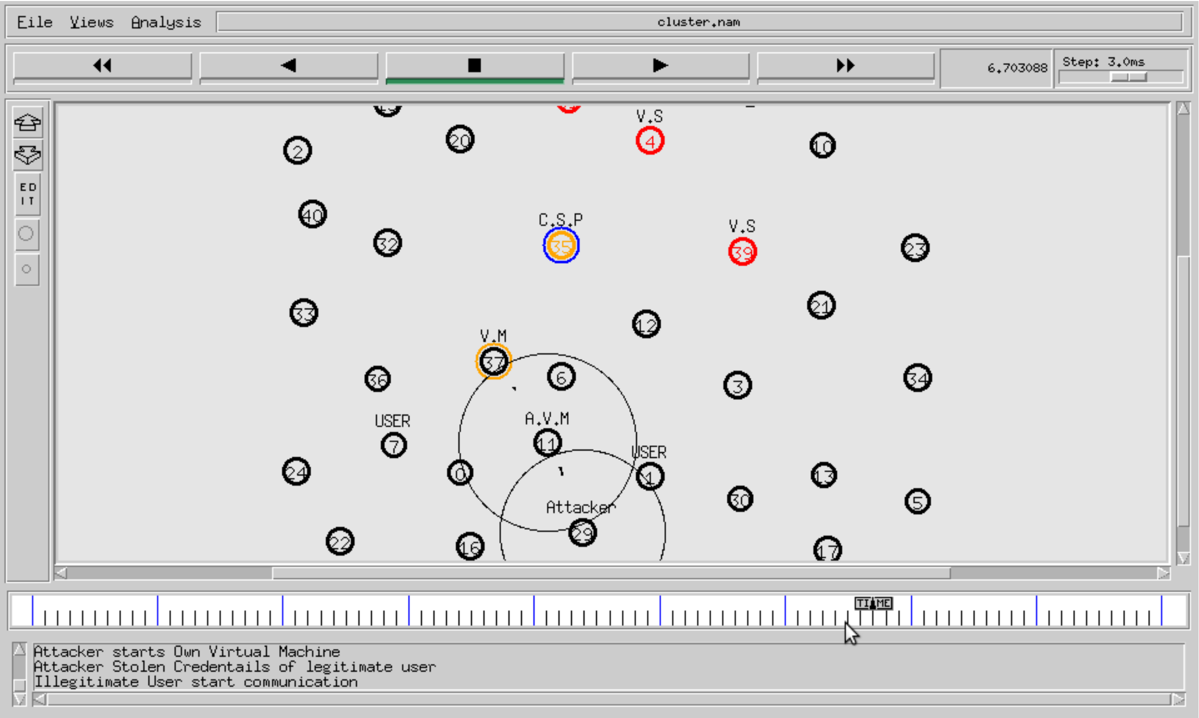
Illegitimate user stoles the credentials of user as shown in Fig.4.8 and use these credentials for further communication and modifying the data.



```
Attacker starts Own Virtual Machine
Attacker Stolen Credentails of legitimate user
Illegitimate User start communication
```

Fig. 4.8 Attacker stole the credentials of User

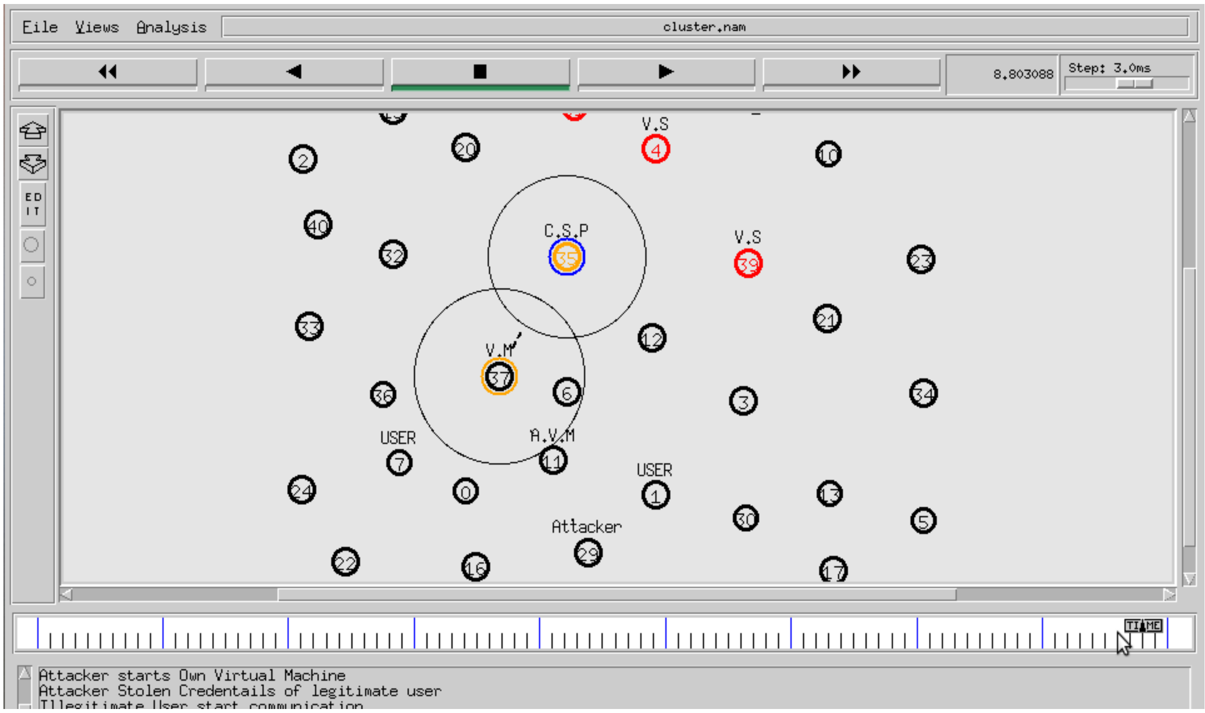
Illegitimate VM gives credential to the attacker on this behalf it communicates with CSP as shown in Fig.4.9. Attacker can easily change data sending from source to destination.



```
Attacker starts Own Virtual Machine
Attacker Stolen Credentails of legitimate user
Illegitimate User start communication
```

