CHAPTER 1

INTRODUCTION

Authentication is used to verify that the user is the same person who he claims to be. Since the network systems are of distributed nature, privacy and security are most important concerns. In the past various authentication methods were invented to prevent unauthorized access. Among the methods developed in the past, password authentication provides the most cost efficient and simple to implement solution to provide protection against unauthorised access. Password authentication schemes are also used in client-server architecture to protect resources against unauthorised access.

Authorization differs from authentication in that it is the process of providing access to individuals based on verification of their identity. Authentication just verifies that the person is same as he claims to be.

Most popular authentication schemes employ username and password to provide security. Human factors play an important role in security, and should they be ignored the security system is most likely to suffer. A password may be thought of as a secret shared between customer and service provider. While storing password on server they are first encrypted to ensure that any access to file system does not disclose passwords.

1.1 Authentication

Entity Authentication is a technique with the help of which one proves the another party's identity. In entity we can take a person, process, client, or server. The two party involved in authentication is known as :

- Claimant: The entity needs to be proved it's identity.
- Verifier: The party tries to prove the claimant's identity is called the verifier.

Entity authentication is different from message authentication in many respect.

- Entity authentication happen in real time but message authentication might not happen in real time.
- Message authentication authenticate one message at a time. If an entity wants to send more than one message to another party for each new message the process must be repeated

But entity authentication authenticates the entity for entire duration of a session.

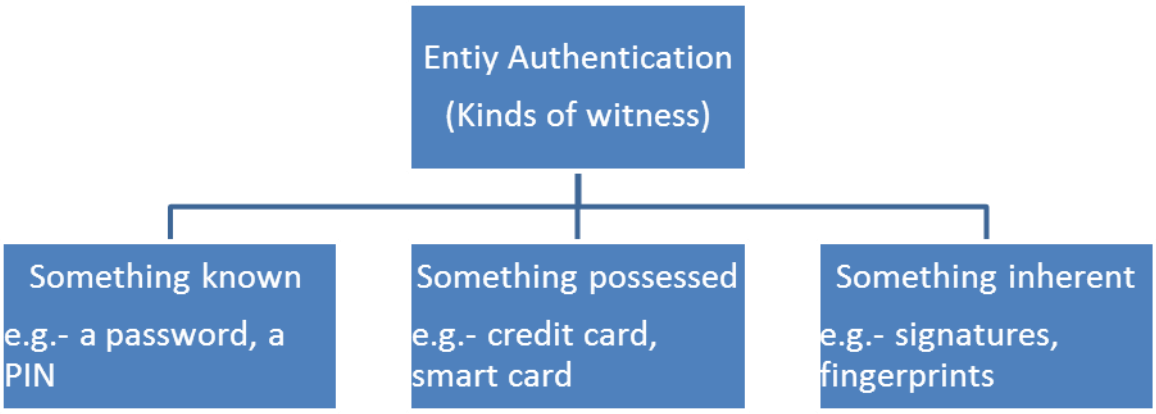

Figure 1.1 kinds of witness

Today, in order to address the problem, a variety of authenticated techniques based on passwords have been published in the literature.

1.1.1 Requirements for Authentication

For multiple server working password authentication technique is very effective and safe if only these following requirements are satisfied (Liao and Wang, 2009):

(R1) Single registration: User can access all the registered servers once a valid user registers.
(R2) No verification table: In this scheme there is no server has to maintain table of verification.
(R3) One can update his/her password, even if offline, securely and freely.
(R4)Mutual authentication and key management: in order to safe transmission phase messages, users and servers both after authenticating each other can agree on a session key.
(R5) Security: A realistic password authentication scheme needs to resist all types of attack.

1.1.2 Nature of Attacks

We generally catalogue some common threats as follows:
(S1) Eavesdropping attack: With the help of this eavesdropping, adversary can easily get the authentication information in the network.
(S2) Stolen verifier attack: If server is having any verification table, the adversary can steal the password table from it and doing so, the adversary can imitate the legitimate user.
(S3) Denial of service (DoS) attack: This attack is resist the service or resource of the server for users.

(S4) Impersonation attack: Message sends by adversary is changed by it to a legitimate party and claims that message comes from a valid sender.
(S5) Replay attack: The exchanged messages are recorded by an adversary and then transmit to legitimate party to obtain the valid information.
(S6) Server spoofing attack: An adversary imitating the legitimate server in an attempt to deceive a legitimate user using a valid message as a fake message.
(S7) Security of the session key: This means that even in disclosing a session key, an adversary could still not be able to get any message from the other sessions.
(S8) Smart card stolen: It is not possible to retrieve the password, even if the smart card is lost or stolen.

1.2 Encryption of Information

Encryption is used to transform data on a computer so that it is not possible to read the same. So, even if anyone manages to get unauthorised access to the system, he would not be able to put this data to any use, unless he has valid key for decryption.

Encryption translates normal text into cipher text. Encryption not only ensures that the information is not available to unauthorized person but it also ensures that information is not altered during transmission.

1.2.1 Types of Encryption

There are three different basic encryption methods.

a. Symmetric methods
b. Asymmetric methods
c. Hashing

a. Symmetric Method

In this method same/single key is used to encrypt and decrypt the information. That's why we call it as private key cryptography. Anyone use that key to decrypt the information. A Sender sends the information (the cipher text) to the receiver by using a key to encrypt the information. Now, the receiver uses the same key to convert the data received from sender into original data, i.e. to perform decryption. Ex. DES

b. Asymmetric methods

In this type of method there is two different keys for encryption and decryption. It is more secure than previous one. Here encryption is performed using a public key and a private key is used to perform the decryption.

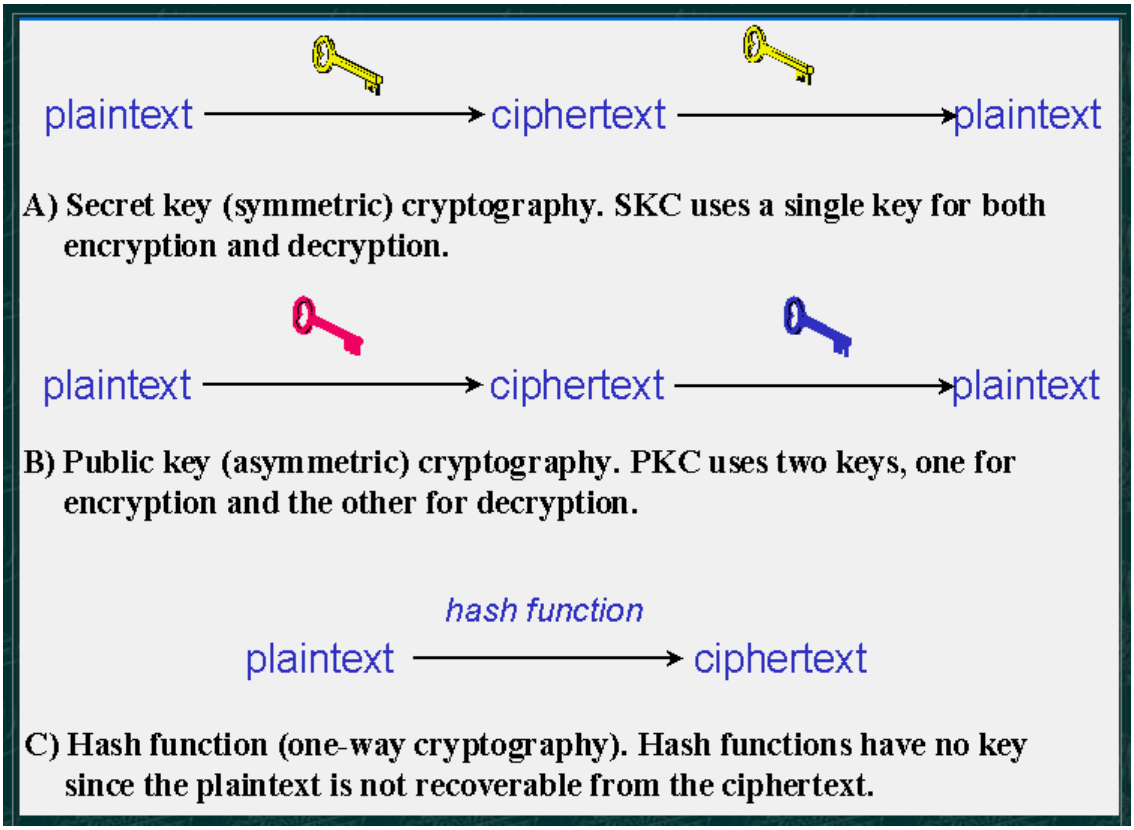

Figure1.2 Various cryptography techniques

c. Hashing

In this method a fixed-length signature that is unique as well is created for a message. Each such signature belongs to a specific message, so minor changes to that message can be easily tracked. Data encrypted using hash function cannot be reversed or deciphered. In hashing method, functions are evaluated based on their ability to provide protection against any adversary.

1.3 Smart Card

A smart card is a device having an embedded integrated circuit chip (ICC). ICC can be a microcontroller or internal memory. To provide connection between the card and reader either a physical contact or a radio frequency interface is used. These cards provide encryption and authentication.

Smart cards may store considerable data as well. They may perform functions like encryption and authentication besides interacting with smart card readers. Smart cards are available in variety of forms like plastic cards, fobs, subscriber identity modules (SIMs) etc.

1.4 Biometrics

Biometrics is device used for identifying individuals based on their physical or behavioural characteristics. Nowadays information security is essential and necessity, so it has crucial role in today's society. Biometrics features can be divided into two categories, physiological characteristics and behavioural characteristics. Physiological characteristics involve face, iris, fingerprints, palm prints, hand geometry and voice. The behavioural characteristics involve signature, handwriting analysis, voice, keystroke pattern and gait. Expected qualities of a good biometric are as follows:

Uniqueness: One individual is having a single particular feature which does not match with that of any other individuals.

Universality: A given biometric feature should be present in maximum possible number of individuals.

Permanence: Individual's traits should not change with age.

Measurability: It should be possible to measure individual traits with simple methods.

Collectability: User convenience is primary concern for performing biometric measurements.

A fingerprint template describes a stored file in a fingerprint scanning system. Whenever we store a fingerprint the image of the finger print is not stored but a template. A fingerprint template has smaller size than that of fingerprint image and using the template reduces processing time. A template provides a digital reference of distinct features extracted from a biometric sample. While the biometric authentication process these templates are employed.

