

“SMART-CARD AUTHENTICATION”

A Dissertation Proposal submitted

By

Rupinderjit Kaur

To

Department of CSE

In partial fulfilment of the Requirement for the

Award of the Degree of

Master of Technology in CSE

Under the guidance of

Prof. Hardeep Singh

(May2015)

School of Science and Technology

DISSERTATION TOPIC APPROVAL FORM

Name of the Student: Rupinderjit Kaur Registration No. 11305681

Batch: 2013-15

Roll No. B34

Section: _____

Parent Section: _____

Details of Supervisor:

Designation: AP

Name: Hardeep Singh

Qualification: M.Tech

U.I.D. 16869

Research Experience: 9

SPECIALIZATION AREA: Computer

(pick from list of approved specializations given by G.A.U)

PROPOSED TOPICS

- Networks
- 1. Wireless Sensor Network-Authentication
 - 2. Adhoc network
 - 3. Cloud Computing

Hardeep Singh
Signature of Supervisor

PAC Remarks:

quite quite positive about student
that she will publish
paper in good journal.

APPROVAL OF PAC CHAIRPERSON

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

*On a final copy of this form a copy PAC approval will be returned by the student and must be attached to the Final Dissertation Proposal.

*This copy to be submitted to Supervisor.

Signature: 11/10/13

Date:

DECLARATION

I hereby declare that the dissertation proposal entitled, “**Smart-card authentication**” submitted for the M.Tech 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: Rupinderjit Kaur

Reg.No: 11305681

CERTIFICATE OF GUIDE

This is certifying that has completed M. Tech dissertation proposed titled”Smart-Card Authentication” under my guidance and supervision. To the best of my knowledge, the present work is the result oh her original investigation 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 submission and the partial fulfilment of the conditions for the award of M. Tech Computer Science & Engg.

Date:

Signature of Advisor:

Name:

Uid:

ABSTRACT

As the number of user increases to access the network services in large extent, there is need to provide reliable and accurate data among all of them. To provide security from any malicious attack, organisations uses firewalls, antivirus and maintain their systems on regular basis. User authentication is important part of security. Authentication is done with number of parameters like username, password and session keys. The various automated tools and encryption/decryption is used to authenticate users. With these, only the legitimate user can see the contents of communication. Smart card is the one integrated circuit that stores the user's information in secured manner. Smart card authentication becomes major topic to research.

ACKNOWLEDGEMENT

I express my sincere gratitude to Prof. Hardeep Singh, Dept. of Computer Science Engineering, at Lovely Professional University, Jalandhar, India, for his stimulating guidance, continuous encouragement and supervision, generous guidance, help and useful suggestions, throughout the course of present work.

I also wish to extend my thanks to HOD Dalwinder Singh, for constructive suggestions to improve the quality of this research work.

I am extremely thankful to, for providing me infrastructural facilities to work in, without which this work would not have been possible.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGENO.
	Title Page	
	Declaration of the Student	
	Certificate of the Guide	
	Abstract	
	Acknowledgement	
	List of Figures	
Chapter 1	Introduction	
1.1	Importance of Networking	
1.2	Devices in the Network	
1.3	Security in Network	
Chapter 2	Literature Review	
2.1	Literature Survey	
Chapter 3	Present work	
3.1	objective of the study	
3.2	Research Methodology	
3.3	Design and implementation	
Chapter4	Result analysis	
Chapter 5	Summary/Conclusion	
Chapter 8	References	
Chapter 9	Appendix	

List of figures

Figure	Page no
1. Trade off performance	2
2. Types of chips card	5
3. Contact cards	5
4. Contact less smart card	6
5. Password authentication protocol	9
6. Challenge handshake protocol	10
7. MS-CHAP	10
8. Extensive authentication protocol	11
9. Secure socket layer	12
10. Proposed system	29
11. Security test analysis	31
12. Performance analysis	32
13. Security comparison	33

Chapter 1

INTRODUCTION

1. Smart-card

Smart cards are the integrated circuit that stores the user personal and financial information in the secured manner. Smart-cards are the need of fast-growing world. In every organization, users use smart card for various purposes. For secure communication and to protect the information from unauthorized user, there is need of secure parameters. User authentication is one of them. When user start communication, he should be assure about the user at other end. Basically, Smart cards are used to provide identity of documentation, authentication, data storage and application processing. The data store in the smart card is usually associated with value, information and both. Such data is used to process within the card chip. The smart card data is transacted via a card reader that is the part of computing. Systems that are enhanced by smart cards are used in daily life in different applications like healthcare, entertainment, banking and transportation. All of the applications take advantage of security and features provided by using smart card. In these days, markets having machine readable card technologies such as barcode and magnetic strips are used to convert smart cards as a calculated value invested by card owner.

1.1 Need of Smart-Card

Smart cards are used to store and process the financial and personal data. Mostly smart cards improve the security and convenience of any transaction. User identification data is stored in the smart card to make transaction. Smart cards are more reliable to use as compared to other card readable machines like magnetic strips and barcode. There is also low cost required to maintain smart card. Smart card provides the components of system security to exchanging the data contents throughout any network. Smart cards help to maintain protection against security threats from careless storage of passwords to system hacks.

To manage cost of password reset is difficult for any enterprises and organisation. Using smart cards, cost is reduced effectively in enterprises and organisations. There are also multifunctional cards available to use. Such cards use to manage network system access and store value and other kinds of data. Nowadays, people use the smart cards for different functions to perform.

1.2 Applications where smart cards can use

Firstly, smart cards are used as a stored value tool for payphones to reduce theft. With developing of smart cards and other chip cards, people start to use smart cards in different ways e.g. charge cards for credit purchases and for record keeping in place of paper. In many countries, users have been using chip cards for everything like to visit libraries to buy groceries. Nowadays Smart cards are used in government applications. Telecommunication industries use the smart cards in their products such as GSM phones and in TV satellite decoders. People use smart cards for daily tasks include:



Figure 1 Trade-off performance

1.2.1 Telecommunication Industries

Telecommunication companies use smart cards in their products like SIM(Subscriber Identity Module). SIM is basic component of the mobile phones that help to communicate. Every mobile phone has unique identity i.e. stored in the SIM. This unique identity use to maintain the rights and privileges of particular user on the different networks. In such way, one half of the smart cards are used in a year approximately.

1.2.2 To Store values

Smart cards are basically used to store the data contents. The way of storage in smart cards is better option rather than to carry the cash in hand. For multi-chain retailers that administer loyalty programs across different businesses, smart cards can locate and track all data. For such cases, numerous applications are available to use like transportation, parking and entertainment.

1.2.3 To Secure Digital Content And Physical Assets

Instead of storing data in smart cards, these are also used to provide security to physical assets and digital contents. For this, access is provided to authorised user only. Digital video broadcast systems have accepted smart cards as electronic keys for protection. Smart cards are also used as keys to settings of machines for sensitive laboratory equipment like library cards and health club equipments.

1.2.4 E Commerce

It is easy to store the information and cash in electronic form rather than carrying cash in hand. It provides number of benefits to consumers. The smart cards can store personal information that can access with a mouse click instead of fill the specific forms. Smart cards help to control and manage financial transactions with reports and limits. By using smart cards, there is no need to pay extra transaction fees associated with credit cards.

1.2.5 Bank issued Smart cards

Under EMV (Euro pay, MasterCard, VISA) standard, banks have controlled number of smart cards. De –facto cards for bank issuance are available in most of the countries. Smart cards provide security for regular transactions at an increased rate. Smart cards improve the customer service at a large extent and increase trust through improved security.

1.2.6 Healthcare informatics

The new challenges are introduced to protect and maintain the patient data and provide privacy safeguards. These challenges from emergency data to benefits status are addressed with the use of smart cards. Smart cards help to carry data between systems and to sites without systems.

1.2.7 Physical Access

Nowadays most of colleges and universities provide identity cards to their students. The data equipment and department data are accessed by each student or employee according to their status. For this purpose, multifunctional cards can be used to store values in different locations.

1.3 Types of smart card

There are number of smart cards available with multiple functions. To define the types of smart cards, two approaches are considered. First one is how the card data is read and written. Second one is type of chip implanted within the card and depends upon its capability. The basic types of smart cards are:

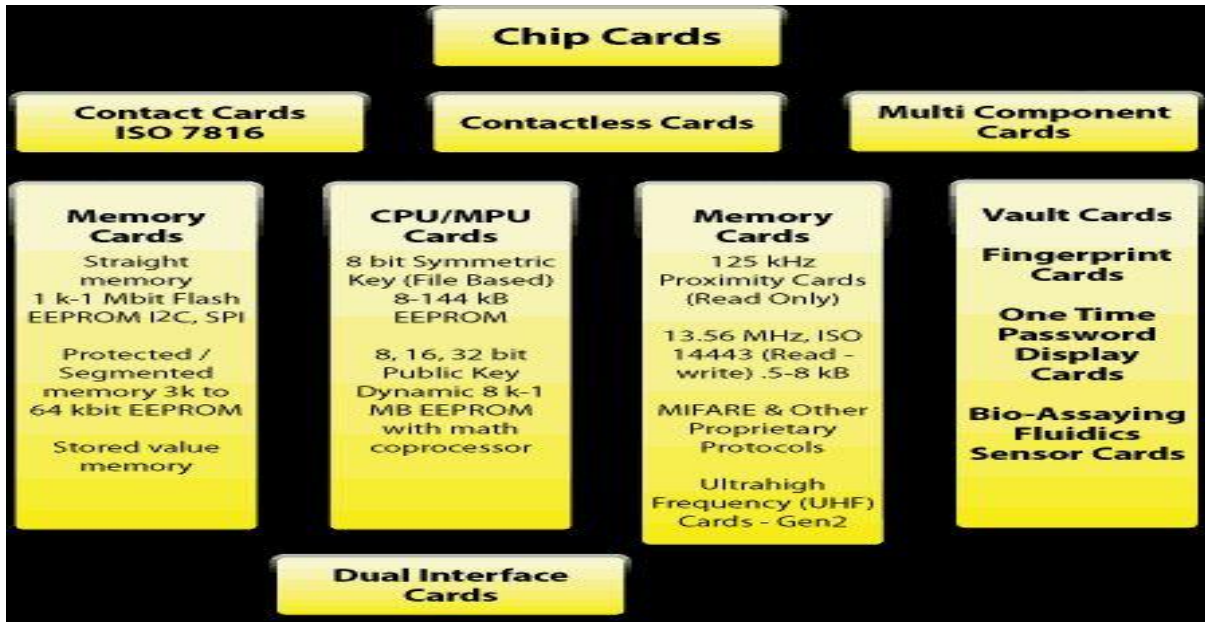


Figure 1.2 Types of Chips Cards

1.3.1 Contact cards

These are the most commonly used cards in which electrical contacts are saved outside of the card reader when insert into the card reader. Because of single function card, it have more cost as compared to other ones.