Fig. 4.9 Attacker presents the Credential of User to VM

Fig.4.10 shows attacker extracts the user's useful data from virtual server through VM.



```
Attacker starts Own Virtual Machine
Attacker Stolen Credentails of legitimate user
Illegitimate User start communication
```

Fig. 4.10 Attacker extracts user's information

4.3 SOLUTION IMPLEMENTATION

First of all, network is deployed with finite numbers of node. . In our case 41 network nodes are deployed as shown in Fig.4.11.

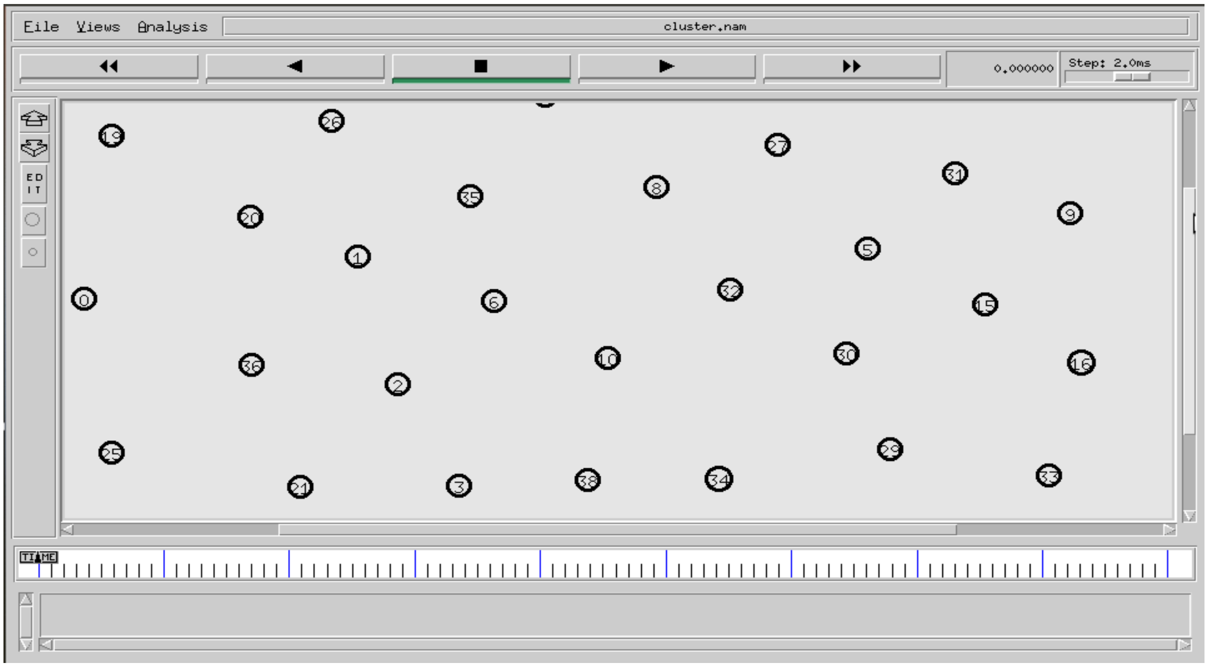
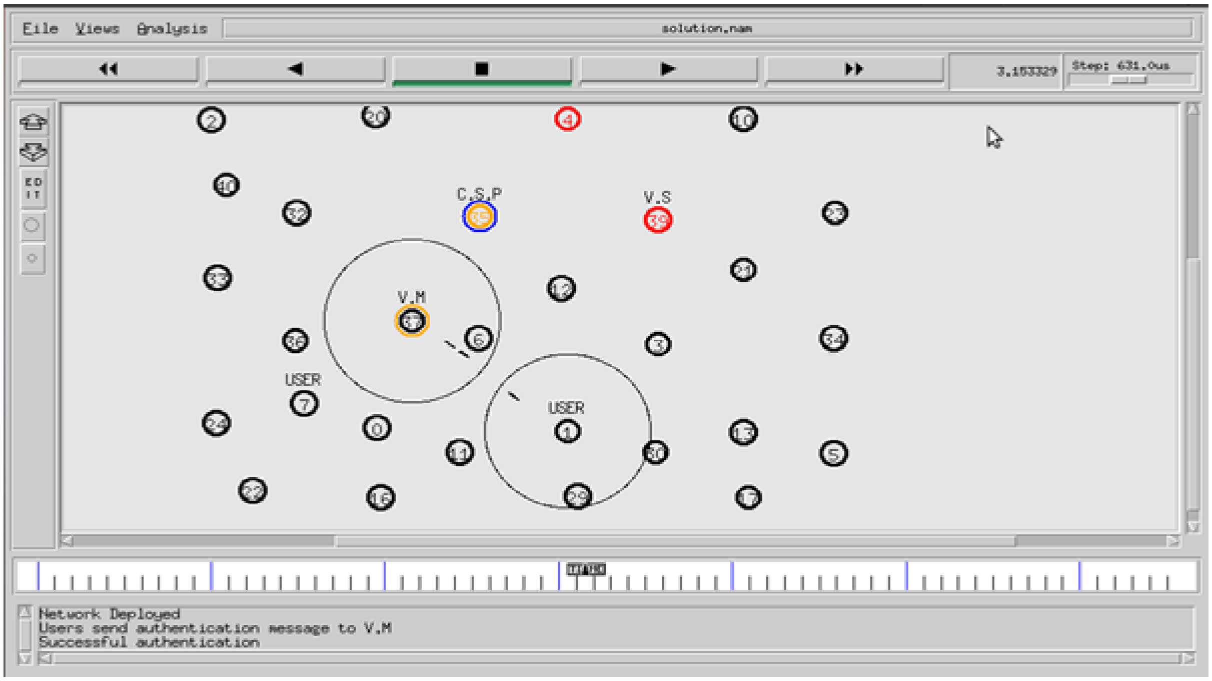