Minutiae termed as a number of unique physical characteristics that a fingerprint contain, it includes some visible features of fingerprints such as ridges, ridge endings etc. Minutiae are usually found near the centre of the fingertips. This helps differentiate between two fingerprints, or to match fingerprints. Fingerprints of even the identical twins do not match.

Optical scanning and capacitance scanning are the common methods used these days for electronic fingerprint readers. Once a fingerprint is passed to the sensor window of the fingerprint reader device, the fingerprint is scanned and capture a gray-scale image. Now key minutiae points are identified from the image of the fingerprint using a special computer software. Template is a digital representation of these points.

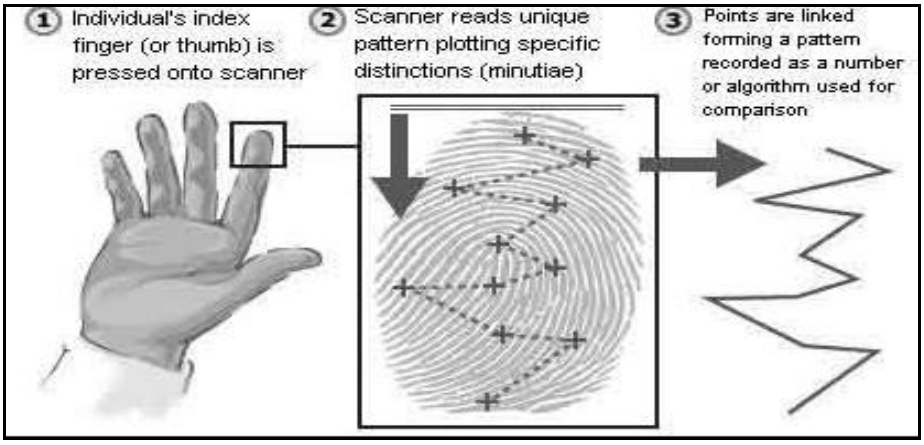

Figure.1.3 Fingerprint template generate from biometric

1.4.1 Biometric Description

Biometrics is the device that involves identification of a individual based on his intrinsic characteristics, such as voice, movement, retina, writing etc. To recognize a person it only results on "who the person is" and not on "what a person is carrying" or "what a person knows". There has been a considerable surge in the use of biometrics for user authentication because of the advantages that it offers over other authentication methods. Such biometrics-based authentication systems should withstand attacks when employed in security-critical applications.

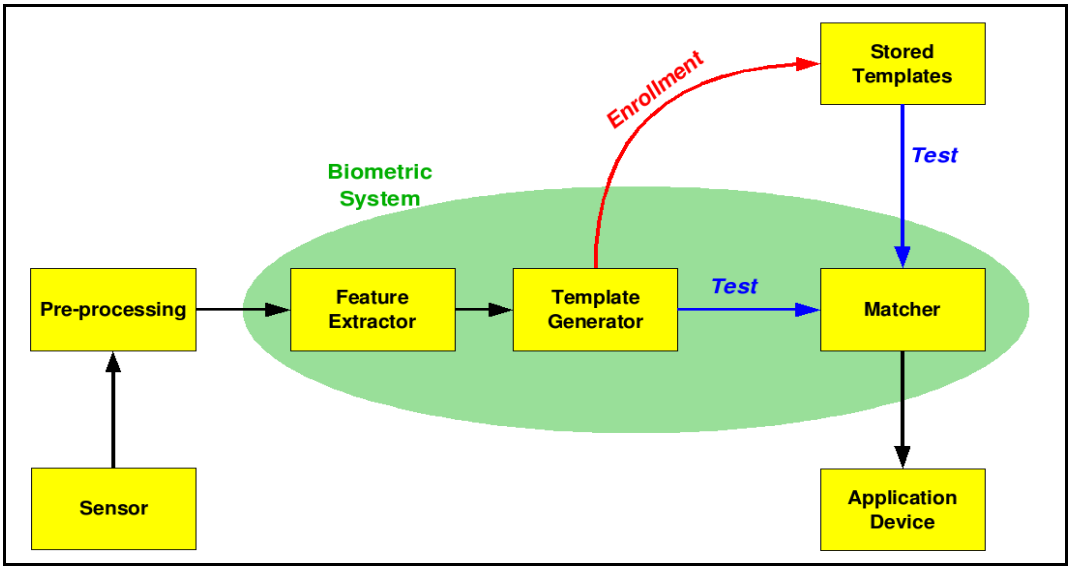

Figure1.4 Template generate from device

This biometrics is used on the database of the approved signatures in banks. The system compares the signatures with previously stored signatures in database to authenticate a person. Biometrics systems may as well use international database, instead of local database, for

determining the identity. The drawbacks of identification systems are their high cost and complex operations.

1.5 Motivation

Previously authentication had been determined on low-level technological design and implementation particulars. Humans are considered weakest link in any security chain. It has been observed that problem does not lie with the system security but with the humans who are either unable or not willing to comply with the security guidelines.

Counting human factors as part of structure design has a direct impact on the security of the system. When users ignore the guidelines on how to use security mechanisms then this may effect in overall security failures despite of the systems' technical reliability.

People are required to authenticate themselves (using techniques like passwords). Passwords hinder the security and usability. Even technical solutions password encryption has been able to determine the human related problems with passwords. The "password problem" refers to the problem where lots of passwords used in way are either weak and memorable or secure but hard to remember.

In this project we will study if it is feasible to enhance both security and usability at the same time. We focus mainly on biometric and smart card authentication. Alternative authentication mechanisms have their own problems that limit their use to specific applications. Password authentication techniques are much popular because of their cost efficiency and simple implementation. For these reasons, we focus on improving knowledge-based authentication schemes. We next turned to geometric based passwords as potentially successful schemes. Geometric based passwords have been proposed in recent years

1.6 Research Objective

A major goal of our study is to determine how to produce secure and usable authentication schemes. Those issue that are not well understood in current systems are also inquiries the interplay between usability and security .For increased security we resolute our research on geometric based password authentication for the reason of their prospective. The main research question is: Can biometric based passwords simultaneously support both authorization and security, while maintaining usability? The work began with a general survey, with new ideas being formed and tested as we progressed with the research. Here three main research objectives of this thesis are:

Objective 1: Record previously biometric password schemes, focusing equally on usability and security features, and identify the existing password scheme that appears most promising and that results the closer evaluation.

Objective 2: Empirically evaluate the most probable system identified through our cataloguing with respect to security and usability.

Objective 3: For success of the newly proposed system identify those key that essential for design and characteristics responsible, and simplify these to develop design strategies that can be applied to other types of geometric based authentication schemes.

1.7 Report Organizations

We start this dissertation with introduction in chapter 1. A detailed description of background is presented in chapter 2 which includes Authentication scheme. Chapter 3 explains about proposed problem statement and its proposed solution. Chapter 3 also gives a brief about the phases of system we have used. Chapter 3 also explains in detail about our proposed algorithm. The performance of the proposed algorithm and technique is evaluated with Biometric based geometric based password authentication. This is done using a smart card. In chapter 4 we conclude about the work done and observations in chapter 5.

CHAPTER 2

BACKGROUND AND RELATED WORK

2.1 Password Authentication

Password-based authentication is the simplest method of entity authentication where the password is something that the claimant knows. It is a protocol where a password is shared between two entities in advance and used as the basis of authentication. There are two types of password authentication schemes[15] :

a) weak-password authentication schemes
b) strong-password authentication schemes.

Weak-password schemes likely to have easy and lighter computational overhead the designs are simpler, and easy to execution, by comparing the strong-password schemes, making them particularly appropriate for constrained enviroments.

On the basis of lifetime of the password authentication schemes can be catagorized into two groups.

a) Fixed Password: A fixed password is a password that is used again and again for every access.
b) One-time Password: If user can use the password only once then it is a one-time password. This kind of password makes eavesdropping and salting avoidable.

Generally password authentication schemes consist of four phases:

1. **Registration Phase:** It is initial phase.User regiters with the system along his identity in registration phase. During this phase exchange of password as private key and id as public key takes place.System stores these information for further authenticate the user. User use these paremeters to login to the system.
2. **Login Phase:** When a registered user access the system, then this phase executes . In this phase user sends password or hash of password to system as claim to inform system that he/she knows some thing which was exchanged at the time of registration.
3. **Authentication Phase:** It is a phase where system checks the user to admitted the system for access. System verify the claim of user based on the key parameters exchanged at the time of registration and the authentication protocol which was agreed by both.

4. **Password Change Phase:** It is a phase for changing the previous password to a new one by the user. This phase executes when a user think that his/her password is guessed by an intruder or he/she is not able to remember the password.

Authentication process can be described as a method of comparing the identification provided to those on an authorized user's file in a stored database. When the credentials are matched, the process is ended. And then user is permitted to access the system. For authentication process user have to claim of their identification entity, he also have to provide some evidence to substantiate for claim. If successfully authenticated by the server, access rights are established to the user. Authorization is the process of an administrator permitting access and the method of glance user account authorizations for access to resources. The advantages and preferences allowed for the authorized account only depend on the user's permissions, which are either stored on local basis or on any authentication server. The settings for all these environment variables are set by an administrator.

2.2 Authentication Schemes

Authentication is the process of constantly verifying the identity of

- A user,
- A computer, or
- Both computer and user.

Forms of authentication (combinations are possible):

- Password-based
- Address-based
- Cryptographic

User authentication vs. machine authentication

For human to computer interactions, user authentication is performed. It is not suitable for guest accounts, or automatically logged-in accounts. Usually, to begin with a system, a user has to login or to choose an ID and provide their password. User verification is very essential for human-to-machine interactions in operating systems and in applications and also for wired and wireless networks to authorize access to networked and Internet-connected systems, also for applications and resources.

The importance of strong machine authentication

As we know that number of Internet-enabled devices is increasing, so it is critical to allow reliable machine authentication to safe communication in networked systems. In today's

internet scenario, almost any imaginable entity or object can be able to exchange information over a network and may be made addressable. It is very important to understand each access point a likely intrusion point. A very strong machine authentication required by the network machines. and also, in spite of their limited activity, these devices require to be designed for a limited permissions access as well, to limit their working even if they are breached.