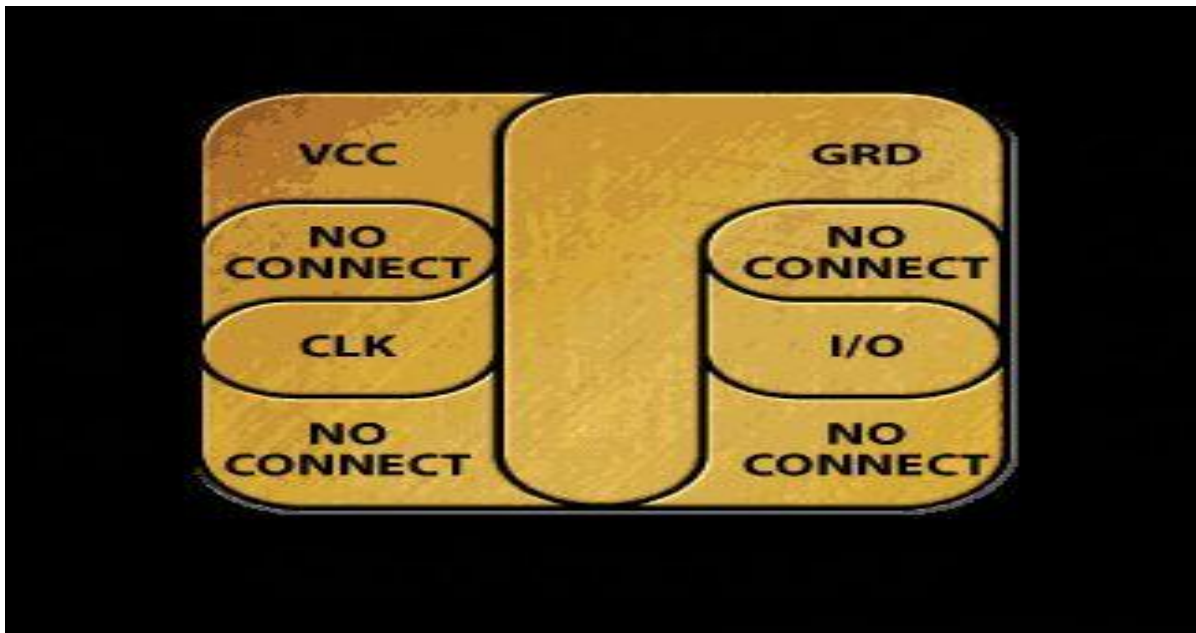


Figure 1.3 Contact Cards

1.3.2 Memory Cards

Memory cards are used to store data but not having its own processing power and cannot manage files to communicate with card reader, there is need of synchronous protocols. Memory cards are further divided into categories: Straight card, protected card and stored value card.

1.3.3 CPU/MPU Microprocessor Multifunctional cards

Multifunctional cards have its own memory to store data and files assigned for specific function or application. In this card, microprocessor and micro-controller are available to manage and control the memory allocation and file access. Debit cards are the example of these cards.

1.3.4 Contactless cards

Contactless cards are used radio frequency between card and card reader without any physical insertion of the card. In these cards, Limited memory is allocated to perform functions and communicate at 125 MHz Contactless cards are divided into number of types. These are:

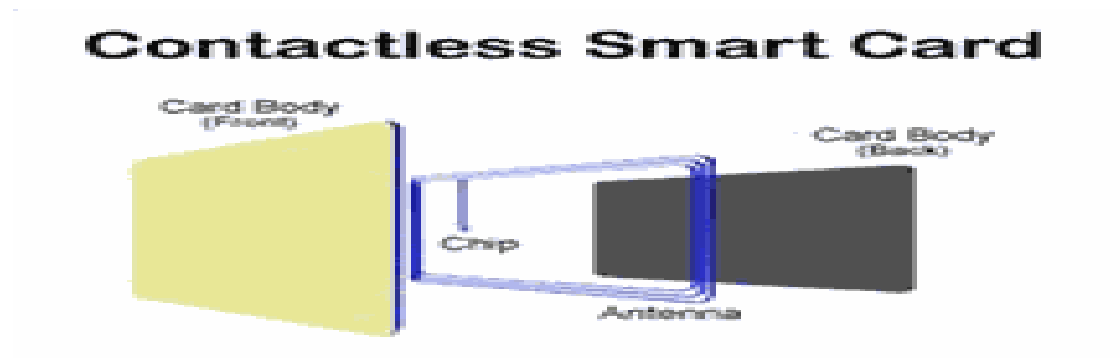


Figure 1.3 Contactless Smart Card

1.3.4.1 Multi-Mode Communication cards

Multi-mode communication cards are cards that have many methods of communication that involves ISO7816 and ISO14443. These cards also include the magnetic-strip and barcodes. These cards are used for identification, authentication and for storing the data. These cards are applicable for business transactions in a secured manner.

1.3.4.2 Hybrid cards

In hybrid cards, multiple chips are included in a same card. These chips are attached to a separate interface to perform multiple functions. The data stored in this card uses independently. These cards are applicable in the specific applications that require separate contact and contactless chip functions. In these cards, data is not shared between multiple chips and helps to secure the data.

1.3.4.3 Dual interface cards.

Dual interface cards are cards that include one chip only to control communication interfaces. In these cards, the chip is attached to the antenna by using hardware connection and bump mechanism.

1.3.4.4 Multi Component cards.

Multi component cards are the cards uses for market applications. The biometric sensor like fingerprint sensors are built in these cards to authenticate user and server and provides security. Some multi component cards are used for industrial purpose that involves one time password to display the data for online transactions. These technologies are used by particular vendor.

1.4 Security for smart card

Smart cards provide number of benefits of portability and security to secure the data contents there are many issues faced to provide security in the smart cards. Sometimes, user uses the cards so far and wide in different applications. Due to advancement in technology, there is needed to ensure data security at a high rate. To secure smart card, following are the features of security need to consider:

1.4.1Data Integrity

Data integrity means to inspect the general characteristics of transaction and document. Data integrity ensures the accuracy of the data contents. Electronic fingerprints are used to achieve data integrity. If there is any change occurs, some parameters identify the tempering contents.

1.4.2 Authentication

Authentication means to confirm about the identity of user involved in the transaction of data and values. To authenticate the user, symmetric and asymmetric keys mechanisms are used. For authentication purpose, hash function algorithm is considered appropriate and helps to implement digital signature.

1.4.3 Non-Repudiation

This eliminates the chances of a transaction to be reputed. This property works as an email system where recipient of data re-hashes the data and verify the digital signature and make a comparison to match both values.

1.4.4 Confidentiality

To protect the data from any attack, there is always needed to encrypt the data contents. Using encryption and decryption process, it is easy to secure data contents for unauthorized access. Cryptography works same as the confidentiality basis and a method to convert the data contents into non-human readable form and again convert modified data contents into readable form. Confidentiality ensures the privacy, uniqueness and integrity of the data and values.

1.5 How Authentication Process carry out to secure the Smart Cards

To protect from various attacks, authentication is important parameter to consider. Administrators have to secure the system, data and values from unauthorized access of intruders and hackers. Several protocols, security policies and number of technologies are implemented to achieve security. To achieve authentication, following features are important to consider:

- Access control
- Data Protection
- Auditing/accountability

Access control means which resources are accessed for authentication. Access control is implemented by specifying permissions for resources and assigns rights to users. Another data

protection means to secure the data when it is transmitted over the channel. The use of encryption and decryption, and public and private keys mechanism provides the protection of data. Authentication is the step to allow users to access the required resources. Mainly user authentication occurs by using user providing personal credentials like user login name, password and user security identity.

1.6 Protocols used to Authenticate Smart-cards

There are number of protocols and security policies implemented to authenticate the smart-cards. These are defined as follows:

1.6.1 Password Authentication Protocol (PAP)

Password authentication protocol is the simplest authentication protocol in which username and password is sent to the remote access server in a plaintext form. To use PAP is discouraged because passwords are easily readable from point to point protocol packets exchanged during authentication process. When older UNIX based remote access server is used to connect, PAP protocol is used but it is not provided more secure authentication.

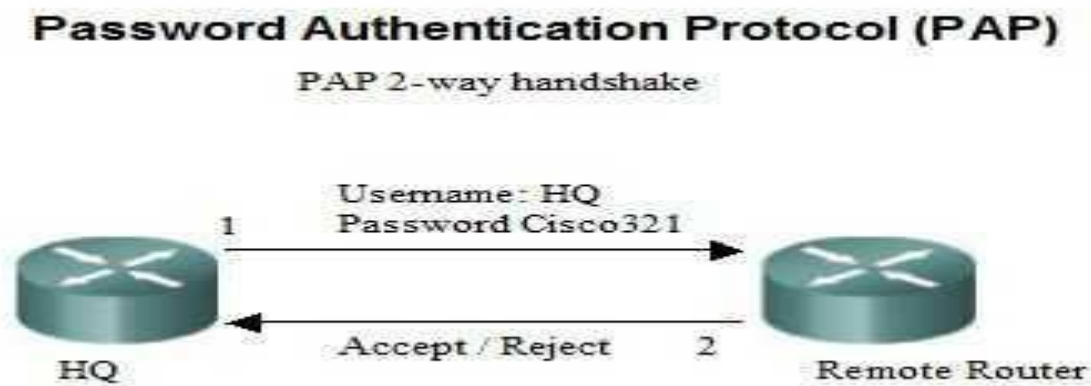


Figure 1.4 Password Authentication Protocol

1.6.2 Challenge Handshake Authentication Protocol

Challenge handshake protocol is the protocol in which authentication of user's password is carried out rather than password itself. In challenge handshake protocol, remote access server sends a challenge to the remote access client. Basically, hash function is used to compute the message value and hash based value is compared with the user's password. The remote access client sends message hash result to the remote access server that already knows hash result and comparison is made using hash algorithm and final result is checked. If the results match to each other, then authenticated user is there otherwise the connection is discarded.