Fig. 4.11 Network Deployment with fixed number of Nodes

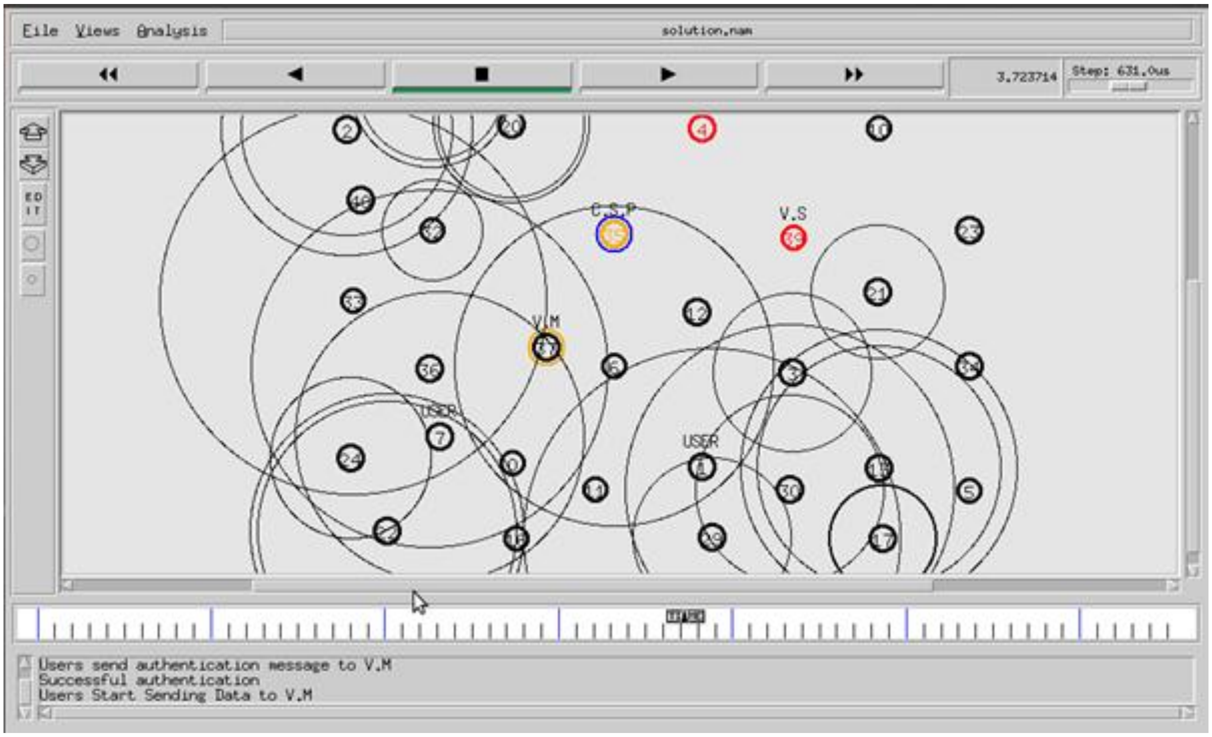
User sends authentication message to virtual machine to verify their credentials as shown in Fig.4.12.



```
Network Deployed
Users send authentication message to V.M
Successful authentication
```