Password-based authentication

In any network system (including the Internet), authentication is usually done by the user's login ID (user names) and passwords. This is assumed by the Knowledge of the login credentials that the user is authentic. User who registers initially (or is registered by someone else, like systems administrator), using an already assigned or self-made password. On each following use, the user must know and use the confirmed password.

Address Based Authentication

The MAC address of a network card is the source of address-based authentication. The client is refused to connect, if the MAC address of a network card is not found in the database of allowed MAC addresses. Security based on MAC addresses alone is very weak, as MAC addresses can be easily spoofed. We have to combine address-based authentication with port security to make sure that a stolen MAC address cannot be used from anywhere in the building and we have to need to use usernames and passwords to verify the employee who uses an authenticated client.

2.2.1 The problem with password-based authentication

It is quite easy to guess the login details as user names are commonly a combination of the individual's first name and last name. If limits are not compulsory, people may used to make weak passwords -- and strong passwords may be copied. Due to these reasons, online transactions require a more accurate and rigid authentication process.

By applying some password rules like minimum length and terms for complexity, like including capitals, alphanumeric and symbols, and smarter user names, password can be spot out to some extent. However, systems that require multiple independent methods are less vulnerable than the system using password-based authentication and knowledge-based authentication (KBA An authentication factor is category of identity verification by using credentials. The three most ordinary categories are usually categorized as: something you know (the knowledge factor), something you have (the possession factor) and something you are (the inherence factor).

- One used in conjunction with software token.
- Inherence factors -- a category of user authentication credentials having elements that are integral to the individual in the form of biometric data.

Sometimes User location and current time are to be considered as the fourth factor and fifth factor for authentication. For enabling reasonable security confirmation of the login location, most smart phones are equipped with GPS,. Lower surety measures include the MAC address of the login point or physical presence verifications through cards and other possession factor elements.

Though, several papers have been released concerned with smart-card-based password authentication schemes in past years. But, in these papers, the authors shows attacks on previous schemes and work out new protocols with assertions of the better aspects of their schemes, while they rule out the advantages that their scheme fail to provide, hence they try to overlook dimensions in which its performance is weak. Along with improper evaluation criteria, another common feature of these studies is that, there is no proper justification on security is presented, this explains why these types of protocols which were previously considered secure fail now a days. We can summarize the research history in the following manner-

New protocol→ broken → improved protocol → broken again → further improved protocol →

It has produced a lot of literature, but negligible attention has been paid to the systematic design area and analysis of these given schemes. Hence, in the following, an adversary model which is in accordance with the reality is explicitly mentioned and a proposed comprehensive criteria set is also laid down.

2.2.2 Smart Card Authentication

Smart Card authentication can be described as the ease of access to the resources on a remote machine just by logging into to ones local machine using a Smart Card and a PIN and then passing this data on to the remote machine Password authentication using smart card is a convenient and effective two factor authentication mechanisms for remote systems to assure one communicating party of the legitimacy of the other party by acquiring corroborative evidence. This technique is heavily used for various kinds of authentication applications, such as remote host login, online banking, e-commerce and e-health. In addition to this, it forms the basis of three-factor authentication. However, there are some issues in both security and

performance aspects due to the stringent security requirements and resource-strained characteristics of the clients.

2.3 Literature Review

Chang and Wu[3] has first introduced the remote user authentication scheme having smart cards in, so based on this many such schemes are proposed . The main issue of this scheme is security against offline guessing attack, which is major threat that a basic and practical scheme must be able to thwart. Previously, for the prevention of launching offline guessing attack, it is needed to make sure that the scheme is not going to leak any information useful about the client's password to the adversary in the protocol run, even if the password is very weak and low-entropy. Observing this kind of behaviour, many schemes used techniques similar to Bellovin and Merritt's Encrypted Key Exchange protocol. The basic feature of these types of schemes is the tamper resistant smart card is used, so that the secret parameters which are stored inside the smart card cannot be guessed. These have been demonstrated in research made in recent years that by some means the secret data stored in the smart card can be extracted, like by analyzing the power used or analyzing the leaked information. Therefore, schemes based on the tamper resistance assumption of the smart card are susceptible to offline password guessing attacks, user impersonation attack, etc, once an adversary has obtained the secret data stored in a user's smart card and/or just some intermediate computational results in the smart card. Consequently, a stronger method [11,15] of security against offline guessing attack is developed to require that compromising a client's smart card should do not help the adversary launch offline guessing attack against the client's password.

In a password authentication schemes, there is a password table, securely maintained by the server and this table is used to authenticate the remote user.

- In 1981, Lamport [1] proposed a remote password authentication scheme which is used in authenticating a remote user on an insecure channel. In this scheme a secure one-way encryption function is used and a microcomputer in the user's end can be used to implement it. The total system will be spoiled and interrupted, if the password table is changed by an adversary with a wrong intension, In this scheme, system stores only the value y = F(u) instead of user's password u. The user identifies by sending u to the system; the identity of the user is authenticated by the system by computing F (u) and then checking that value to the stored value y, which is already computed.

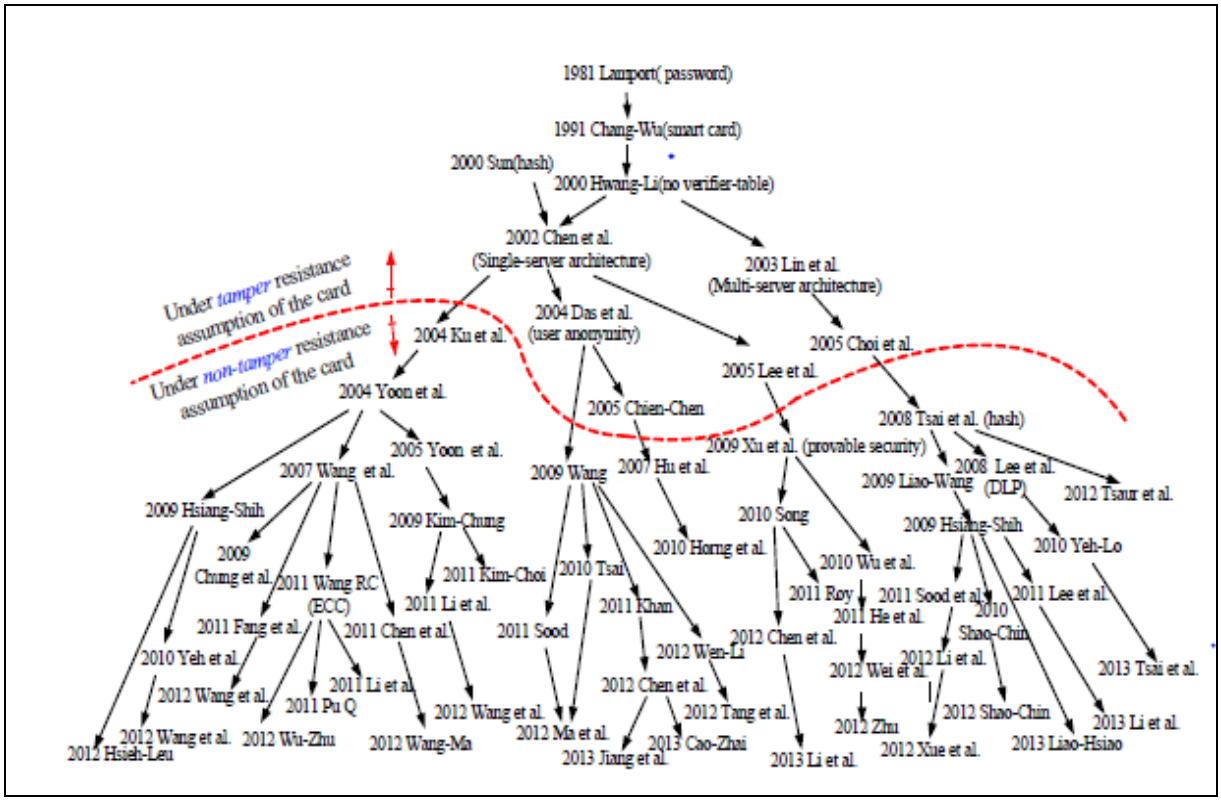

Fig2.1 Password authentcation schemes

- Reducing these types of risk, in 1990, Hwang et al. [2] proposed a password authentication which is non-interactive in which Shamir's ID-based signature is used. The system cannot store any secret of user. User can select his own password. However it can't remove the attack of replaying previous login and password.

- In 1991, Chang and Wu [3] proposed a password authentication method in which password table based on Chinese remainder theorem is considered. In this method some of the secret keys of the password generation centre can be derived by the information in the network. Then, that person can reveal the password from the intercepted authenticating message and imitate the legal user in a later login. In this method, any legal user can easily derive some of the secret passwords those are kept by the system, from the smart card. And therefore, he/she can pretend to be a different user and login to the system invalidly after intercepting another user's login request. The main weakness in their scheme is that they use CRT to conceal the random numbers. Thus, their scheme is breakable. But that scheme is vulnerable to a forgery attack as Chang and Laith [4] showed.

- In 1995 Wu [5] proposed an efficient "remote login authentication scheme based on a geometric property" of the Euclidean plane. But this scheme is not secure longer.
- In 1999, Hwang [6] proposed a Cryptanalysis to show that an illegitimate user can create a valid login request from the eaves dropped login request. An illegal user can impersonate as a other legal users and pass the system authentication.
- In 2000, Sandirigama and Toda [19] proposed a security enhance apart from low processing, transmission overhead and storage management compared to previous schemes. The proposed protocol was 'Simple and Secure' protocol. This method can use in several application like electronic payment, remote login etc. But that scheme was also suffer from stolen verifier attack.
- In 2001 Lin Sun and Hwang [15] give solution for strong security password authentication which use hash function twice, The registration phase executes only once while the authentication proceeds at every user login. But this scheme suffers from reply and denial of service attack. The same authors propose the Optimal Strong Password Authentication (OSPA) protocol to overcome the drawback of SAS protocol. OSPA protocol was secure against replay and denial of service attack and stolen verifier attack. M. Peyravian and N. Zunic [16] employ the collision resistance password scheme for protecting passwords while being transmitted and changed over insecure networks. Drawback of above scheme was overcome by Hwang [18], which use hash function to resist the guessing attack.
- In 2001, Chien et al. [7] proposed a modified remote login authentication scheme based on geometric approach incorporating one extra hash function and bitwise xor operation to the method instead of addition. However that scheme is also not secure further, as proposed by Chang and Lin [8] in 2005.
- In 2004 Ku propose [17] A Hash-Based Strong-Password Authentication Scheme without Using Smart Cards that can resist the offline guessing attacking. 2005, Ku et al. [9] proposed geometric based password authentication scheme which uses smart card having better resistant to the offline password guessing attack and is easily reparable.
- Unfortunately this scheme is more difficult as because user needs to enter two information (PIN and password) for enhance the higher security.