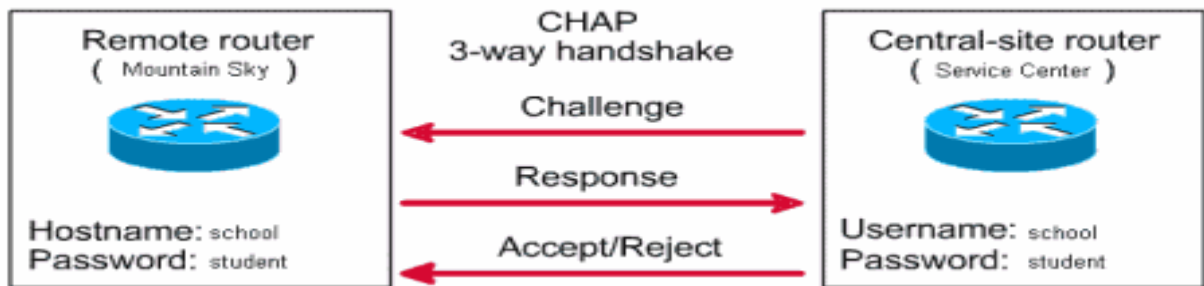


Figure 1.5 Challenge Handshake Protocol

1.6.3 Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

MS-CHAP is the protocol that uses to authenticate remote windows based workstations. Like CHAP protocol, MS-CHAP protocol uses challenge authentication mechanism to authenticate connections and not sent the passwords. In MS-CHAP protocol, message digest4 (MD4) hash algorithm is used for authentication purpose. MS-CHAP also provides services to detect connection errors and changing in the user's password.

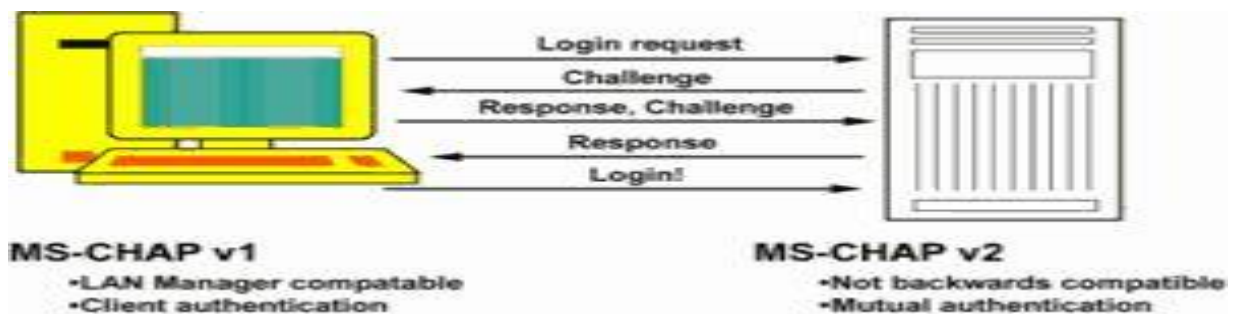


Figure 1.6 MS-CHAPS

1.6.4 Extensible Authentication protocol (EAP)

Extensible Authentication protocol is implemented to response to the increasing demand for authentication methods that uses services such as smart cards, token cards, and crypto calculators. Extensible authentication protocols have further types that provide strong authentication schemes. Strong EAP types offer better services and security against brute-force attacks, dictionary attacks and password guessing attacks as compared to CHAP and MS.

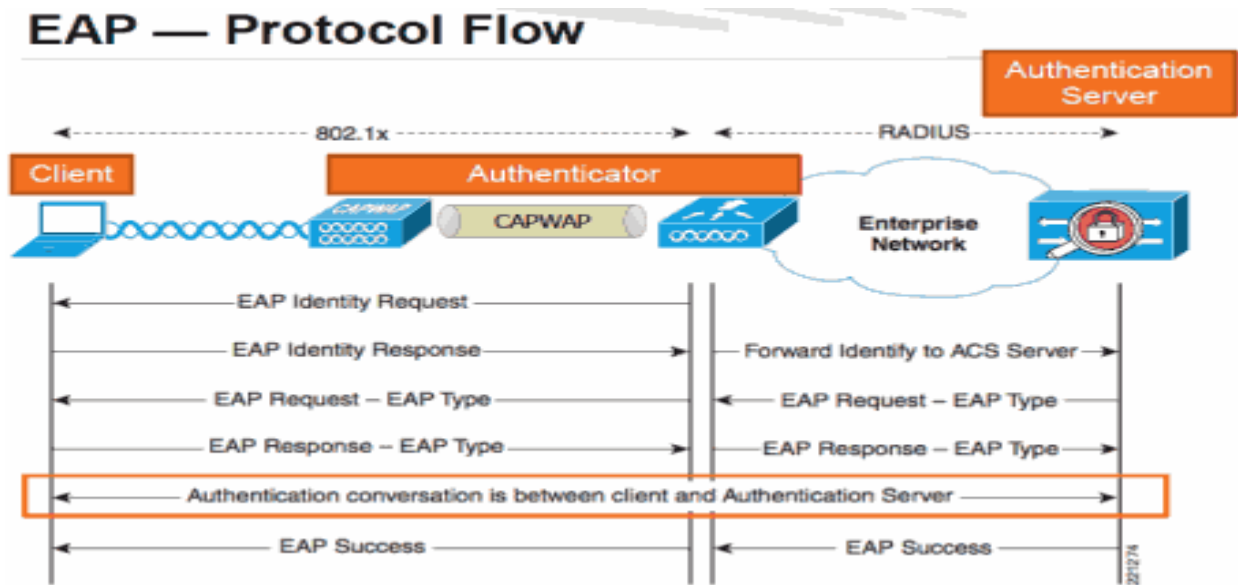


Figure 1.7 Extensive Authentication Protocol

1.6.5 Secure Socket Layer Protocol (SSL)

Secure socket layer protocol is used to provide security for websites with the help of public key technology and secret key technology. SSL protocol is basically supported by web browsers, Microsoft, and Netscape. SSL protocol works mainly at the application layer. To provide authentication using SSL, digital certificates are used to identify the server and user during the connection establishment. In SSL protocol, certificates of two types are used i.e. server certificates and client certificates.

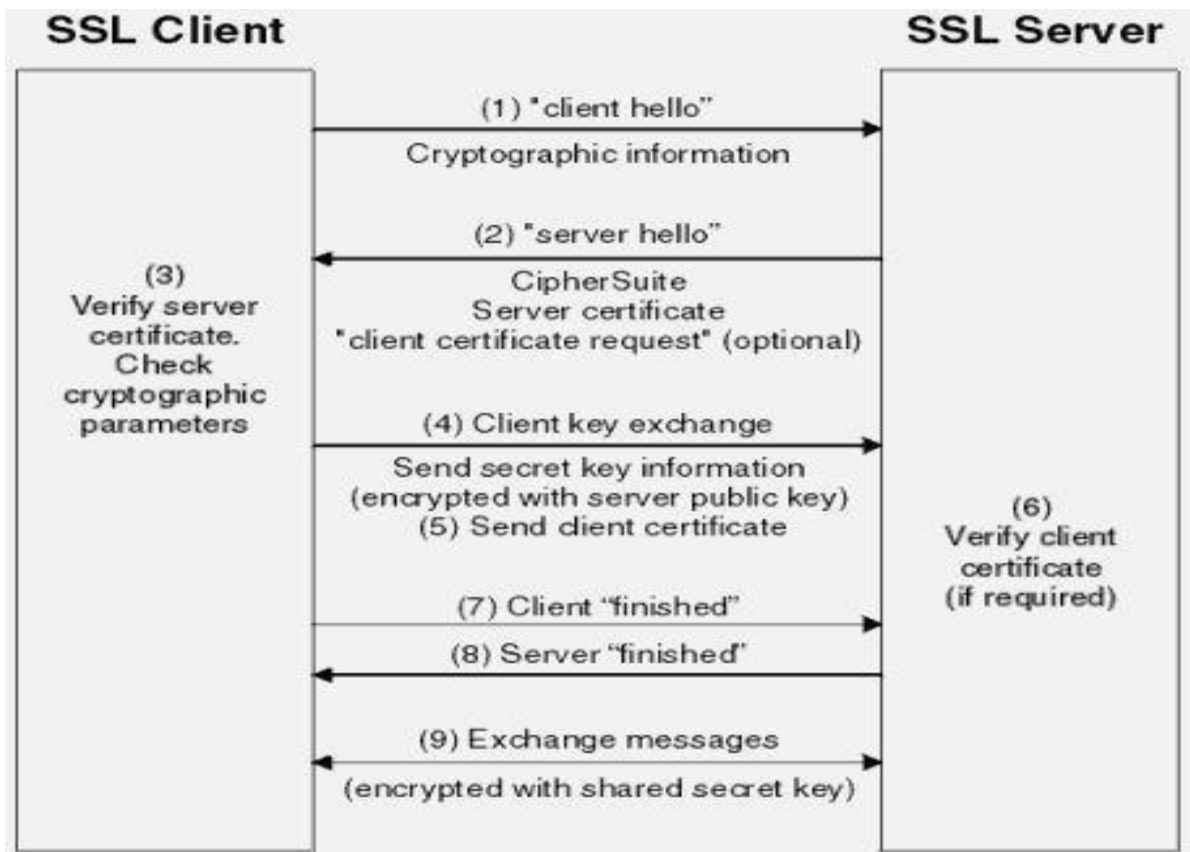


Figure 1.8 Secure Socket Layer

Chapter 2

REVIEW OF LITERATURE

In literature survey, I read the research paper on networking's subfields i.e. Network Security Wireless Adhoc Networks, Wireless Sensor Network and Cloud Computing. The descriptions of Related Research papers are as

Dr. Kennan Balasubramanian in this paper "Secure Implementation of Routing Protocols for Wireless Adhoc Networks" describes the way how to provide security for routing protocols in Wireless Adhoc Networks. Routing is a basically networking function in every communication system including wireless adhoc networks. There are number of attacks like collision attack, impersonation attack, black hole attack, denial of service and wormhole attack that can interrupt the communication services. He analyzes the process to secure the routing protocols like Dynamic Secure Routing (DSR) and Adhoc on Demand Distance Vector (AODV). There are basically two protocols are designed to provide security. One of them is Adhoc on Demand Distance Vector (AODV). AODV is the advancement of Destination Sequenced Distance Vector (DSDV) protocol. AODV initiates a route discovery process using RREQ (Request) and RREP (Reply). The source node broadcasts the RREQ message to its neighbour node and set a timer to wait for reply. If RREQ is lost during transmission, the source node is allowed to broadcast RREQ message again using route discovery mechanism. And if the destination node moves to other location, the node initiates Route Error (RERR) to the affective and active neighbour node. Another one is DSR is a routing protocol which is worked on with caches. In this protocol, two essentials steps are performed like Route Discovery and Route Maintenance. Every node maintains a cache to store the recent discovered path. If any node wants to communicate with other node, it will check the entries of caches. If there is path for that node, source node will send message. Otherwise source node will send request all nearby nodes in the network. Routes maintain will control all the routes and try to manage the failure that occurs in the network. In this paper, Dr. Kennan Balasubramanian proposes these protocols that keep security trade-offs balance and able to satisfy certain security constraints.