Fig. 4.12 Authentication Messages between User and VM

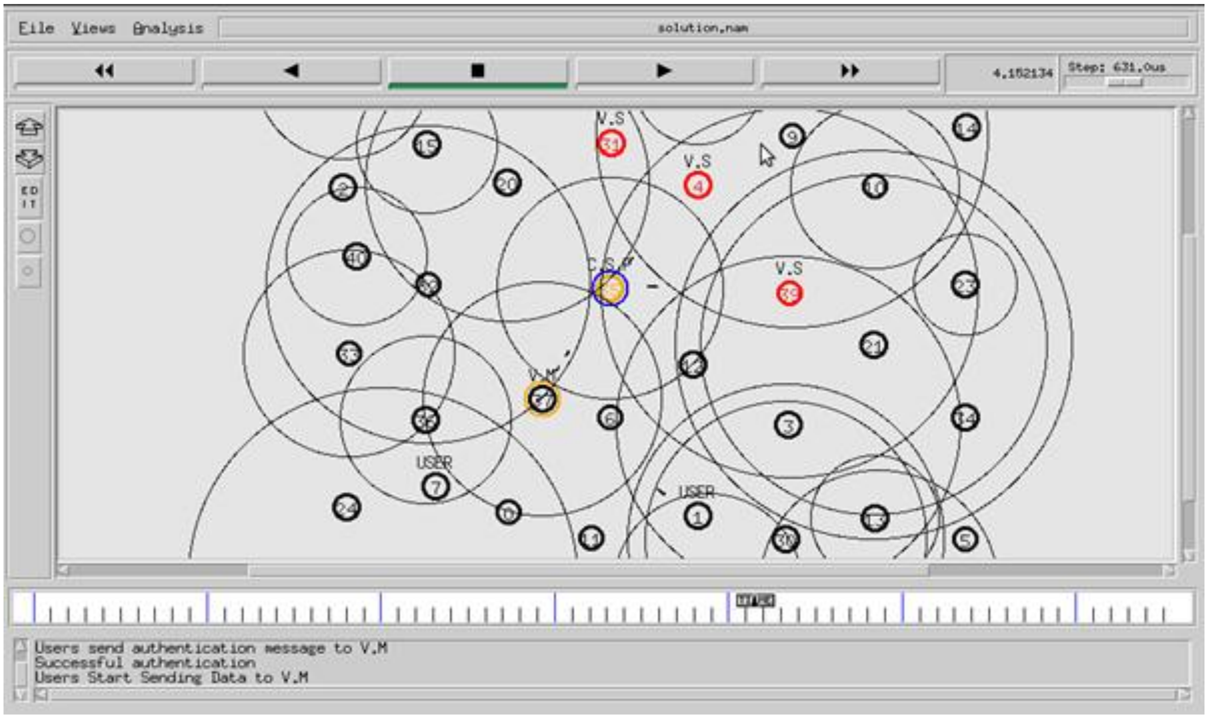
VM verifies credentials of the user responds back with OK messages as shown in Fig.4.13.



```
Users send authentication message to V.M
Successful authentication
Users Start Sending Data to V.M
```

Fig. 4.13 User successfully authentication

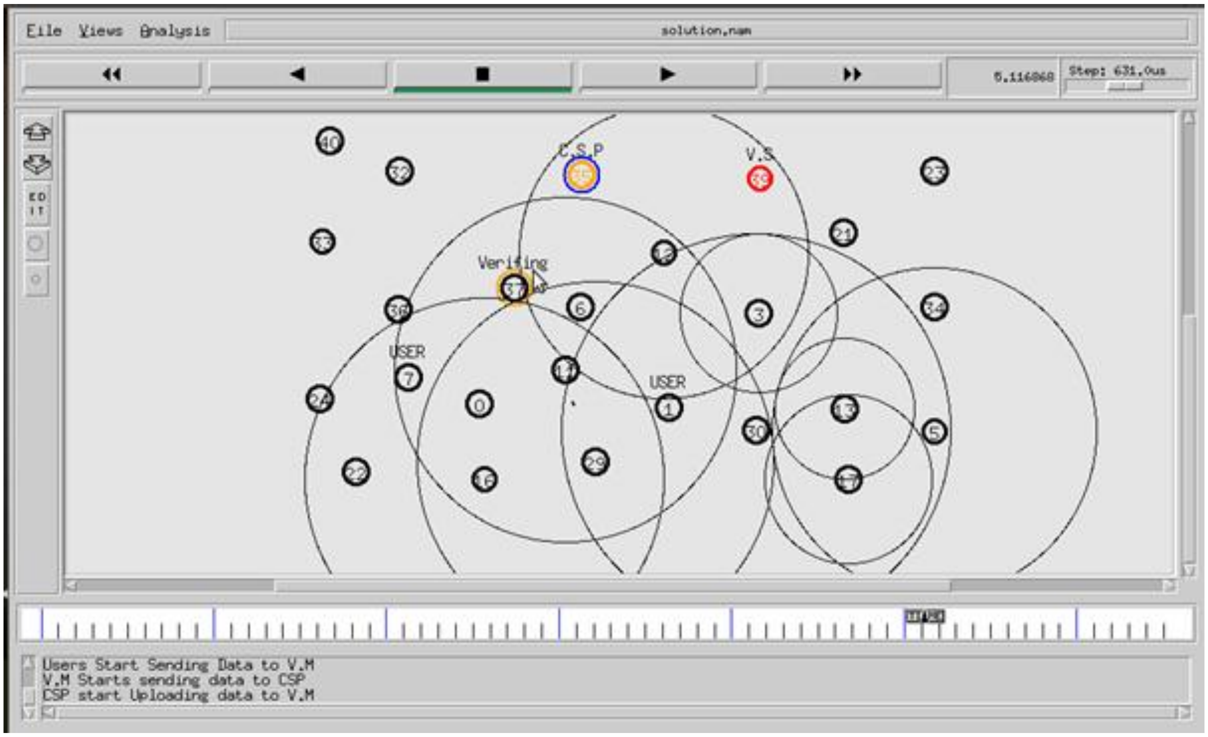
Communication starts between user and virtual machine. After that virtual machine sends data to cloud service provider and upload to other virtual servers as shown in Fig.4.14.



```
Users send authentication message to V.M
Successful authentication
Users Start Sending Data to V.M
```