- In 2004 Lin and Lai [10] proposed a 'flexible biometric remote user authentication scheme'. But Khan and Zhang [11] have shown that, this method of authentication is suspected to have the server spoofing attack. There are several main features and advantages of proposed scheme which are discussed as follows. (1) It is implemented so that the

computation cost of each participant is optimized using small communication round. (2) By using bit-wise exclusive-OR (XOR) operation and one-way hash functions it achieves cryptographic goals. The one way hash function is collision free in nature as their main cryptographic operations without any additional requirements of server's public key and digital signatures. (3) It is secure against well-known cryptographically attacks such as replay attack, guessing attack, parallel session attack, reflection attack, insider attack and impersonation attack, and also provides mutual authentication and secure password change function without the help of remote server. As a result, the proposed method is very useful in smart card-based Internet and wired/wireless communication environment to access remote information of the system as it provides security, reliability and efficiency.

- In 2010 Li and Hwang [12] proposed a remote user authentication scheme which has the basis of biometric verification but above described method do not provide proper authentication and cannot avoid man-in-the middle attack, as shown by Li et al. [13] in 2011. In this paper we integrated passwords (what the user know), smart card (what the user has) and biometric (what the user are), and then construct a secure three factor authentication scheme that can be solved the above problems. Here we presents a geometric based authentication scheme using smart card having finger print, in this scheme the user needs to be enter only password and impression of finger print which provides better resistance in all aspect easily reparable than the improvement versions of Ku et al.[9] and it can avoid man-in the middle attack.

CHAPTER 3

PROPOSED SCHEME

In proposed scheme there having five different phases namely User Enrollment Phase, Login Phase , Remote User Authentication Phase, Remote server Authentication Phase and Password change Phase . There are three kinds of participants the login user, Remote server (RS) and a Central authority (CA), where CA is assumed to be trusted. Initially, CA chose a large prime number P, a one way function **f** and pair of $\mathbf{(x_0, y_0)}$ is generated by CA and securely stored in CA and Server. The one way function f defined as follows:

Given x, it is easy to compute y=f(x)

Given y, it is infissible to compute $x=f^{-1}(y)$.

3.1 Phases of proposed scheme

3.1.1 User Enrollment Phase

Proposed idea for generate the finger print template:-

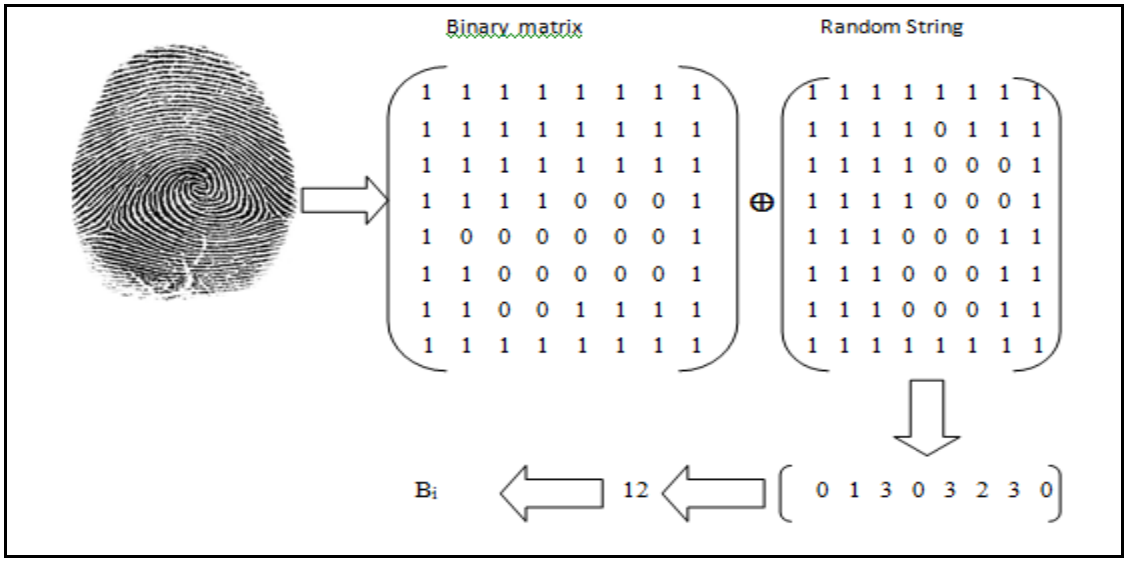

Fig 3.1. Generating finger print template

Suppose a new user U_i , register to the systems, U_i first choose his/her password PW_i and identification of Id_i and the user obtains her/his fingerprint image via a sensor and then extracts the minutiae from the finger print image to form a template of the fingerprint and present f(

$PW_i \| B_i$) to CA, where B_i is the unique extracted template from imprint finger print on the input device. Then CA performs the following jobs:

1. Computes the point r_{iw} and r_{io} as (0, f($PW_i \| B_i$)) and (f ($ID_i \| x_0$), f($ID_i \| y_0$)) respectively.
2. CA also computes $V_i = f (f (PW_i \| B_i))$.
3. Construct a line L_i passing through point r_{iw} and r_{io} .
4. Compute a random point A_i in the ratio of m:n where (m > n) in the line L_i so A_i can be expressed as

$$A_i = \frac{m.r_{i0} + n.r_{iw}}{m+n}$$

Store the parameters { Id_i , f, P, V_i , A_i , G,H } into the smart card for the user U_i,where $G= (m + n) \oplus f(PW_i \| B_i)$, $H=(m \times n) \oplus f(PW_i \| B_i)$ and secretly deliver this card to U_i.

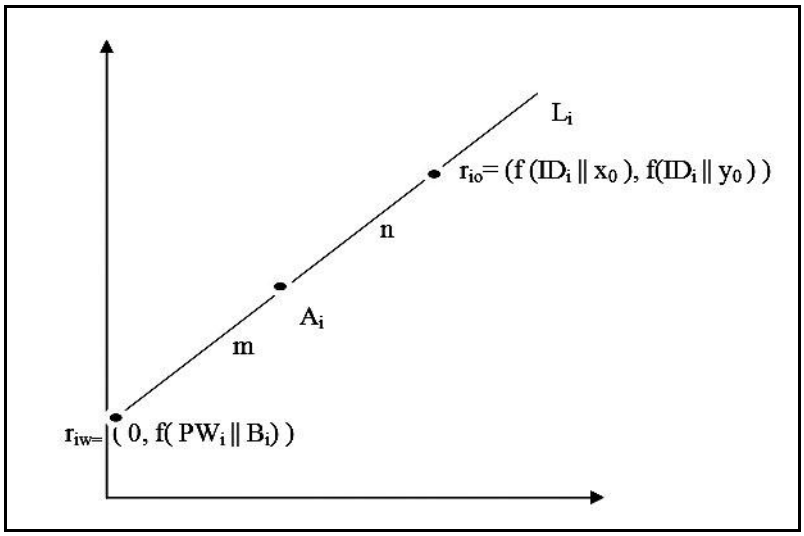

Fig3.2 graphical representation of enrollment phase

3.1.2 Login phase

When logging in, the registered user U_i first attaches his/her own smart card into the card reader and imprints the finger print. Then he/she needs only to enter their password PW_i and enter a onetime random number r_u into the system. If U_i passes the finger print verification then the smart card performs the following tasks:

1. Get the time stamp T from the system.
2. U_i smart card computes $r_{iw} =(0,f (PW_i \| B_i))$ and construct the line L_i passing r_{iw} and A_i

3. Again it will computes the another arbitrary point C_i, in the ratio of m:n in between the point r_{iw} and A_i.where m:n can be retrieves by computing $m+n= G \oplus f(PW_i \| B_i)$ and $m \times n= H \oplus f(PW_i \| B_i)$.

4. Now we can compute m and n by computing the following:

$$(m-n) = \sqrt{(m+n)^2 - 4(mxn)}$$

$$m1 = \frac{(m+n)+(m-n)}{2}$$

$$n1 = \frac{mxn}{m1}$$

if(m1 >n1)then

m=m1 and n=n1

else

m=n1 and n=m1 (as m>n)

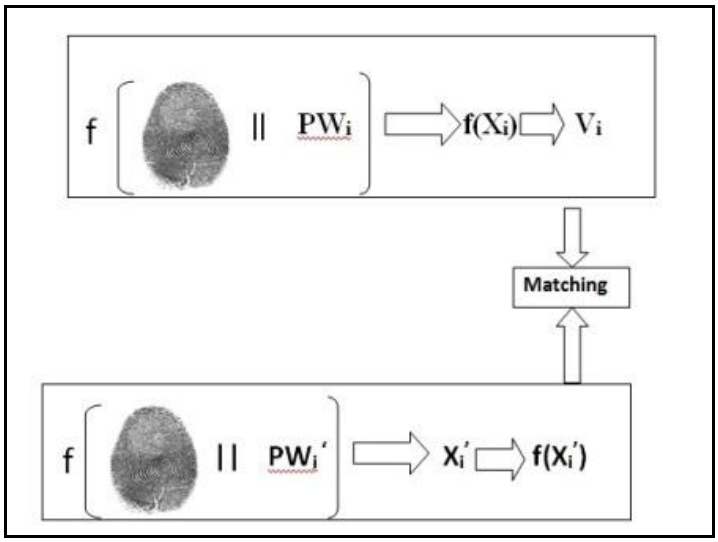

Fig 3.3.Login and password change phase

5. Find $r_{iT} = (0, f (f (PW_i \| B_i) \oplus f (T)))$
6. Construct a line L_{wT} passing through the point r_{iT} and C_i .
7. U_i smart card randomly select a point R_i which is differ from r_{iT} and C_i ,on the line $L_{wT.}$ U_i smart card also computes $E_i= r_u \oplus f(PW_i \| B_i)$ and $K_i =f(PW_i \| B_i)$.

8. Construct an authentication message $\{ID_i, A_i, R_i, T, E_i, K_i, G, H\}$ and transmit to the system for authentication.