Chi-Tsun Cherg (member of IEEE) in this paper “A Delay Aware Data Collection Network Structure for Wireless Sensor Networks” describes to how to save the energy consumption by sensor nodes so that life-time of sensor nodes can increase. Wireless Sensor Network is a network having number of sensing nodes, that can also appear at extreme environment. When transmission of Messages occurs at sensor nodes, life time of these nodes decreases due to high energy consumption. For this, basic method for conserving energy is Clustering method. In this, two basic parts involves Cluster Head and Cluster Member. Cluster Head will collect all the information from the cluster member directly or by multi-hop manner. After that, fusion techniques are used to fuse the collected data. At last, a report of fused data is sent to remote base station. Based on these methods, two clustering algorithm named as LEACH i.e. organized in multiple cluster 2 hop networks(cluster member → cluster head → base station) is proposed. Another clustering algorithm i.e. PEGASIS, organizes into a single chain network is also proposed. In this, a node is elected as cluster head and by minimizing cluster heads, the energy consumed in long distance transmission is further minimized. To implement these methods, Chi Tsun Cherg uses the algorithm of Minimum Spanning Tree (MST) in this paper.

Hassan Zia fat in this paper “A method For Reduction of Energy Consumption in Wireless Sensor Network using Neural Network” describes how to reduce the energy consumption in Wireless Sensor Network using neural network. Wireless sensor nodes are battery-powered devices that can consume energy. Because of more energy consumption, lifetime of these nodes decreases. Such network requires continues monitoring so that lifetime and network coverage of these network are of great concerns. And it is impossible to replace or recharge the dead sensor nodes. Hassan Zia fat proposes energy based clustering protocol through using of Self-organising Map (SOM) neural networks (called EBC-S). His work is related to LEACH-Centralised algorithm but it is quite different from it. Self Organising Map based neural network is followed by K-means and present a considerable profit. This proposed protocol is able to cluster the nodes not only based on their coordinates but also based on their energy levels in each set-up phase by using SOM capability on multi-dimensional data classification. In The Cluster setup phase, the distance is minimised using Euclidean distance in learning phase. This phase is repeated until stabilization occurs. After that, SOM cluster n samples into m map units and this input is sent to K-Means algorithm that partitions the data

set into k subsets so that all objects in a given dataset are closest to same centroid. He describes cluster head is selected based on the following: Sensor node having maximum energy level, nearest sensor to base station and nearest sensor to centroid of clusters.

C.M. Poole and J.V Trappe in their paper “Radiotherapy Monte Carlo simulation uses cloud computing technology” describe a technique that allows for Monte Carlo radiotherapy calculations to perform. For this, they use GEANT4 and then execute on the cloud that helps to reduce cost and calculate the required time for such calculations. They introduce the time completion that seems to decrease by $1/n$ for n systems. The GEANT4 is a toolkit that is used in various fields like high energy physics and widely use for radiotherapy treatment plans. For their simulation work, they execute on Amazon Elastic Compute Cloud that provides usefulness of cloud computing for radiotherapy dose calculation. Their results show the wide range of EC2 instance types and available configurations that allows it to use in different fields of science. To compute these calculations, there is need of large amount of CPU time and RAM. Using this technique, it become easy for GEANT4 user to perform simulating calculations in a distributed computing environment with lower cost. For this, there is no need of specific hardware to allocate. They introduce HOPE (hospital platform for e-health) to use for verification purpose in radiotherapy treatment.

Chang Choi, Junho Choi and Pankoo Kim in their paper “Ontology Based Access Control model for Security Policy reasoning in cloud computing” introduce about the issues faced in cloud computing. There are many problems related to the security of the system like virtualization and big-data processing. In cloud computing environments, there are requirement of control and management of data access. According to their work, the services related to cloud differs with different security policies. In their paper, they introduce new scheme of Onto-ACM (Ontology based Access Control Model). Using this model, it become easy to address the difference in access control between service provider and users. Their model is used for applying the access level to the resources based on the ontology reasoning. To prevent intrusions, access control model are required for detection and prevention purpose. The paper provides an access control model for context, performance level, condition on permission and to define policy of access for user and administrator. In their work, they

analyze the basic requirement of access control model using the general characteristics of cloud computing. The efficiency and management level features can achieve using this model. To authorize particular user, context ontology based information is used through various interferences. Using proposed model, limitations of cloud computing can overcome.

Philippe Owezarski, Deep Medhi and Jorge Lobo in their paper “Network and Service Management for cloud computing and Data centres” explains about technical sessions, and tutorials that focus on the issues and services related to the network system. They evaluate the definition and new formulations of cryptography problems. There are many features of information processing like self service of user, computation of power and resources. They define service of delivery like software as a service and platform as a service. They uses mainly two concepts to introduce the cloud computing. These are virtualization and distributed computing on demand that provides new formulation for cryptography. There is need of elastic services to operate efficiently in a network. According to their work, there is requirement of specific properties of cloud information communication like elasticity to develop new statements of problems for information protection, designing of protocols, security assessments and implementation of cryptography and stenography system. The asymmetric of computation provides new statements of issues that become effective for performance basis and resources used in the networks.

Paul Manuel in his paper “A Trust Model of Cloud Computing based on the Quality of Service” describes a model required to ensure quality of service for data. For cloud computing, trust is the important factor to consider. Trust basically depends on the resources allocated for cloud infrastructure. The main features like availability, data integrity, reliability and efficiency are used to measure trust value. According to his work, service level agreement is implemented, to combine the quality of service requirement of user and resources allocation. They consider their models provide best service as compared to other first in first out models. To compute the trust value in the cloud computing, they give a particular formula of computation. The auditing and accountability is considered as parameters to compute trust value. They carry out experiments in a real environment like Linux, UNIX and MS platform. To architect a trust model, they uses other models i.e. capability based models, behaviour

based models and identity based models. These models help them to select particular types of resources according to the proposed scheme. To carry out job process, resource having highest value selected for processing purpose. According to their work, three factors like cost, security and networking speed are considered to ensure quality of service requirement of users. In this paper, they describe the architecture of QOS model in cloud computing their scheme is applicable for the real time applications in an efficient way.

Euu Su Jeong and Dong Hoon Lee in their paper “A Generic Partial Energy Scheme for Low Power Mobile Devices” introduce the scheme for content protection. In business days, it become necessary to allow only legitimate user to access important data contents and give privileges to access the system and network. To secure the data contents, encryption and decryption is used in several applications of systems like mobile devices. Their work evaluates the partial encryption scheme for low power mobile devices. As the internet grows day by day, downloading and uploading process on mobile devices is carried out in large extent. Euu Su Jeong and Dong Hoon Lee introduce a general architecture for partial encryption of downloadable and real time application data. Their proposed scheme actually works for real world multimedia contents and help to reduce time overhead due to decryption. Due to this scheme, power overhead also reduces at a large extent. Their scheme is applicable for multimedia contents on mobile devices and any kind of data contents like image, video and audio data can process. Data type flexibility, security and effective costs are general advantages of their scheme. They improved the time of decryption on mobiles. To implement OMA-DRM for real world application, proposed scheme can be used. The efficiency of algorithm used in proposed scheme is applicable for low power mobiles devices.

Hong Yu and Ting Zhang in their paper “Enabling End to End Secure Communication between Wireless Sensor network and internet” describes that sensors not only collect and process the data at the internet nodes and transform into knowledge, information and wisdom and into services that are beneficial for humans. But by using sensors in the network, human can access, control and manage the sensors nodes in the wireless network through the nodes in the internet. The number of protocols is developed to work on the symmetric authentication and key management based on the public key algorithms. The main issues faced in such cases

are resource constraint in sensor nodes that interrupt the sensor's processing. The security mechanisms developed for wireless sensor networks focuses on the key management at the data link layer. They propose a secure end to end communication for WST in wireless sensor networks and follow an asymmetric approach for authentication and key arrangement purpose. Their scheme works for identify the users in a secured manner and resists various attacks. According to their work, cost of resources reduces in the terms of processing and storage. Using their scheme, main workload and access control is shifted to the gateway instead of sensor node itself. According to their work, result shows that computation and communication overhead is reduced by 50% and 16.4%. Their work is useful for real applications in several aspects.

Georgios Kambourak in his paper "Exposing Mobile Malware from inside" introduces number of malware created mainly for the mobile phones. In today, it become serious threats. As the wire, wireless and cellular networks is developed day by day, number of malicious software are also increased and creates or affects the network badly. The services associated with particular network are vulnerable to damage i.e. main risk in a specific network. They introduced such risks to resolve using static solutions. They considered a full fledged tool to analyze software of iOS. Using this tool, the occurrences of malicious content in the software are traced or checked according to them, his work is appropriate for practical applications to detect malicious content using dynamic analyses. It become easy to trace the actual values that are passed to a method when it is called and that are going to returned from called method. According to him, there are problem of detection in the previous work that he improved. Therefore he considered API oriented malware detection proposals for Android and iOS platform. He works on iDMA to create profile of number of widely used iOS applications the\at provides security and reduce vulnerability in practical applications.

Victor, Khader and Mehta in their paper" Build an IEEE 802.15.4 Wireless Sensor Network for Emergency Response Notification for Indoor Situations" introduces emergency respone system of future. In today's life, different types of emergency in indoor environment occur. To provide responses for such situations and provide protection to resources is difficult. They

identify new emergency response system that reports the emergency to the users in different forms like send SMS on the mobile phones and so on. Because of low cost and easy of deployment wireless sensor network emergency response system prefer for future use. Like temperature and others factors are considered for WSN emergency response system. This response system mainly focuses on aspect of emergency detection which is fire, gas leaks, gunman on campus and weather changes that mostly occur at numbers of campuses. This systems reduces the false positives and response time in a cost effective way. In this system, various efficient methods can be incorporated to validate threat by adding some additional options to the sensors like image processing and multiple sensors.