Fig. 4.14 Communication between user and VM and data storing at virtual server

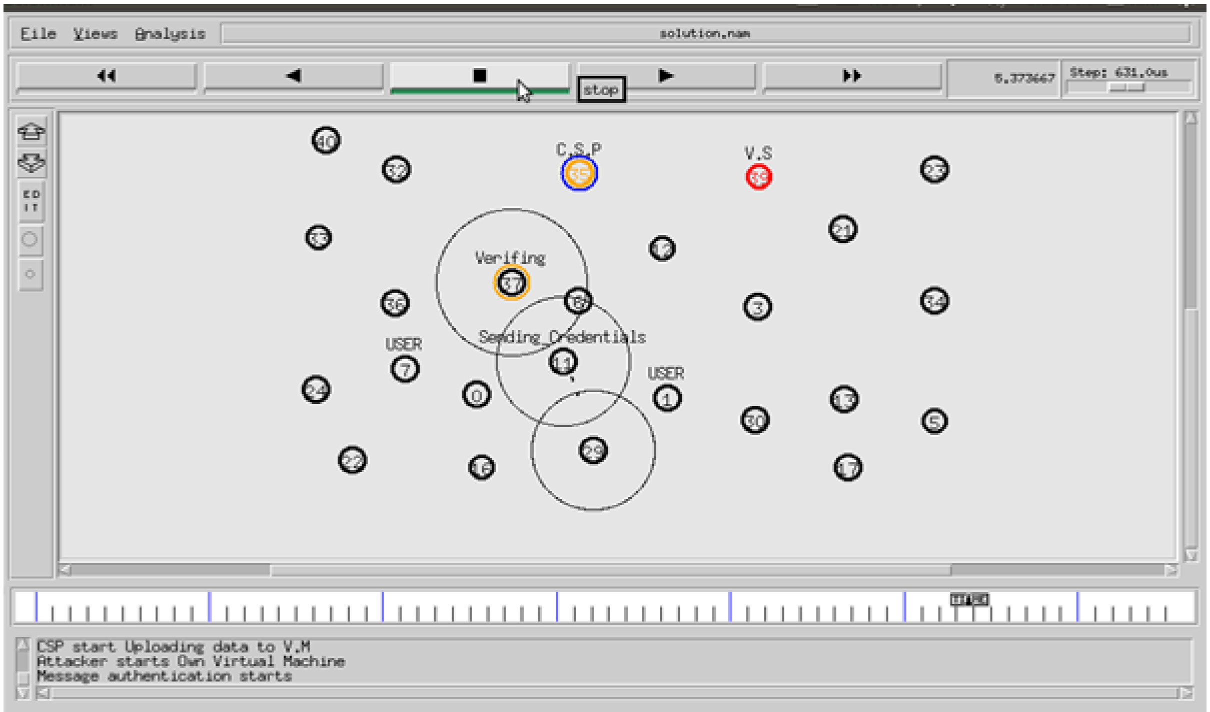
Attacker start their own illegitimate machine. Node 29 is act as an attacker node and node 11 act as malicious virtual machine shown in Fig.4.15.



```
Users Start Sending Data to V.M
V.M Starts sending data to CSP
CSP start Uploading data to V.M
```

Fig. 4.15 attacker placing his virtual machine

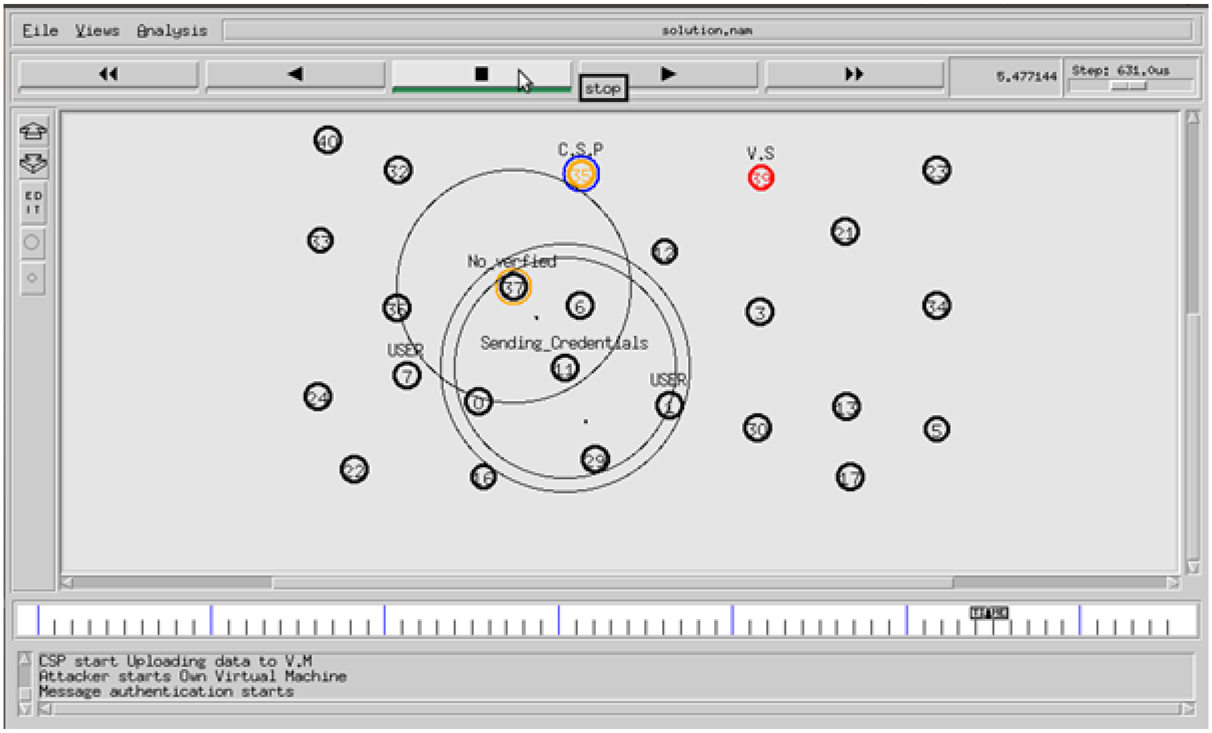
Legitimate user shows their virtual credential to the illegitimate VM shown in Fig.4.16.



```
CSP start Uploading data to V.M
Attacker starts Own Virtual Machine
Message authentication starts
```