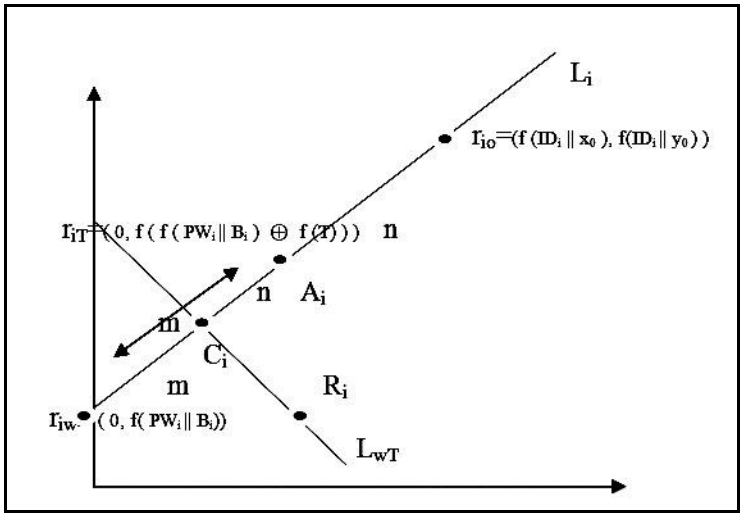

Figure.3.4 The graphical representation of login phase.

3.1.3 Remote User Authentication phase

After receiving the message $\{ID_i, A_i, R_i, T, E_i, K_i\}$ the system performs the following task to authenticate U_i login request:

1. Check the validation of identity ID_i . If it is invalid then login request will be rejected.
2. If $(T - T^{'}) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then the system will rejected the login request.
3. Calculate $r_{io} = (f (ID_i \| x_0), f(ID_i \| y_0))$.
4. Then reconstruct the line L_i passing through the point r_{io} and A_i .
5. Find the intersection point of the y-axis and line L_i denote P_i. Let $r_{iw} = (0, P_i)$ and then compute $r_{iT} = (0, f (P_i \oplus f(T))$.
6. Reconstruct the line L_{wT} passing through the point r_{iT} and R_i , and then computes the intercept point D_i of L_i and L_{wt} .
7. If the $D_i = \frac{m.A_i + n.r_{iw}}{m+n}$ is the identical, then

Correspondence holds and remote user is authenticated and proceed further for server authentication, where m and n is computed as step 4 in Login phase .

8. Now SR retrieves r_u by computing $E_i \oplus K_i$.
9. SR chose a one time useable random value r_s and send the message $\{ r_s \oplus K_i , f(r_s, r_u)\}$ to the remote user smart card.

3.1.4 Remote Server Authentication Phase

After received the message { $r_s \oplus K_i$, $f(r_s,r_u)$} from the server, the smart card performs the following task to check the authentication of server.

1. Smart card retrieves r_s by computing $r_s \oplus K_i \oplus f(PW_i \| B_i)$
2. Computes $f(r_s,r_u)$.
3. Compares the calculated and received value of $f(r_s,r_u)$, if not equal then the connection is terminated, otherwise the Remote Server RS is authenticated.
4. Access to the RS is granted.

3.1.5 Password change phase

Whenever user wants to change his/her current password PW_i to the new password PW_i^*, he/she needs to imprint his/her finger print and insert U_i smart card into the smart card reader and then enter the current password.

1. U_i smart card uses PW_i and finger print template B_i to compute $Q_i = f(PW_i \| B_i)$ and $f(Q_i)$.After U_i passes finger print verification with the stored value of V_i, he/she needs to input the old password PW_i and new password PW_i^*. U_i's smart card set the point $r_{iw} = (0, Q_i)$. Otherwise request will be rejected.

2. U_i's smart card computes $r_{i0} = \dfrac{(m+n)A_i - m.r_{iw}}{n}$

Where m and n is computed as step 4 in Login phase

3. $r_{iw}^{(new)} = (0, f(PW_i^* \| B_i))$

Next U_i's smart card computes

$$A_i^{(new)} = \frac{m.r_{i0} + n.r_{iw}^{(new)}}{m+n}$$

4. U_i's smart card replaces the stored A_i and V_i with $A_i^{(new)}$ and $V_i^{(new)}$, where

$V_i^{(new)} = f(f(PW_i^* \| B_i))$

3.2 Description of Proposed Scheme

ENROLLMENT PHASE

U_i CA

1. $f(PW_i || B_i), Id_i$ **2.** Computes r_{iw} , r_{io} , V_i , A_i

3.{ Id_i , f, P, V_i , A_i , G.H, f(Bi) }

LOGIN PHASE

U_i RS

1. Input the smart card and inputs B_i,PW_i
2. Get the timestamp T
3. Computes r_{iw} and draw the line L_i in between r_{iw} and A_i and take a point C_i in the ratio m:n
4. r_{iT}=(0,f (f (PW_i , B_i) $\oplus$ f (T))
5. construct line L_{WT} from r_{iT} and C_i
6. select a random point R_i other than r_{iT} and C_i
7. compute E_i= r_u $\oplus$ f (PW_i , B_i)

   K_i=f (PW_i , B_i)

8. {ID_i ,A_i , R_i ,T, E_i, K_i, G,H}

AUTHENTICATION PHASE

U_i	RS
	1. check the format of ID_i 2. computes $(T - T') \leq \Delta T$ 3. calculate r_{io} 4. reconstruct the line L_i from r_{io} and A_i 5. fine the intersection point P_i on Y axis then computes $r_{iT'} = (0, f (P_i \oplus f (T)))$ 6. reconstruct the line $L_{wT'}$ from the point $r_{iT'}$ and R_i 7. computes the point D_i and compare with $\frac{m.A_i + n.r_{iw}}{m+n}$ 8. if matched then $\mathbf{U_i}$ is authenticated and proceed further. 9. Retrieve r_u by $E_i \oplus K_i$
	10. $\{ r_s \oplus K_i , f(r_s,r_u)\}$ ←
11. retrieves $r_s = r_s \oplus K_i \oplus K_i$	
12. computes $f (r_s , r_u)$	
13. if computed value is identical with received $f (r_s , r_u)$ then **RS** is authenticated.	

3.2 Advantages of Proposed Work:

i. Ease to choose login id/password:

User can freely choose login id and password. It helps user to memorize the login id and password.

ii. Free from Brute Force attack:

The brute force attack is also known as exhaustive key search attack. In this type of attack, all possible combinations of password apply to break the password. Using brute force attack was a difficult task in the past but it is easier today using computer.

In the proposed scheme there is one hash function F() is used. It works on the output of some logical computation based on both password and figure print template. So it is very difficult and time consuming to apply brute force technique to crack F() , because it will not give the actual password or figure print template.

iii. The Deriving the Secret key of the System:

In this type of attack intruder tries to derive the secrete key of the system. If suppose n=p*q then intruder tries to find p and q to break the system.

In the proposed scheme the secret key (p) selection is not based on any calculation It is a very large prime number which is selected by system from a large collection of prime numbers. So it is very difficult to find n from a large collection of prime numbers whose number is increasing day by day.

iv. The Dictionary Attack:

This type of Attack is relatively faster than brute force attack. In this attack the attacker doesn't check for all possible value of password of given length but, he tries to match with some well known format of passwords.

The proposed scheme is not only depends on the password which can be guessed but also depends on the parameters stored in the smart card and the figure print template. So dictionary attack is very difficult to implement for this scheme.

v. The Shoulder Surfing Attack:

In this type of attack the attacker spies the user's movements to get his/her password. He observes the user to know, how he enters the password i.e. what keys of keyboard the user has pressed.

In the proposed scheme smart card and figure print template are used. So the possibility of Shoulder Surfing Attack is very low.

vi. The Phishing Attacks:

It is a web based attack in which the attackers redirect the user to the fake website to get password/Pin codes of the user.An attacker will again fail to implement phishing attack on the proposed scheme, because here server authentication also takes place.

vii. The Stolen-Verifier Attack:

In this attack intruder Steals the verification/password table and try to break the system.

In the proposed scheme no verification table is needed .So, it is impossible for an attacker to mount the stolen verifier attack on it.

viii. The side channel attacks:

Side channel attack is a branch of cryptography in which sensitive information is gained from the physical implementation of a targeted cryptosystem. The two main side channel attacks are

i.) Power attack

ii.) Time attack

In this section we illustrate the inexistence of these attacks on proposed scheme.

ix. The power attack:

It is a form of side channel attack in which the attacker studies the power consumption of a cryptographic hardware device (such as a smart card, tamper resistant "black box", or integrated circuit). The attack can extract cryptographic keys and other secret information from the device.Proposed scheme also uses smart card so there is a chance of power attack. The power attack generally based on statistical analysis of power consumed in the algorithm in different steps.

In proposed scheme random numbers are used which change in each iteration. So, it is very difficult to know about random number ru and rs with the help of power attack. Also there is not conditional branches in proposed scheme which are vulnerable to power attack.

x. The time attack:

It is a side channel attack in which the attacker attempts to compromise a system by analyzing the time taken to execute cryptographic algorithms. Every logical operation in a computer takes time to execute , and the time can differ based on the input; with precise measurements of the time for each operation, an attacker can work backwards to the input.

The proposed scheme is free from time attack because by knowing about the steps, it is very difficult to break this scheme .This scheme is not only based on password which is fixed for a user for every login but also depends on random number ru and rs which change in each login.

3.4 Example of Proposed Scheme

Let P=29 and $(x_0,y_0) = (3,5)$.

Registration phase:

In the registration phase, a new user U_i chose his/her password PW_i, say 1234 identification of Id_i , say pooja and unique extracted template from imprint finger print B_i, say 7 and present $f(PW_i \| B_i)$,say 6 to CA. Afterwards, CA performs the following tasks:

1. Point A_i in the ratio of m:n where (m > n),say (2,1) in the line L_i so A_i can be expressed as

$$A_i = \frac{mr_{i0} + nr_{iw}}{m+n} = (4,9)$$

$$X = \frac{2 \times 5 + 1 \times 10}{2+1} = (6+1) \bmod 29 = 10$$

$$Y = \frac{2 \times 9 + 1 \times 6}{2+1} = (6+0) \bmod 29 = 2$$

2. Store the parameters { Id_i , f, P, V_i , A_i , G,H } ={ 15,f,29,6,(4,9),12,13} in a smart card and deliver the smart card to U_i.