Hui Wang and Nazim Agoulmine in their paper “Utility maximization Approach for Information Communication Tradeoff in Wireless Body Area Networks” describe deployment of biomedical sensors around the human body with the help of Wireless Body Area Network. There is dramatic change or developments occur in the area of healthcare systems. There is mostly large amount of data regarding to the patients available in hospitals and clinics. When resources of biomedical sensors are limited to use, it become impossible to provides efficiency. Hui Wang and Nazim Agoulmine provide an idea to reduce the load of sensors that depends between data and diseases that detect. For this, there is needed to make advancements to save energy of sensors. Their idea is basically show how to lifetime of medical Wireless Body Area Networks extend by taking advantages of relation between information about disease and sensing data to provide best medical sensor’ s scheduling. The group of some sensors can used to collect required information for correct diagnosis. Their algorithm achieves high performance to save energy of sensors and delay to detect particular disease. The information based sensor tasking has proposed by them. For this, information validation time and diseases features identification are required and these factors having important impact on the performance of the diagnosis and also on lifetime of wireless body area networks.

Mohammad Fathi and Vafa Maihami in this paper “Reinforcement Learning for Multiple Access Control in Wireless Sensor Networks” explains about the model and open issues of wireless sensor network. According to their work, Wireless Sensor Network is network in

which node sense, collect and forward target data to the centralized system in a effective manner. They introduce a particular protocol i.e. MAC (Medium Access Control) protocol available for wireless sensor network. With this protocol, nodes coordinate for a shared channel to avoid interference between nodes. In wireless sensor network, application and networking issues are occurred and need to resolve. The areas where this technology can deploy having number of challenges. When communication is not occurred between nodes, the energy of nodes are wasted in large extent. The cause of such wastages is mainly to listen the channel in idle mode. To overcome such limitations, energy efficient multiple access control schemes are developed. In this paper, Mohammad Fathi and Vafa Maihami present comparative review and a multi reinforcement learning framework for MAC (Multi Access Control) design in wireless sensor networks. They also provides information about challenges and open issues of distributed MAC design using reinforcement learning. They have introduced open issues like Space complexity, Time complexity, Update Q Table, Reward function and Step size.

Jing Chao in his paper” An improved Remote Password Authentication Scheme with Smartcard” evaluate mainly about Security Performance. Jing Chao proposed a two factor user authentication scheme. In this paper, he analysed the authentication scheme for remote user. He introduced a dynamic id for user that is not remained same in each case. According to his work, password was not involved in verification phase in every time. There was not need of password value to calculate at each phase of authentication. He resisted the password guessing attack and replay attack. With such scheme, costs become less to involve security in different fields. It improves the mutual authentication between user and server. He proposed an improved remote password authentication based on remote ID. In his scheme, password is not involved in calculation of verification phase. Because of this, scheme having less cost as compare to other ones. As development of internet increases day by day, authentication uses in different fields on regular basis. His scheme resists password guessing attack, user masquerade attack and server masquerade attack. His scheme provides efficient performance.

Wang and Ma in this paper “Security flaws in a Smartcard based Authentication Scheme for Multi-server environment” proposed a smartcard authentication with multi-server

environment scheme. By using this scheme, he overcomes the different attacks i.e impersonation attack and offline password attack. Multi-server scheme provided different services to register at different locations by users. But In single-server environment, user needs to register repeatedly at each location. For this, he used hash function to improve the scheme. There are also different stages involved to login, authentication and verification. Every stage performed different functions. That authentication scheme based on multi-server environment helps to protect user from different attacks and introduced scheme that was useful for practical applications.

Jiang Hong Wei in this paper “Cryptanalysis and Improvement of a Robust Smart Card Authentication scheme for Multi-server Architecture” introduced remote user access with multi-server authentication scheme. By using this scheme, remote user may access services provided by different server. To protect user form attacks, they introduced username and password based scheme with multi-server architecture. First they analysed the pippel’s scheme that cannot resist the offline password attack. That’s why they introduced new scheme with BAN logic. This scheme is not more practically secure but provided different functions like password change phase. The analysis of efficiency and security describes that his scheme is not only appropriate for security purpose like forward secrecy and authentication, but also appropriate for practical applications. This scheme resists number of attacks e.g. offline password guessing attack and replay attacks.

Liu Wen- hao in this paper “Robust Password and Smart Card based Authentication Scheme for Smart Card Revocation” worked at authentication scheme. By this scheme, a session key generated for user and server after authentication of user and server. Smart card stolen attacks and password guessing attacks are main key points to analyse. By analysing these, a new smartcard revocation scheme proposed to provide efficient security and authentication. He worked at the weakness of not having exact forward secrecy. To design a new scheme, a nonce is introduced to use in login, authentication and registration phase. Diffie-hellman algorithm used to make a session key for user and server. User can change their password in this scheme. This scheme improved the efficiency and security performance in real applications.

Yongg Wang in his paper “Password Protected Smart Cards and Memory stick against Off-Line Dictionary Attack” describes security requirements is most important to attain for user that accessing internet. Password Protected smart cards are used for remote authentication. There are several protocols defined for password protected smart cards. These protocols are used to provide authentication between client and the server that access remotely. In this paper, he mainly focuses upon the password based authentication between smart card owner and smart card reader. To authenticate the smart card, user inserts smart card into an untrusted smart card reader and enters the password. But there is no guarantee to secure from impersonation of card in future. To provide guarantee against impersonation of card, new scheme is introduced by him. The new proposed scheme is used to provide security against number of attacks like insider attack, replay attack, and impersonation attacks. For security purpose, another case i.e. stolen card attack is considered. When smart card is stolen in future, adversary could not use the smart card by impersonating the smart card owner. To overcome such cases, new password protected authentication scheme is used to secure the systems. This proposed scheme is applicable for real time applications.

Qi Xie and Wen Hao Liu in their paper “Robust password and smart card based authentication scheme with smart card revocation” explains user authentication scheme. Such schemes are used to authenticate the user and server using session keys for communication on the internet. To resist the password guessing attack and smart card stolen card, various user authentication protocols are proposed. These are two major problems to design the smart card for user authentication scheme. Very recently, li and lee was identified a smart card and password based user authentication protocol that resists these attacks. In this paper, Qi Xie and Wen Hao proposed a new scheme that shows previously proposed scheme vulnerable with offline-password guessing attack. When the information stored in a smart card, this information is extracted but not provided forward secrecy. Then they proposed a new robust authentication scheme that provides security against different attacks and authenticate the user and server in a secured manner. In their scheme, they use a specific tool named as Pro Verif based on

applied pi calculus for verification purpose. Using this tool, the proposed scheme ensures the security and authentication of user and server.

Jongpil Kim and Sungik Jun in their paper “Authentication and Key Agreement Method for Home Networks Using a Smart Card” explains about the authentication of home networks. To secure the home networks remotely, they introduced a new proposed scheme. For authentication purpose, they uses strong authentication and key management method for home network system. Smart cards are used to store the credentials information of user. The public and private key combination is used to provide security against different attacks. To secure the home network system, session keys are used. By using this scheme, it becomes difficult to access the personal information of user. The 3GPP security system is used to secure the home network systems. The symmetric key algorithm features are added to home network systems Using their scheme, new additional features are added to encrypt the data contents.

Youn-Hee Gil and Yongwha Chung in their paper “Performance Analysis of Smart Card-Based Fingerprint Recognition for Secure User Authentication” introduce us with electronic world to provide security and confidentiality against various attacks. The authentication of specific user is important in these days. Instead of using personal identification number in smart cards, the use of biometrics method to identify a particular person has many advantages. There is also number of issues introduces to use biometrics features into smart cards. Some authentication algorithms due to resource constrained into smart cards are not operated in real time applications. That’s why it creates issue upon the use of such features. To resolve such issues, they introduce a new scheme to use. In this paper, they describe about the light weight finger recognition algorithm. Using this proposed scheme, they combine the features of algorithm into the smart card. The smart cards are designed in such a way that it becomes easy to store the user’s personal data contents and biometrics parameters. To secure the smart cards, newly propose scheme is effective and efficient to use. By using this algorithm, performance increases at a high rate. This proposed scheme works for real-time applications.

Manoj Kumar and Aavushi Balvan “Security Vulnerabilities of a Novel Remote User Authentication Scheme Using Smart Card Based on ECDLP” in their paper describes about the proposed scheme. Their new proposed is implemented on the based of Elliptic Curve Discrete Algorithm Problem. This algorithm is used for user authentication that login remotely to access the system using the smart card. This paper actually analyzes Jena et al.’s proposed scheme. Their scheme works to remove the security threats. This scheme is used to improve mutual authentication, session key generation to carry out secure communication throughout the network. The proposed scheme uses to change the password capability i.e. not given by previous scheme of Jena et al. according to Manoj Kumar and Aavushi Balvan, they have overcome weakness of previously proposed scheme by Jena et al. that scheme is not applicable for real time application and vulnerable of some serious security threats.

Ashok Kumar Das and Adrijit Goaswani(2013) “Security Analysis of an Efficient Smart Card-Based Remote User Authentication Scheme Using Hash Function” explains about user authentication scheme. To authenticate specific user, there is always a remote server for verification. The number of user authentication schemes is proposed. For authentication and security purpose, several schemes use the mechanism of biometrics smart card and password. A password based user authentication scheme proposed by Sonawanshi. In her proposed scheme, she uses smart card mechanism with hash function and bitwise XOR operation. Hash function is more effective to provide security and authenticate the user trustworthily. The number of known attacks like replay attack, impersonation attack and known- key attack are prevented with the help of her hash function based scheme. Ashok Kumar and Adrijit Gosewani overcome weaknesses of Sonawanshi’s scheme. They identify several attacks like offline password guessing attack and stolen card attack cannot be resolved by her scheme. To overcome these problems, they proposed a new scheme of user authentication.