Fig. 4.16 User presenting his credential to malicious VM

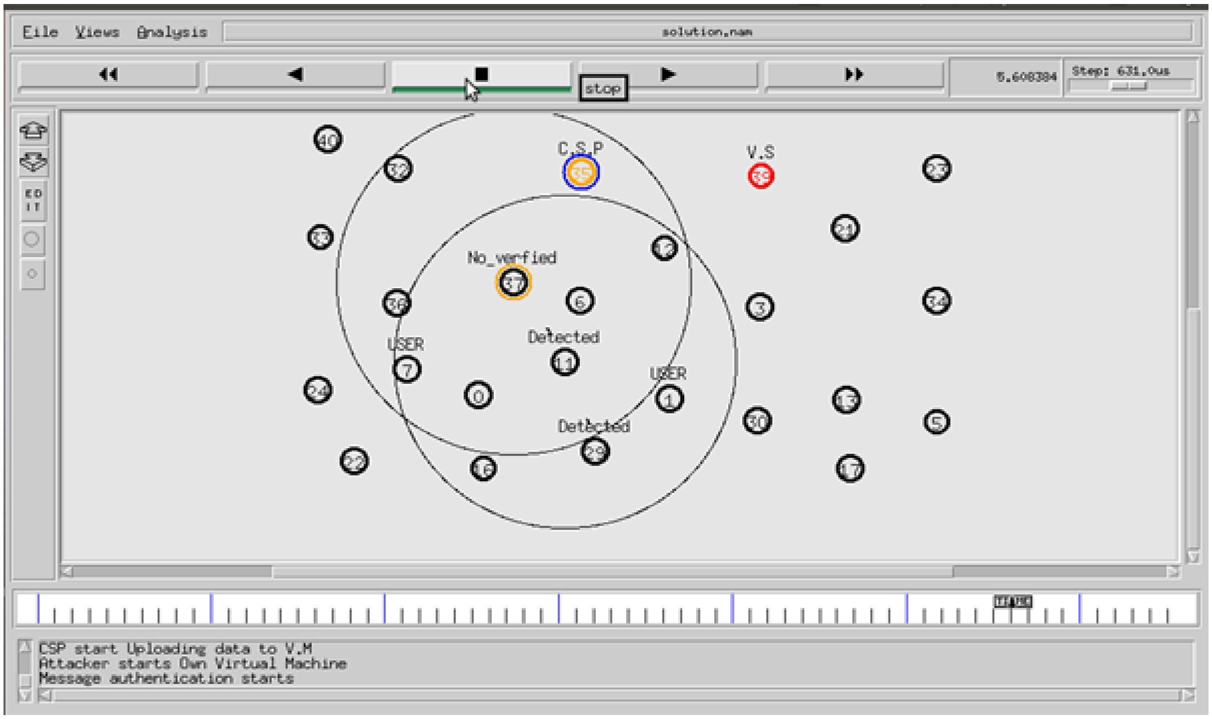
Virtual machine ask for mac address for identify proof as Shown in Fig. 4.17.



```
CSP start Uploading data to V.M
Attacker starts Own Virtual Machine
Message authentication starts
```

Fig.4.17 Attacker failed to give the identity proof

Illegitimate user fails to give it's identify proof and virtual machine identify them as an attacker and communication halts as shown in Fig. 4.18.

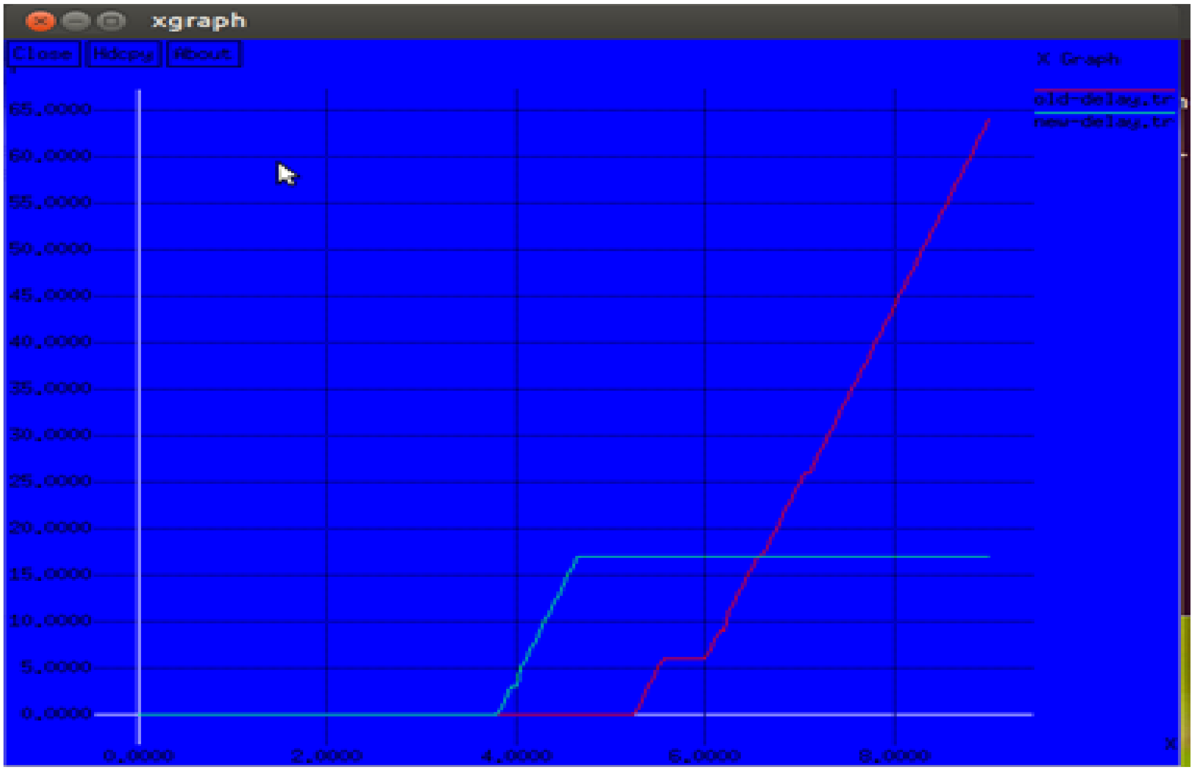


```
CSP start Uploading data to V.M
Attacker starts Own Virtual Machine
Message authentication starts
```