Login phase :

1. Get the time stamp T from the system, say T=10.
2. U_i smart card computes r_{iw} =(0, f (PW_i || B_i)) = (0,15) and construct the line L_i passing r_{iw} and A_i= (4,9) .
3. Again it will computes the another arbitrary point C_i, in the ratio of m:n in between the point r_{iw} and A_i.where m:n can be retrieves by computing m+n= G $\oplus$ f(PW_i || B_i)=3 and m x n= H $\oplus$ f(PW_i || B_i)=2.

Now we can compute m and n by computing the following:

$$(m-n) = \sqrt{(m+n)^2 - 4(mn)} = +1,-1$$

$$m1 = \frac{(m+n)+(m-n)}{2} = 2 \quad \text{or} \quad m1=1$$

$$n1 = \frac{mxn}{m} = 1 \quad \text{or} \quad n1=2$$

i.e m=2 and n=1

4. Find r_{iT} = (0, f (f (PW_i || B_i) $\oplus$ f (T))) = (0,3)
5. Construct a line L_{wT} passing through the point r_{iT} and C_i .
6. U_i smart card randomly select a point R_i, say (11,13)which is differ from r_{iT} and C_i , on the line L_{wT} .
7. U_i smart card also computes E_i= r_u $\oplus$ f(PW_i || B_i)= 7and K_i =f(PW_i || B_i)=15.
8. Construct an authentication message {ID_i ,A_i, R_i ,T, E_i, K_i, G, H}= {15,(4,9),(11,13),10,7,15,12,13} and transmit to the system for authentication.

Remote user Authentication phase

Suppose the system receives valid ID_i and (T-T') ,in the authentication message. The system performs the following task to validate U_i's login request and further operation for mutual authentication.

1. Calculate r_{io} = (f (ID_i . x_0), f(ID_i . y_0)) = (6,6)
2. Then reconstruct the line L_i passing through the point r_{io} =(6,6) and A_i = (4,9) .
3. Find the intersection point of the y-axis and line L_i denote P_i. Let r_{io} = (0, P_i)=(0,6) and then comput r_{iT} = (0, f (P_i $\oplus$ f(T))=(0,3).
4. Reconstruct the line L_{wT} passing through the point r_{iT} and R_i , and then computes the intercept point D_i of L_i and L_{wt} .
5. If the D_i = $\frac{mr_{iO}+nr_{iw}}{m+n}$ is the identical, then

correspondence holds and remote user is authenticated and proceed further for server authentication, where m and n is computed as step 4 in *Login phase* .

6. Now SR retrieves r_u by computing E_i $\oplus$ K_i.=3$\oplus$6=5
7. SR chose a one time useable random value r_s, say 4 and send the message { r_s $\oplus$ K_i , f(r_s,r_u)} = { 2,12}to the remote user smart card.

Remote Server Authentication Phase

After received the message { 2 , 12} from the server, the smart card performs the following task to check the authentication of server.

1. Compute $r_s = r_s \oplus K_i \oplus K_i = 2 \oplus 6 = 4$.
2. Calculate $f(r_s, r_u) = f(4|5) = 12$

i.e calculated $f(r_s, r_u)$ becomes equal to received $f(r_s, r_u)$, so remote server is authenticated successfully.

CHAPTER 4

PERFORMANCE EVALUATION AND RESULTS

In the proposed work we developed an secure and erfficient password authentication scheme. We have to perform the cryptanalysis ,to measure the security of our propsed scheme. If our system resist the attackers to mount different types of attack then it will automnatically refelect the security of our proposed scheme. The outcomes of cryptanalysis of given proposed schme is as follows:

4.1 Security Analysis

i. Resistance of stolen smart card and known password, PIN attack:

In ku et al. scheme [9], [23], suppose an user smart card is stolen and he knows the user password and PIN then adversary can easily authenticate as a legal user. But in our scheme, in case the adversary can achieve the legal user's smart card and password, he/she has not theft the fingerprint template in any phase. On checking the adversary's fingerprint minutiae with/by the minutiae template registered on the smart card, the illegal access will be discarded.

ii. Resistance man-in-the middle attack:

MITM is a common attack, relevant on many cryptographic approaches. This attack ignores the internal structure of system.

An attacker requires pairs of plaintexts and corresponding cipher texts for control to encryption and decryption. In Li and Hwang's [6] approach, server selects a random number R_s for any login credential message (ID_i , M_2), the attacker E eavesdrops the message (ID_i , M_2) and stars a session with server using the same message (ID_i , M_{E2})= (ID_i , M_2). By changing the corresponding authentication messages, attacker can execute the man-in-the middle attack. But in our scheme the shared line L_i constructed in the initial registration phase, so that even if the attacker E eavesdropped the login credentials {ID_i ,A_i , R_i ,T, E_i, K_i, G,H}, however the L_i is only known to the system (constructed from points r_{i0} and A_i) and the registered user U_i (constructed from points r_{iw} and A_i) .Thus, the correct line L_i can't be reconstruct by the attacker E without perceptive r_{i0} or r_{iw}. So man-in-the middle attack can't be performed by the attacker.

iii. Resistance to Insider attack:

An insider attack is a type of malicious attack . Insiders that perform attacks have a distinct advantage over external attackers because they As insider have authorized system access and also recognizable with network system architecture, so it have a distinct advantage over external intruder.

As we have seen in this proposed scheme the user U_i register with CA by submitting $f(PW_i || B_i)$ instead of PW_i or $f(PW_i)$ to CA. Any challenger may discover no useful knowledge for learning a user password from the public parameter by applying the secure one way function f. So this scheme is withstand the insider attack.

iv. Resistance off-line password guess attack:

In this proposed scheme, let that the adversary has intercepted the login massages { ID_i, A_i, R_{i1}, T_1 } and { ID_i, A_i, R_{i2}, T_2 } transmitted in step 8, at time T_1 and T_a respectively in login phase. Next he can guess the candidate password $PWi^{"}$ and then attempt to confirm his guess by using intercepted credentials. If the adversary can compute $r^{"}_{iT1} = (0, f (f (PW_i {}^{"}||B_i) \oplus f (T_1)))$, he can determine $L^{"}_{WT1}$ passing through the $r^{"}_{iT1}$ and R_{i1}. Similarly if the adversary can compute $r^{"}_{iT2,}$ can find out $L^{"}_{WT2}$ passing through the $r^{"}_{iT2}$ and $R_{i2.}$. Then the adversary can compute the intersection point $D^{"}_i$ of $L^{"}_{WT1}$ and $L^{"}_{WT2.}$ On the other hand, if the adversary can compute $r^{"}_{iw}$, he can easily obtain the middle point $D^{""}_i$ of $r^{"}_{iw}$ and A_i. Once the equation $D^{"}_i = D^{""}_i$ holds, the adversary has correctly guessed $PW_i^{"}$. However, since the adversary guessed password successfully he can not authenticate until he will not change the stored B_i with his own finger print template B_{i1} and respective parameter, from smart card. Therefore this scheme is resist off-line password guessing attack.

iv. Resistance of reply attack:

In replay attack information is stored without any authorization and then retransmitted through unauthorized operations such as fake credentials or authentication or a replica/duplicate transaction.

In our propsed scheme, suppose the adversary intercepted the login message {ID_i ,A_i , R_i, T, E_i, $K_{i,}$ G,H} then adversary can attempt to impersonate U_i to login through server by directly replying intercept message to server. Clearly server will rejected the login request because step 2. In Remote User authentication phase will be invalid. In other way if the adversary change the intercepted message with {ID_i ,A_i , R_i ,T_1 , E_i, $K_{i,}$ G,H},with the current

timestamp T_1, then also the login request will be rejected by the server, as because T_1 is inconsistent with R_i and as a result, the computed H_i can not be identical with A_i . So our presented scheme resists reply attack successfully.

v. Reparability:

If adversary has learned password PW_i then also he cannot impersonate U_i to login server as because he cannot generate B_i. But however if any how he passed the fingerprint verification then he can impersonate U_i to login server. In this case, if U_i finds or suspect that some one impersonate, then he can change his password by changing only his old PW_i with new password PW_i^* as mentioned in password change phase. Hence this scheme is easily reparable than Ku et al. proposed scheme, because in this scheme, it needs to change only the password not anything else.

vi. The Brute Force attack:

In this type of attack, all possible combinations of password apply to break the password. Using brute force attack was a difficult task in the past but it is easier today using computer. Brute-force attacks are straightforward to recognize. It is also called exhaustive key search attack. Encrypted file is stolen by attacker. They know that encrypted file contains message which they(attacker) wants, and the can unlock the message through encryption. Attacker tries by every single key to decrypt the message so he can success to create the original message.

In the proposed scheme there is one hash function F() is used. It works on the output of some logical computation based on both password and figure print template. So it is very difficult and time consuming to apply brute force technique to crack F() , because it will not give the actual password or figure print template.

vii. The Deriving the Secret key of the System:

In this type of attack intruder tries to derive the secrete key of the system. Let n=p*q then intruder tries to find p and q to break the system.

In the proposed scheme the secret key (p) selection is not based on any calculation It is a very large prime number which is selected by system from a large collection of prime numbers. So it is very difficult to find n from a large collection of prime numbers whose number is increasing day by day.

viii. The Dictionary Attack:

Dictionary Attack is relatively faster than brute force attack. The attacker doesn't check for all possible value of password of given length but, he tries to match with some well known format of passwords.

The proposed scheme is not only depends on the password which can be guessed but also depends on the parameters stored in the smart card and the figure print template. So dictionary attack is very difficult to implement for this scheme.

ix. Rainbow table attacks

By using the hash as the key it is possible to target a time space trade-off by pre-computing dictionary words from a hash list. But Attack execute faster as it require considerable less amount of preparation time. Due to the low cost of disk storage the storage requirements for the pre-computer tables were the major cost. It is less of an issue now a days .Pre-computed dictionary attacks are particularly effective when a large number of passwords are to be hacked. To find the corresponding password we can refer password hashes instantly any time.

The proposed scheme is not only depends on the password which can be guessed but also depends on the parameters stored in the smart card and the figure print template. So dictionary attack is very difficult to implement for this scheme.

x. The Shoulder Surfing Attack:

The attacker spies the user's movements to get his/her password. He observes the user to know, how he enters the password i.e. what keys of keyboard the user has pressed.