Hang Tu and Neeraj Kumar in their paper “An improved authentication protocol for session initiation protocol using smart card” describes a protocol that used to control communication on the internet. To secure the communication on the internet, several authentication algorithms and protocols are proposed. There is one protocol named as session initiation

protocol (SIP) used signaling protocol. The session initiation protocol is responsible to establish, maintain and terminate the sessions. The authenticated key agreement protocol for session initiation protocol was proposed by Zhang et al. For this protocol, he used smart card. Hang Tu and Neeraj Kumar identified number of attacks possible on Zhang's scheme. In this paper, they mentioned impersonation attack possible. Then, they proposed an improved protocol to resolve the weaknesses of previous work. Performance and security analysis shows effective improvement as compared to Zhang et al. protocol.

in this paper “An enhancement of Smart-Card Authentication Scheme for Multi-server Architecture” User authentication is an important security issue for network based services. Multi-server authentication scheme resolves the repeated registration problem of single-server authentication scenario where the user has to register at different servers to access different types of network services. Recently, Pippel et al. proposed a smart card authentication scheme for multi-server architecture. They claimed that their scheme has some advantages and can resist kinds of attacks. This paper overcomes the weakness of Pippel's proposed scheme. In scheme, there are three parties, i.e. the users, servers, and the registration centre (RC), where the registration centre is responsible for the initialization of the system, the registration of the servers and the users, and the number of the servers is not fixed. Our scheme also contains four phases, i.e. the initialization phase, registration phase, login and authentication phase, and password change phase. To initialize the system, RC selects a large prime number p (of 1024 bits), and selects a generator $g \in \mathbb{Z}^*_p$. Besides, RC chooses a one way hash function $h(\cdot)$, and two secret keys x and y as the system parameters, where the binary length of x and y should be large enough to resist dictionary attack. In the proposed multi-server user authentication system, all the servers and the users need to register themselves to the RC, and the registration phase contains the server registration phase and user registration phase. In Login and Authentication Phase, This phase involves four steps to perform login and authenticate user. In Password Change Phase, This phase is invoked when U_i wants to change the password. U_i inserts the smart card into the card reader and keys in the identity UID_i and password PWD_i . In this paper, the weaknesses of a recently proposed user authentication scheme for multi-server architecture by Pippel et al. analyses and the analysis results show that it is more security and efficient than Pippel et al.'s scheme.

Chapter 3

PRESENT WORK

Today's Security is the major concern for providing confidentiality, integrity, and authenticity to the data to be shared communication. Smart card is the integrated circuit that stores the personal information of user. In these days, smart cards are more popular indifferent organisation. For this, authentication is the main concern to authenticate original user of smart card. There are number of ways to attack the system and fetch the user's useful information for financial use or something else. The proposed scheme will work to provide authentication to users and servers. Authentication is the feature that makes system secure at large extent. With authentication, large number of attacks can resist. The proposed scheme will be useful for organisation, institutions and enterprises to authenticate the original user. As the number of users increases to use the internet, remote access is popular in different fields to share information. Using proposed scheme, users can register at different location using multi-server authentication environment. Because of this, proposed authentication scheme will work in practical applications.

3.1 OBJECTIVE OF THE STUDY

In this section, we define the main objectives of study smart card authentication is an popular research in terms of security for network services. The proposed scheme will carry out with following objectives:

- Analysis the existing scheme and its relevant work.
- To evaluate the security authentication in multi-server architecture.
- To enhance the security using session tokens.
- To improve data security using session tokens.

3.2 RESEARCH METHODOLOGY

In this section, research methodology is described. Research methodology of proposed work will be:

- Implement the multi-server architecture.
- Implement security test application.
- Evaluate multi-server architecture.
- Enhance security using token mechanism
- Evaluate new updated system
- Present result analysis.

3.3 Design and Implementation

3.3.1 Proposed Algorithm:

At user Interface:

- Accept User and Password as input.
- Compute P' password encrypted string.
- Check if $P' = P$
- Generate a Session token, timestamp and nonce.
- Combine session token with P'.

At Server:

- Check identity UID.
- If true, generate nonce and save session id with user id and associate with user.
- Computes and send authentication results to user.

At User:

- Use session ID and timestamp for further communications.

As proposed technique is developed in MATLAB 2013, user is authenticated using session tokens. The following figure shows the result of authenticated user with specific session id. In this code, number of code files like user authentication, server, stolen card attack and impersonation attack code files. With the help of these code files, the result shows comparison and performance analysis of authentication scheme. In the proposed scheme, user inputs the data as username and password. After that, such information is combined with the session id, timestamp and token value. The password is encrypted with keys. After encryption, session token value is combined with the password. At the other end of server, server checks the User

ID and allocates a specific session id to the particular user. The session id is used for further communication. The graph shows comparison and performance analysis. For authentication of user, session id and timestamp value is used. The code of authentication of user having specific value is entered by user used to check whether the user is authenticated or not. The particular length of password is assigned to know legitimate user. In authentication phase, password of specific length and nonce is generated to compute final result. For comparison purpose, three attacks like impersonation attack, insider attack and stolen card attack are resisted. In comparison analysis shows that existing work takes more time and performance is not efficient. To enhance the performance, proposed scheme is used.

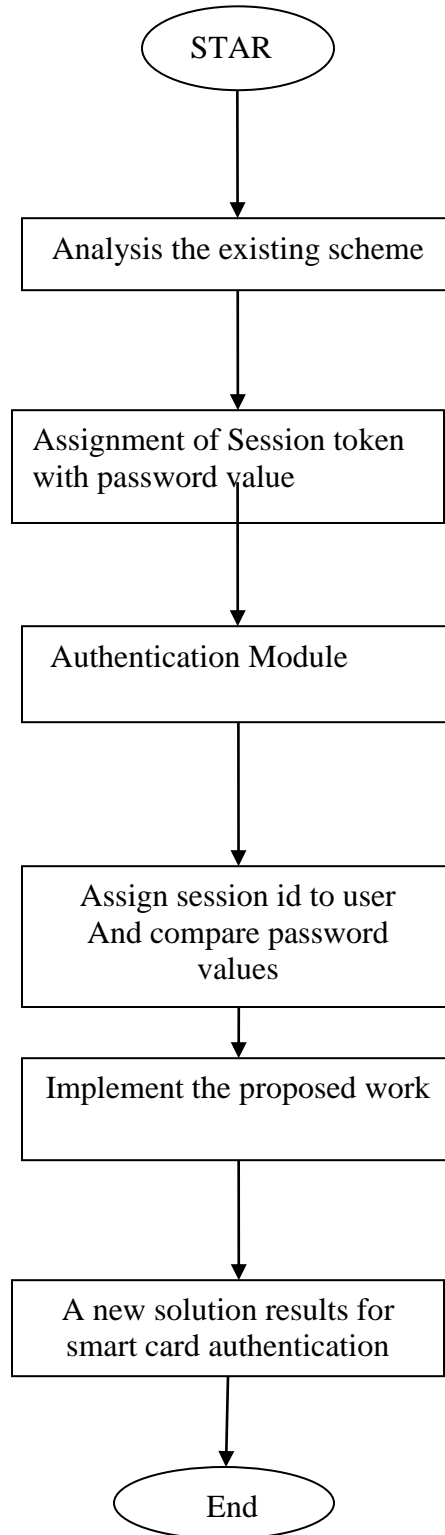


Figure 1.9 Flow chart of proposed scheme

Chapter 4

Result Analysis

By using proposed scheme of smart card authentication, weakness of existing scheme will analyse. A new expected smart card authentication scheme with multi server environment for remote user will be proposed. The efficiency and security performance will be improved to authenticate user and server. The proposed scheme will resist specific attack to overcome weakness of previous work.

Input parameter:

Request Servers = 5

Authentication Servers= 3

Clients= 20

Test Name	Existing Result	Enhanced Result
Without verification table	Yes	Yes
Choose and change password freely	Yes	Yes
Early wrong password detection	Yes	Yes
Proper mutual authentication	No	Yes
Correct session key agreement	Yes	Yes
Resist impersonation attack	No	Yes

Figure 2.0 security test analysis

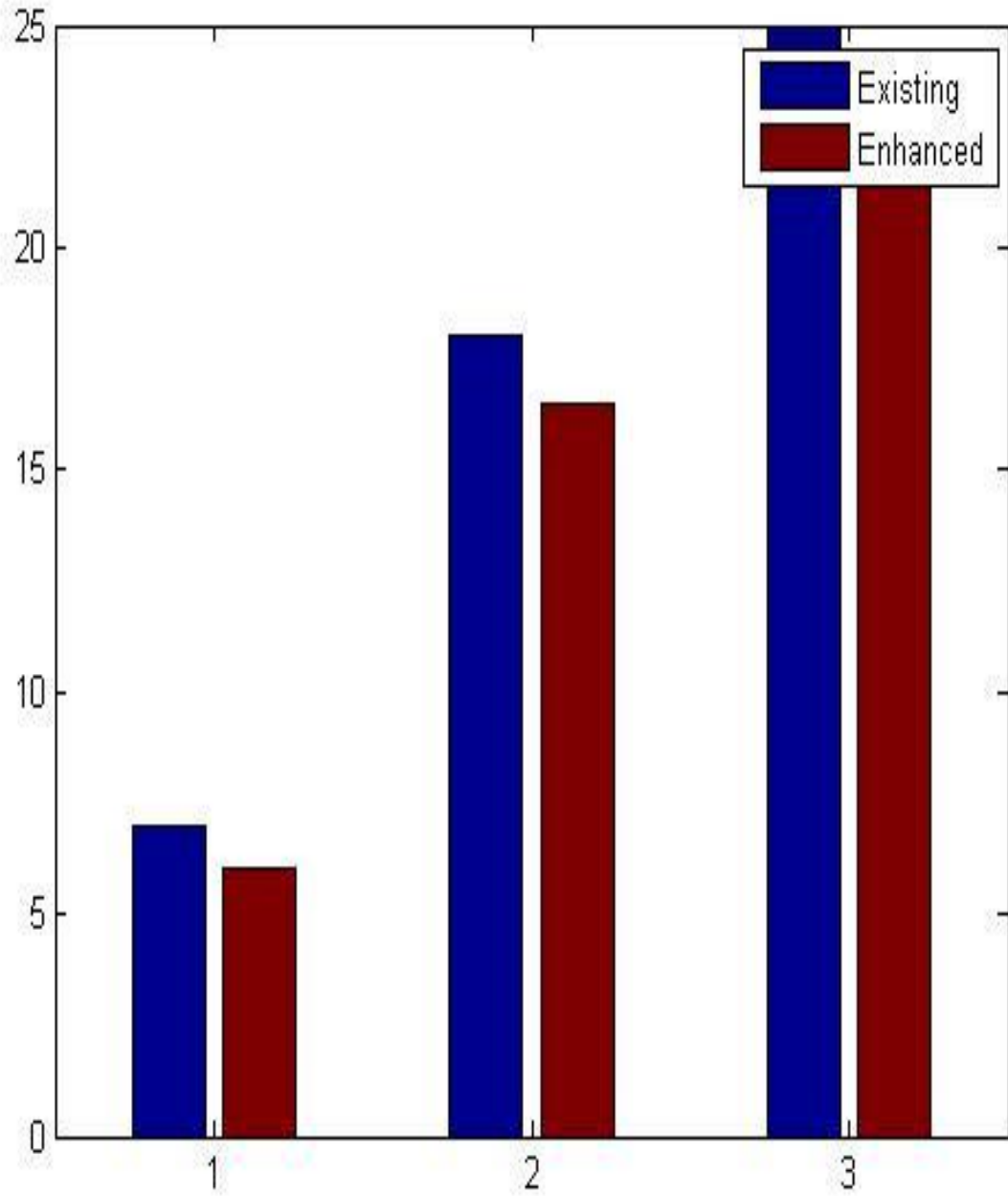


Figure 2.1 Performance analysis


```
Command Window
>> Compare_Security
Starting impersonation attackCompleted impersonation attackStarting Insider attackComleted in
ans =

    7.0000    6.0000
   18.0000   16.5000
   25.0000   23.0000

>> Compare_SecurityIm
Starting impersonation attackCompleted impersonation attackStarting Insider attackComleted in
ans =

    18.0000   16.5000

>> Compare_SecurityImp
Starting impersonation attackCompleted impersonation attack
ans =

    18.0000   16.5000
    19.0000   17.5000

fx >>
```