Fig. 4.18 Detection of Attacker and malicious virtual machine

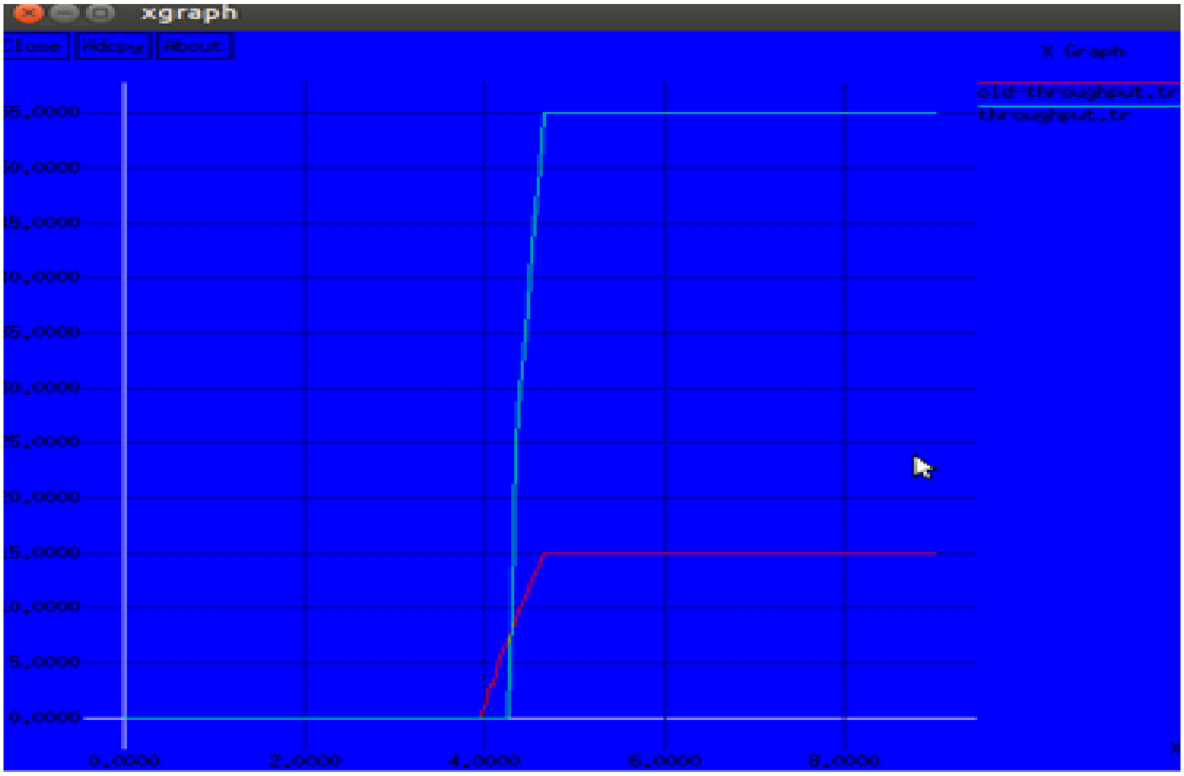
4.4 GRAPHS

Through graphs performance of network is analyzed. A comparison is made between old technique and new proposed technique and shown that new proposed technique is better and increases the performance of the network. The comparison is made between the delay and the throughput analysis of network.



Graph1. Delay

In above graph1 red line shows old delay and green line shows new delay. It concludes the proposed technique graph is better than the existing technique's graph. Here x-axis donates time in second. Y-axis denotes packets per second. When the time increases packet loss increase and this degrade performance of the system. To overcome this new technique is proposed which is better than old technique.



Graph 2 Throughput

In graph 2 red line represent old throughput and green line represent new throughput which is better than existing technique.

CHAPTER 5
CONCLUSION AND FUTURE WORK

CONCLUSION

As cloud computing is accepted widely all around the world, it has many benefits like large storage space, easy access to system anytime and anywhere, cost effective etc. With these benefits of cloud computing some security issues needs to be spotted that assure safe, reliable internet service. As multi-tenancy and virtualization features of cloud computing enhanced the resource utilization. However cloud computing has many security challenges that are exacerbated by virtual resource sharing. The sharing of resources among potential untrusted tenants can result in an increased risk of information leakage due to vulnerability of virtual resources causing side channel attacks or VM escape. For big data application, an access control policy such as RBAC can be used to control the data sharing among cloud customers. In this technique the side channel attack is possible. To isolate the virtual side channel attack KAMAN protocol is used which enhance the performance of network. Through using this proposed technique throughput of network is increased and delay is reduces by reducing the packet lost. Thus give better performance than the old technique.

FUTURE WORK

As in Cloud Computing, the Role Based Access control has some issues like virtual side channel attacks. We tried to avert these attacks by using the KAMAN Protocol. In future if there any other technique that is better than we are proposed, will help in improving the results and network performance.