In the proposed scheme smart card and figure print template are used. So the possibility of Shoulder Surfing Attack is very low.

xi. The Stolen-Verifier Attack:

In this attack intruder Steals the verification password table and try to break the system and guess the password.

In the proposed scheme no verification table is needed .So, it is not possible for an attacker to apply the stolen verifier attack on it.

xii. The side channel attacks:

Side channel attack is a branch of cryptography in which sensitive information is gained from the physical performance of a targeted cryptosystem .The two main side channel attacks are

a) Power attack

b) Time attack

In this section we show the inexistence of these attacks on our proposed scheme.

xiii. The power attack:

It is a form of side channel attack in which the attacker concentrate the power consumption of a cryptographic hardware system, (such as a smart card, tamper resistant or integrated circuit). Cryptographic keys and other secret information can extract by the attacker from the device .Proposed scheme also uses smart card so there is a chance of power attack. The power attack generally based on statistical analysis of power consumed in the algorithm in different steps.

In proposed scheme random numbers are used which change in each iteration. So, it is very difficult to know about random number ru and rs with the help of power attack. Also there is not conditional branches in proposed scheme which are vulnerable to power attack.

xiv. The time attack:

It is a type of side channel attack .By analyzing the time taken to perform cryptographic algorithms, the attacker attempts to compromise a system. Every logical operation in a computer takes time to execute with precise dimensions of the time for each operation; an attacker can work in reverse to the input as time can differ based on input parameter.

The proposed scheme is free from time attack because by knowing about the steps. It is very difficult to break this scheme .This scheme is not only based on password Which is fixed for a user for every login but also depends on random number ru and rs which change in each login.

xv. Denial of service attack:

System may slow or totally damage/interrupt the services by the DOS. Many strategies use by the attacker to achieve this. It is designed to bring the whole network system damaged with useless traffic. For all known DoS attacks, there are software so that user can install to limit the damage caused by the attacks.

In our scheme smart card is used and at first the verification of login id takes place then after further computation completed. If a message arrived to server having wrong login id then that message will be discarded by server without performing the computation on that

message. The bandwidth usage of our scheme is very low so, it can survive with extra network traffic.

iv. The Phishing Attacks:

It is a web based attack in which the attackers redirect the user to the fake website to get password/Pin codes of the user. An attempt to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication List of phishing types :

Spear phishing

Phishing attempts directed at specific individuals or companies have been termed **spear phishing**. Attackers may gather personal information about their target to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.

Clone phishing

A type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address (es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original. This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

Whaling

Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term **whaling** has been coined for these kinds of attacks. In the case of whaling, the masquerading web page/email will take a more serious executive-level form. The content will be crafted to target an upper manager and the person's role in the company. The content of a whaling attack email is often written as a legal subpoena, customer complaint, or executive issue. Whaling scam emails are designed to masquerade as a critical business email, sent from a legitimate business authority. The content is meant to be tailored for upper management, and usually involves some kind of falsified

company-wide concern. Whaling phishermen have also forged official-looking FBI subpoena emails, and claimed that the manager needs to click a link and install special software to view the subpoena.

Rogue WiFi (MitM)

Attackers set up or compromise free Wifi access-points, and configure them to run man-in-the-middle (MitM) attacks, often with tools like sslstrip, to compromise all access point users.An attacker will again fail to implement phishing attack on the proposed scheme. Because here server authentication also takes place.

From the result of cryptanalysis we observed that our scheme is not at risk to different types of attacks. It means as compare to other existing schemes our scheme is more secure.

4.2 Performance Analysis Comparing to other schemes

After that we performed the Comparison of the overall performance of our scheme with the existing (Assume each string used in these protocols has length L)

	SAS [19]	OSPA [15]	Peyravian and Zunic's Scheme[16]	Lee-Li-Hwang's scheme [18]	Ku's scheme [17]	Our scheme
Ease to choose the password	no	no	no	No	no	yes
Type of Password	Numeric only	Numeric only	Numeric only	Alphanumeric only	Numeric only	Alphanumeric even special symbol can be used
Total messages transmitted in a single session	4	4	5	5	6	2
Total number of complex one way hash function used	8	11	3	3	12	1
Storage space for each user in server	3L	3L	2L	2L	3L	1L
Resistance to Dos attack	no	no	no	no	no	yes
Resistance to MITM attack	no	no	no	no	no	yes
Resistance to verifier-stolen attack	no	no	no	no	no	yes
Resistance to guessing attack	no	no	no	no	no	yes
Resistance to replay attack	no	no	no	no	no	yes
Password change phase	no	no	no	yes	no	yes
Fault Tolerant	no	no	no	yes	yes	Yes

Table 4.1 : Performance analysis with existing schemes

4.3 Overhead Performance Parameter

After performing the cryptanalysis on our scheme we tried to find the overhead of our scheme. For doing it we take three parameters these are as follows

1. No of operation performed
2. Network Usage
3. Size of data base used

No of operation performed

In our scheme we are using smart card. The computational capacity of smart card is limited. So, the measure operation is performed at server. Now a day calculation of hash function is very time and power consuming. In our scheme we are used only one hash function. Smart card performs the execution only one time of this only hash function. Rest of operation are simpler arithmetic operations.

Network Usage

In our scheme we performed the all operation on galious field GF_n , Where n is a prime number. So any intermediate value cannot be more than n. In the login phase smart card sends a message to server for authentication but the length of this message is very small and its depend on chosen n.

The maximum size of transmitted message= $8 * \log_2^n$

So, the transmitted message will take less bandwidth to travel from smart card to authentication server.

Size of data base used

In our scheme central authority only store the value of n and the ratio of interception. The size of these parameters is very small. So there is no need to maintain a large database. Some time if the size of data base became very large then it takes even more time to access the value of secure parameters. So, the performance of our scheme is better.

4.3 Screenshots

The screen shots of our scheme for given four phases are here:

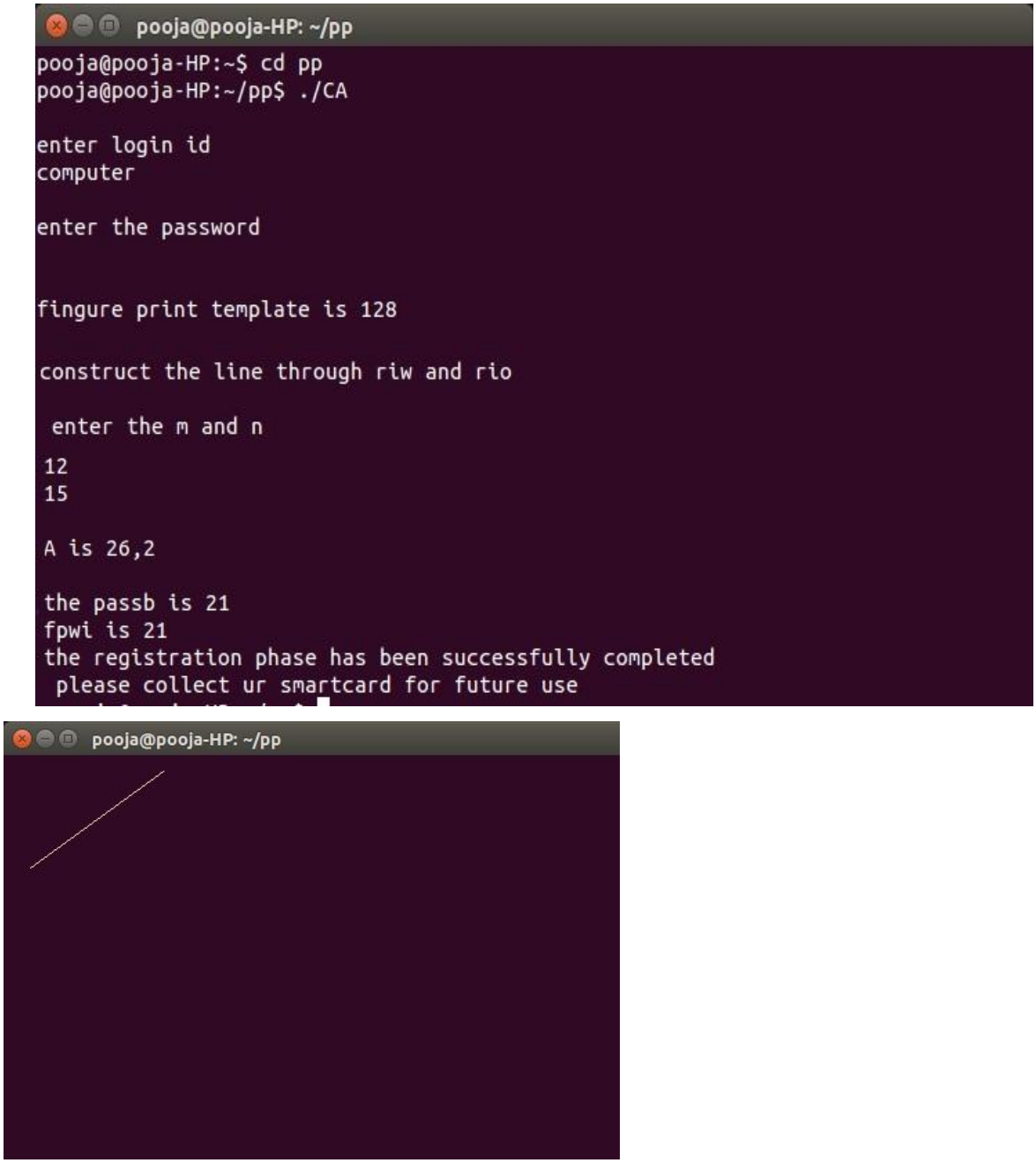

Figure 4.2: User Registration phase

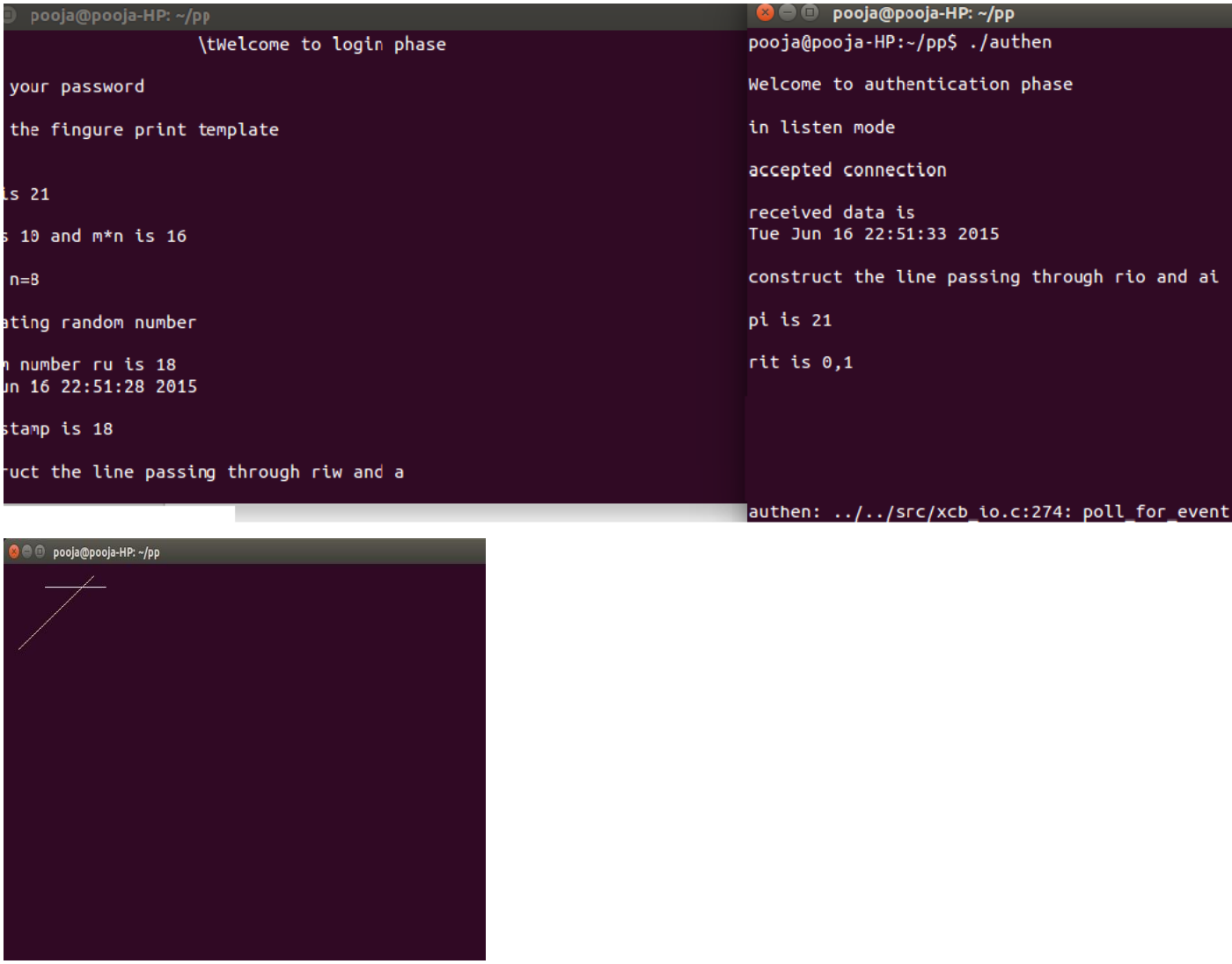

Figure 4.3: User Login and Authentication phase

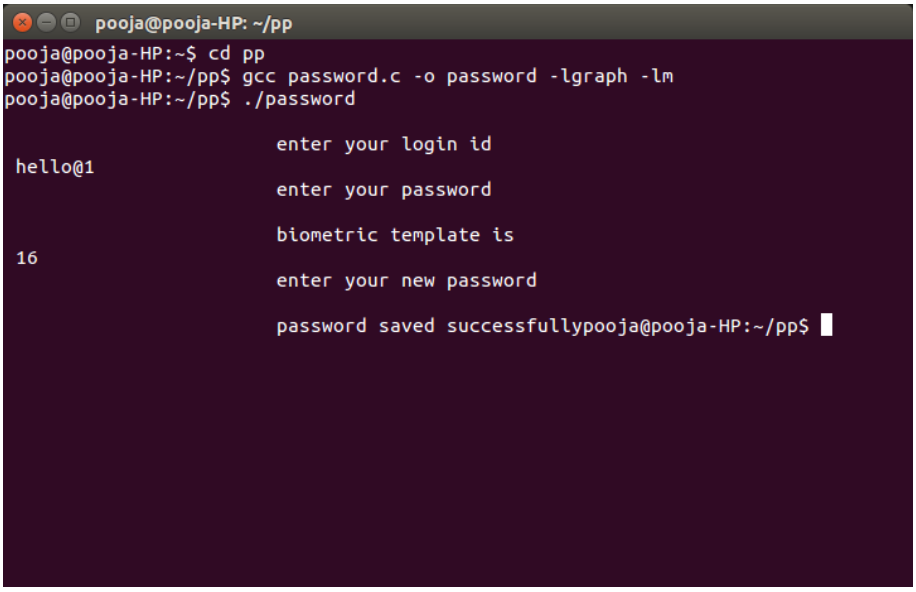

Figure:4.4: Password change phase

Chapter 5

CONCLUSION AND FUTURE WORK

In this report we have proposed a Biometrical authentication scheme based on geometric approach using smart card. Here we focused the problem of user of ku et al. and 2010 Li and Hwang scheme. ku et al scheme is vulnerable in stolen smart card and known password and PIN. Li and Hwang proposed a remote user authentication scheme based on biometric verification but above scheme does not provide proper authentication and cannot resist man-in-the middle attack.

In this report we integrated passwords (what the user know), smart card (what the user has) and biometric (what the user are), and then construct a secure three factor authentication scheme that can be solved the above problems. In this scheme the user is need not to remember two passwords (password & PIN) to enhance the higher security. This scheme also can resist offline password guessing attack, reply attack, insider attack, man in the middle attack. We have also shown how this scheme is easily reparable. We performed the cryptanalysis on proposed scheme and found that our scheme is non vulnerable to different types of attacks like password guessing attack, reply attack, Brute Force attack, Dictionary Attack, Phishing Attacks, side channel attacks and so on.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," Communication of the ACM , vol. 24(11) ,pp. 720-722, November 1981. doi: 10.1145/358790.358797.

[2] T. Hwang, Y. Chan, C.S. Laih, "Non-interactive password authentication without password tables," IEEE Region 10 Conferrence on Computer and Communication systems, IEEE Computer Society, 1990 (September), pp. 429-431.

[3] C. C. Chang and C. S. Laih, "Remote password authentication with smart cards," *IEE Proc. E Comput. Digit. Tech.*, vol. 139, no. 4, p. 372, 1992. doi: 10.1049/ip-e.1992.0053

[4] C. C. Chang, C. S. Laith, "Correspondence: Remote password authentication with smart cards," IEE Proc.- E,vol.139, no.4, pp. 372, 1992.

[5] T. C. Wu, "Remote login authentication scheme based on a geometric approach," Computer Communication, vol.18, no.12, pp. 959-963, December 1995. doi: 10.1016/0140-3664(96)81595-7

[6] M. S. Hwang, "Cryptanalysis of remote login authentication scheme," Computer communication, vol.22, no.8, pp. 742-744, 1999. doi: 10.1109/30.920451

[7] H. Y. Chien, J. K. Jan, Y. M. Tseng, " A modified remote login authentication scheme based on geometric approach," J. System Software, vol.55, no.3,pp.287-299,January 2001.

[8] C. C. Chang, I. C. Lin, "Cryptanalysis of the modified remote login authentication scheme based on geometric approach," Informatica, vol.16, no.1, pp. 37-44,2005.

[9] W. C. Ku, H. H. Chen, S. T. chang and C. H. Hwang, "An improved geomatric based password authentication scheme using smart card," Proceeding of the 2005 workshop on Consumer Electronics and signal processing, 2005.

[10] C. H. Lin and Yi-Yi Lai, " a flexible biometrices remote user authentication scheme," Computer Standard and Interfaces, vol.27, pp. 19-23, 2004. doi: 10.1016/j.csi.2004.03.003.

[11] M. K. Khan and J. Zhang, Improving the security of " a flexible biometrices remote user authentication scheme," Computer Standard and interfaces vol. 29,no.1,pp.82-85,2007.

[12] T. C. Lie and M. S. Hwang, " An efficient biometrices based remote user authentication scheme using smart card." Jurnel of Network and Computer Applications, vol.33, pp. 1-5, 2010.

[13] X. Lie, J. W. Nieu, J. Ma, " Cryptanalysis and improvement of a biometrices based remote user authentication scheme using smart card," vol.34, pp. 73-79, 2011.

[14] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," *IEEE Trans. Consum. Electron.*, vol. 49, no. 4, pp. 1246–1248, 2003.doi: 10.1109/TCE.2003.1261225.

[15] C. L. Lin, H. M. Sun, and T. Hwang, "Attacks and solutions on strong-password authentication," *IEICE Trans. Commun.*, vol. E84-B, no. 9, pp. 2622–2627, 2001.

[16] M. Peyravian and N. Zunic, "Methods for protecting password transmission," *Computers and Security*, vol. 19, no. 5, pp. 466-469, 2000. doi: 10.1016/S0167-4048(00)05032-X

[17] W.-C. Ku, "A hash-based strong-password authentication scheme without using smart cards," *ACM SIGOPS Oper. Syst. Rev.*, vol. 38, no. 1, pp. 29–34, 2004. doi: 10.1145/974104.974107

[18] C. Lee and L. L. M. Hwangt, "A Remote User Authentication Scheme Using Hash Functions," pp. 23–29, 2002.

[19] M. Sandirigama, A. Shimizu and M. T. Noda, "Simple and secure password authentication protocol (SAS)," IEICE Transactions on communication, vol.E83-B(6), pp. 1363-1363, 2000. doi: 10.1145/974104.974107

[20] J. Lu, S. Zhang, and S. Qie, "Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards."

[21] I. Jeon, H. Kim, and M. Kim, "Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards," 2011.

[22] Ku, H. C. Tsai, and S. M. Chen, "Two simple attacks on Lin-Shen-Hwang's strong-password authentication protocol," *ACM Operating Systems Review*, vol. 37, no. 4, pp.26-3 l, Oct. 2003.

[23] M. K. Khan and J. Zhang, "Improving the security of ‘a flexible biometrics remote user authentication scheme'," Computer Standards and Interfaces, Vol. 29, No. 1, pp. 82-85, 2007.

[24] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, Vol. 33, No. 1, pp. 1-5, 2010.