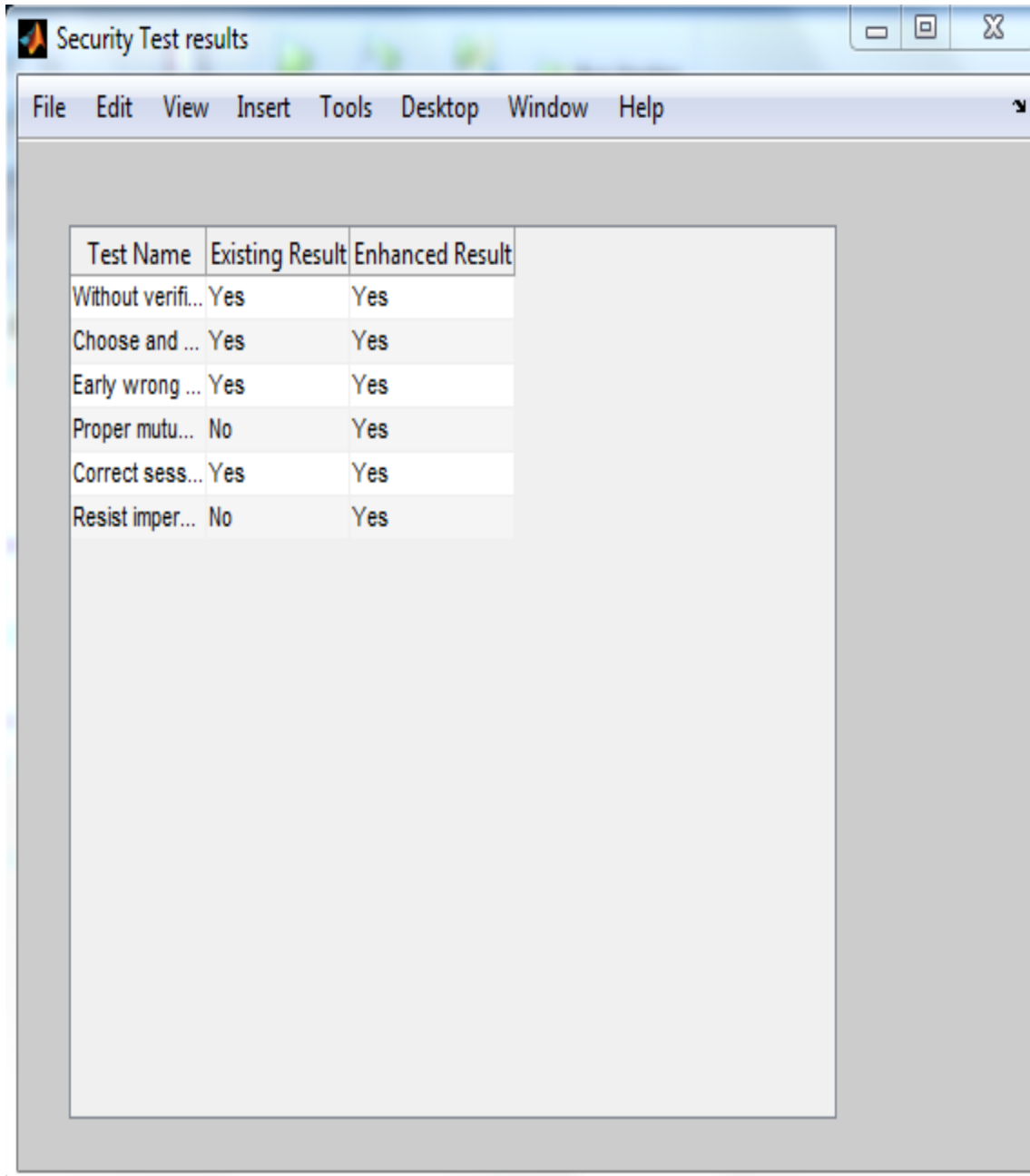
Figure 2.2 :Security comparison

Input parameter:

Request Servers = 6

Authentication Servers= 4

Clients = 25



The screenshot shows a window titled "Security Test results" with a menu bar containing "File", "Edit", "View", "Insert", "Tools", "Desktop", "Window", and "Help". The main content area contains a table with the following data:

Test Name	Existing Result	Enhanced Result
Without verifi...	Yes	Yes
Choose and ...	Yes	Yes
Early wrong ...	Yes	Yes
Proper mutu...	No	Yes
Correct sess...	Yes	Yes
Resist imper...	No	Yes

Figure 2.3 security test analysis

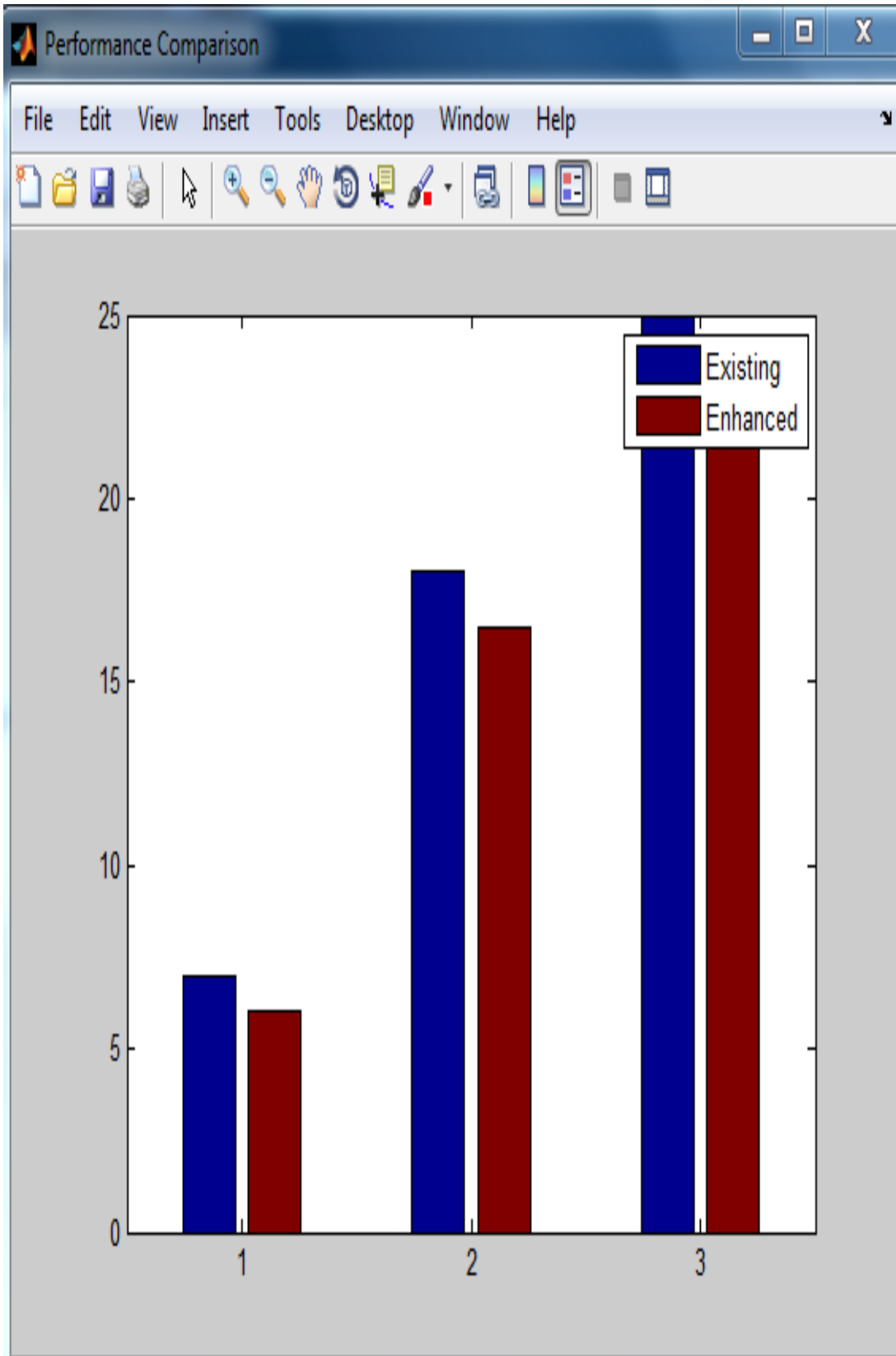


Figure 2.4 Performance analysis

```
Command Window ▼
>> Compare_Security
Starting impersonation attackCompleted impersonation attackStarting Insider attackComleted in
ans =

    7.0000    6.0000
   18.0000   16.5000
   25.0000   23.0000

>> Compare_SecurityIm
Starting impersonation attackCompleted impersonation attackStarting Insider attackComleted in
ans =

   18.0000   16.5000

>> Compare_SecurityImp
Starting impersonation attackCompleted impersonation attack
ans =

   18.0000   16.5000
   19.0000   17.5000

fx >>
```