CHAPTER 6
REFERENCES

[1] A Prasad, et.al "A mechanism design approach to resource procurement in cloud computing", IEEE, vol. 63, issue 1, pp. 17-30, 2014.

[2] Abdulrahman Almutairi, Arif Ghafoor "Risk aware virtual resources management for access control-based cloud datacenters" CERIAS Tech report 2014.

[3] Asad Amir Pirzada, Chris Mcdinald "Kerberos assisted authentication in mobile ad-hoc networks" Australian computer society, inc 26, 2004.

[4] B. Clifford Neuman, "Kerberos: an authentication service for computer networks" IEEE communication magazine September, 1994.

[5] Bibin K Onankunju (2013) "Access Control in Cloud Computing" International Journal of Scientific and Research Publications, Volume 3, Issue 9.

[6] Diogo A. B. Fernandes, Liliana F. B. Soares, Joas V. Gomas, Mario M. Freire Pedro R.M. Inacio, "Security issues in cloud environment: a survey" published online: Springer, 28 September 2013.

[7] Gitanjali (2013) "Policy Specification in Role based Access Control on Clouds" International Journal of Computer Applications (0975 – 8887) Volume 75– No.1.

[8] Gouglidis Antonios (2011) "Towards new access control models for Cloud computing systems" University of Macedonia, Department of Applied Informatics.

[9] K. Alhamazanni, R. Ranjan et.al "An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state of the art" arXiv: 1312.6170, pp. 357-377, 2014.

[10] K. Hashizume, et.al, "An analysis of security issues for cloud computing" j. internet services application, vol. 4, issue 1, pp. 1-13, 2013.

[11] Kanupriyya, Richa Sapra "Role-Based Access-Control Backup and Restoration Ontology" international journal of emerging trends and technology in computer science 2013.

[12] Karsten Sohr, Michel Drouineaud, Gail-Joon Ahn "Analysing and managing Role-based access control policies," IEE transaction on knowledge and data engineering (TKDE), vol.20, no 7, pp. 924-939, July 2008.

[13] Mazhar Ali, et.al, "Security in cloud computing: opportunities and challenges" Elsevier, information sciences 305, pp. 357-383, 2015.

[14] Q. Duan, Y. Yan, et.al, "A survey on service oriented network virtualization toward convergence of networking and cloud computing", IEEE trans. Netw. Service manag. vol. 4, issue 1, pp. 373-392, 2012.

[15] Rabi Prasad Padht, et.al, "Evolution of cloud computing and enabling technologies", IAES, IJ-CLOSER, vol. 1, issue 4, pp. 182-198, 2012.

[16] Ramadan Abdunabi and Indrajit Ray (2008) "Extensions to the Role Based Access Control Model for Newer Computing Paradigms.

[17] Ravi S.Sandhu, Edward. Coynek, Hal L.Feinsteink and Charles E. Youmank "Role Based access control Models" IEEE computer volume 29, no.-2, pages 38-47, February 1996.

[18] Shikha Singh, Binay Kumar pandey, et.al "Cloud computing attacks: a discussion with solution" open journal of mobile computing and cloud computing, 2013.

[19] Shin-jer Yang, Jia-Shin Chen, Kuei- Chin Chen, " A study of security and performance issues in designing Web based applications," in proc. of IEEE international conference on e-business engineering (ICEBE), pp.81-88, October 24-26, 2007.

[20] Shin-jer,Yang, pei-ci Lai, Jyhjong Lin "Design role-based Multi-Tenancy Access control scheme for cloud services" international symposium on biometrics and security technologies, IEE computer society 2013.

[21] Syam Kumar P, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2011.

[22] Vijay Varadharajan, et.al "Counteracting security attacks in virtual machine in the cloud using property based attestation" journal of network and computer applications, vol. 40, pp. 31-35, 2013.

[23] Wei-Tek Tsai, Qihong Shao "Role based access control using reference ontology in clouds" 10th international symposium on autonomous decentralized system, IEEE computer science 2011.

[24] Xiao-Yyong Li, Yong Shi, Yu Guo, Wei Ma, “Multi-Tenancy based access control in cloud,” in proc. Of international conference on computing intelligence and software engineering(CISE),pp. 1-4, Wuhan, China, December 10-12-2010.

[25] Young-Gi Min (2012) “Cloud Computing Security Issues and Access Control Solutions” Journal of Security Engineering.

CHAPTER 7
APPENDIX

KDD	Knowledge Discovery in Database
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
SLA	Service Level Agreement
CSP	Cloud Service Provider
DoS	Denial of Service
VM	Virtual Machine
RBAC	Role Based Access Control
MAC	Mandatory Access Control
DAC	Discretionary Access Control
ACL	Access Control List
SQL	Structure Query Languages
USE	UML-based Specification Environment
UML	Unified Modeling Language
OCL	Object Constraint Language
SWAP	Secure Web Applications Project
MTA	Multi –Tenant Architecture
MTACM	Multi Tenancy Based Access Control Model
RB-MTAC	Role-Based Multi-Tenancy Access Control
KAMAN	Kaman-Kerberos Assistant Mobile Ad-hoc Network
KDC	Key Distribution Centre

AS	Authentication Server
TGS	Ticket Granting Server
TGT	Ticket Granting Ticket
V	Application Server
MAC	Address Media Access Control address
NS	Network Simulator
IP	Internet Protocol
UDP	User Datagram Protocol
RTP	Real Time Transport Protocol
TCP	Transmission Control Protocol
LAN	Local Area Network
FIFO	First In First Out
DARPA	Defense Advanced Research Project Agency
VINT	Virtual Internetwork Test-bed
NAM	Network Animator