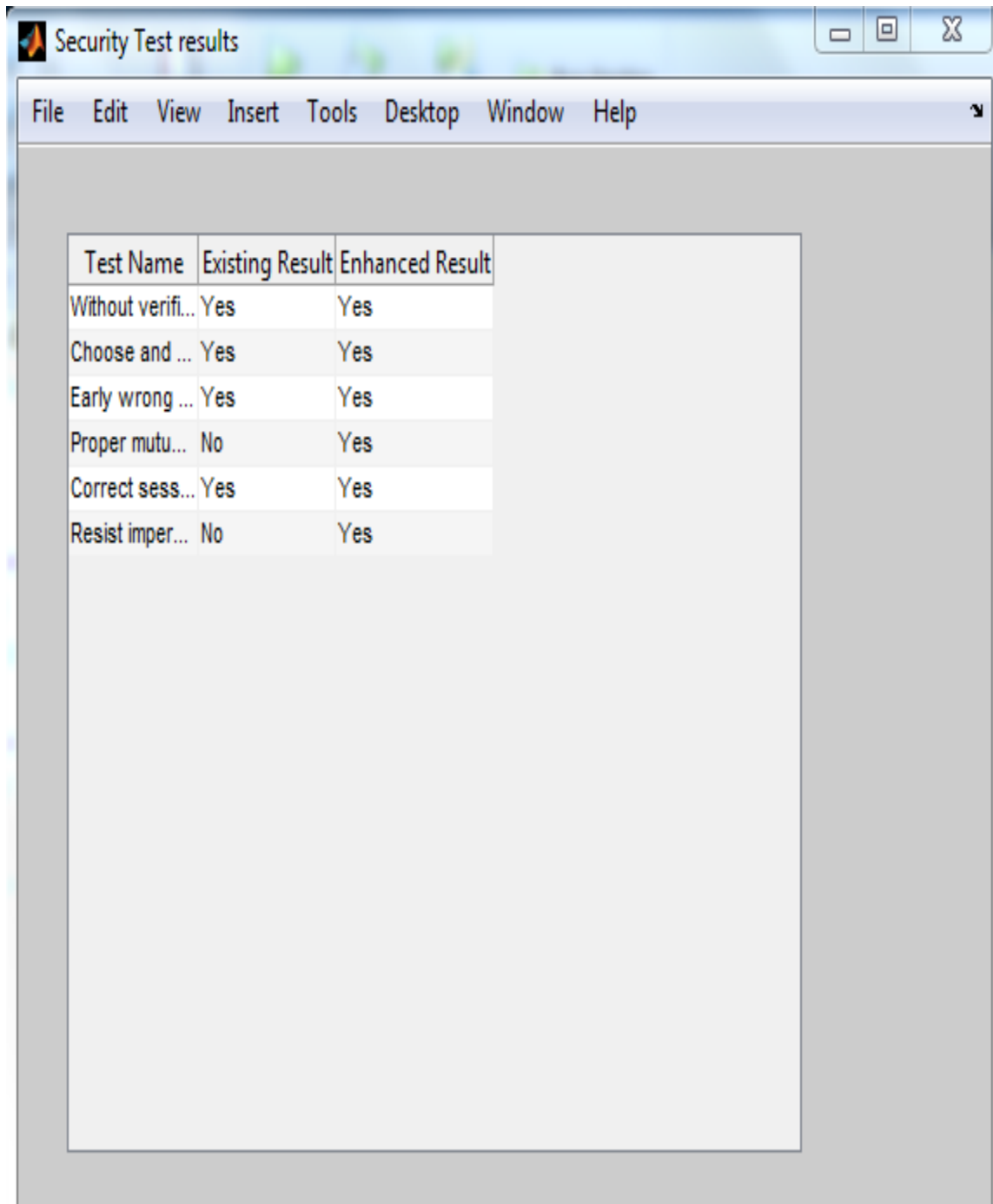
Figure 2.5:Security comparison

Input parameter:

Request Servers = 8

Authentication Servers= 5

Clients = 30



The image shows a window titled "Security Test results" with a menu bar containing "File", "Edit", "View", "Insert", "Tools", "Desktop", "Window", and "Help". The main content area contains a table with three columns: "Test Name", "Existing Result", and "Enhanced Result". The table lists seven tests, comparing their existing results with enhanced results.

Test Name	Existing Result	Enhanced Result
Without verifi...	Yes	Yes
Choose and ...	Yes	Yes
Early wrong ...	Yes	Yes
Proper mutu...	No	Yes
Correct sess...	Yes	Yes
Resist imper...	No	Yes

Figure 2.6 security test analysis

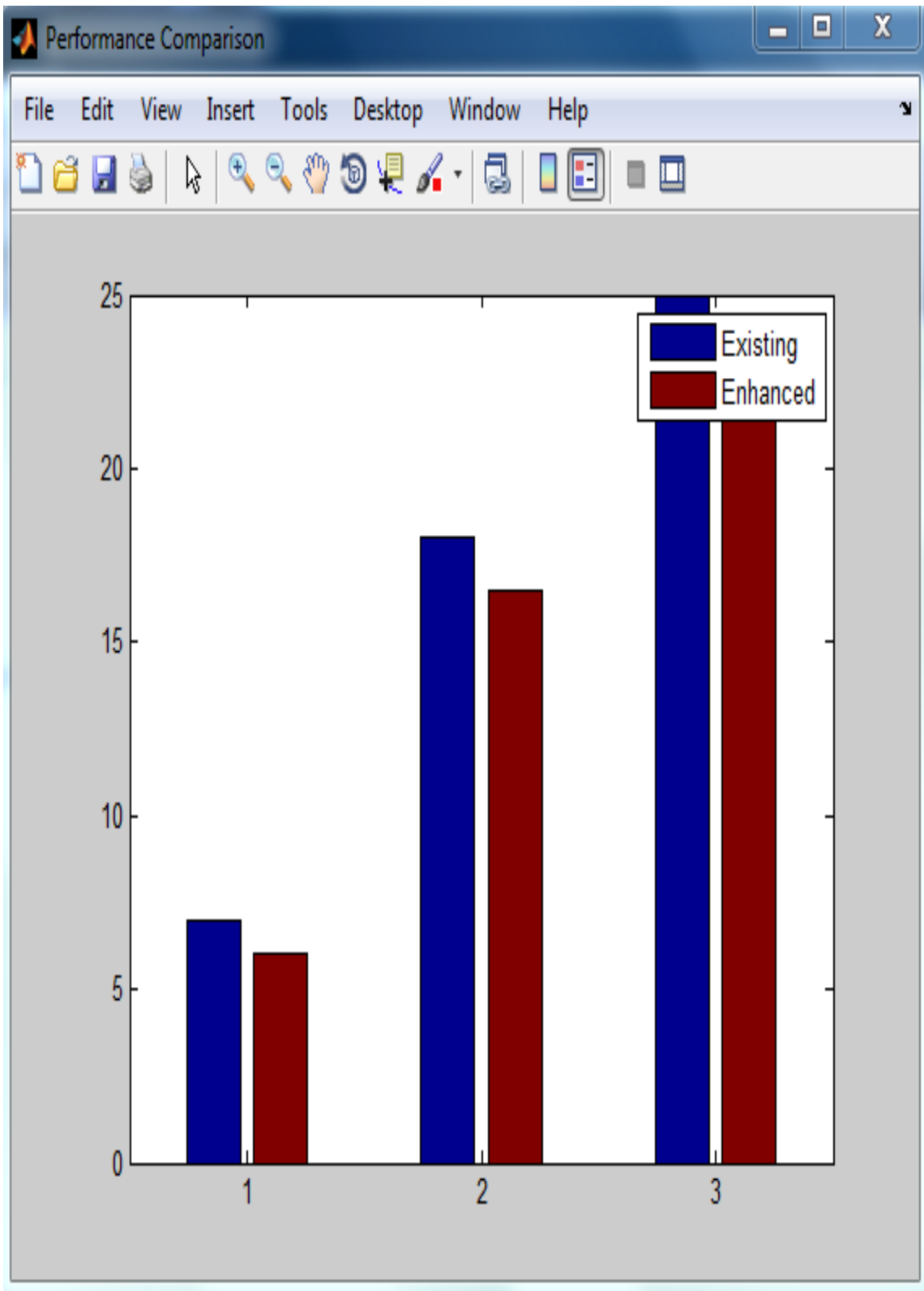


Figure 2.7 Performance analysis

```
Command Window
Starting impersonation attackCompleted impersonation attackStarting Insider attackCompleted ins
Starting impersonation attackCompleted impersonation attackStarting Insider attackCompleted ins
ans =

    7.0000    6.0000
   18.0000   16.5000
   25.0000   23.0000

>> Compare_Security
Starting impersonation attackCompleted impersonation attackStarting Insider attackCompleted ins
ans =

    7.0000    6.0000
   18.0000   16.5000
   25.0000   23.0000

>> Compare_SecurityImp
Starting impersonation attackCompleted impersonation attack
ans =

   18.0000   16.5000
   19.0000   17.5000

fx >>
```

Figure 2.2 :Security comparison

Chapter 5

SUMMARY/CONCLUSIONS

The proposed scheme will be more feasible for practical applications and will provide protection from some specific attacks. User authentication with dynamic id will secure the network for reliable communication. The weakness of existing scheme will overcome. The network efficiency and security performance will improve.

Chapter 6

LIST OF REFERENCES

1. Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, 24(11), 770–772.
2. Lee, J., Ryu, S., & Yoo, K. (2002). Fingerprint-based remote user authentication scheme using smart cards. *Electronic Letters*, 38(12), 554–555.
3. Hwang, M., & Li, L. (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(1), 28–30.
4. Li, X., Niu, J. W., Khan, M. K., & Liao, J. G. (2013). An enhanced smart card based remote user password authentication scheme. *Journal of Network and Computer Applications*, 36(5), 1365-1371.
5. H. M. Sun. An efficient remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(2000)4, 958–961.
6. Pippal, R.S., Jaidhar, C. D., & Tapaswi, S. (2013). Robust smart card authentication scheme for multi server architecture. *Wireless Personal Communications*, 72(1), 729-745.
7. D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks. “*Mobile Computing T. Imielinski and H. korth, Ed., pp. 153-81. Kluwer, 1996.*
8. S. Tao, K. Xu, A. Estepa, T. F. L. Gao, R. O. C. H. Guerin, J. Kurose, and Z. L. Zhang, Improving VoIP quality through path switching, presented at 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Philadelphia, PA, USA, 2005.
9. Y. Wu, C. Wu, B. Li, X. Qiu, and F. C. Lau, Cloud media: When cloud on demand meets video on demand, presented at Distributed Computing Systems (ICDCS), 2011 31st International Conference on, Minneapolis, MN, USA, 2011.
10. R. Chandra, R. Mahajan, T. Moscibroda, R. Raghavendra, and P. Bahl, “A case for adapting channel width in wireless networks,” *SIGCOMM Computer. Communication. Rev.*, vol. 38, pp. 135–146, August 2008.

Chapter 7

APPENDIX

A:

Authentication

Authorization

Availability

B:

BANLOGIC

C:

Confidentiality

D:

Decryption

Digital Signature

E:

Encryption

F:

Foreign key

Freequency

I:

Integrity

H:

Hash function

K:

Key

M:

Memory

Multimode

P:

Primary key

Password

Protocol

S:

Security

Smart card

Symmetric

T:

Transaction

