Fortification of Transport Layer Security Protocol by using Password and Fingerprint as Identity Authentication Parameters

Kuljeet Kaur
Lovely Professional University
School of Computer Applications
Systems and Architecture Domain

G.Geetha
Lovely Professional University
School of Computer Applications
Networks Domain

ABSTRACT
Whenever there is communication between Client and Server over a public link and resources are to be accessed from remote systems, then proving an identity becomes quiet complex because there is need of proper access rights with authentication. Complete security at the transport layer starts with proof of authentication, majority organizations only use password for security but this research paper would include one more tier of security to the transport layer security protocol by using fingerprints for identity authentication. Bio Hashing with the help of Minutiae Points at the fingerprints would be used for mutual authentication. Complete comparative analysis of all the existing password authentication schemes on the basis of security requirements and attacks is done in this paper. Result is generated that which existing scheme could withstand security requirement of mutual authentication for using fingerprint as identity parameter along with password. Proof is generated that with mutual authentication intruders could not practice Phishing, IP or Server Spoofing, Smurf attack and DNS Poisoning etc. Research paper focuses on implementing Password and Fingerprints for mutual authentication in Multi Server environment which will generate an Ideal Password Authentication Scheme and will result in fortification of Transport Layer Security Protocol.

General Terms
Ideal Password Authentication Scheme, Multi Server Environment

Keywords
Password Authentication, Minutiae Points, Mutual Authentication

1. INTRODUCTION
The most convenient mechanism to prove authenticity over public link to access from remote systems is the use of Password. So over a public network, communication could be started by sharing a (short) password within a session created between Client and Server with Session key. For this, Secure Shell protocol is deployed [1].

Public Network is an insecure network so Password authentication is one of the simplest and the most convenient authentication mechanisms to deal with secret data over such an insecure networks. Password Authentication is required in areas such as computer networks, wireless networks, remote login systems, operation systems, and database management systems etc [2]. e.g Whenever user wants to access Online Banking facility, each of them should have an identifier (ID) and password (PW). The user enters the Username and Password on the login screen, and then server verifies the same username and password in the Password (verification) table. If the submitted ID and PW match the corresponding pair stored in the server's password table, the user will be granted to access the server. The Bank Industry is using public key infrastructure in which the entity (server) knows the secret key corresponding to the public key embedded in a certificate of security. But there is a possibility that an intruder can impersonate a legal user by stealing the user's ID and PW from the password table whenever user accesses data from remote server. Moreover intruder can make use of various attacks (Dictionary Attack, Denial of Service, Forgery Attack, Man in the Middle Attack etc) during transportation or communication of the data and could possibly impersonate the legal user. All these attacks and impersonation is possible only on the transport layer because when the data is being transferred security protocols (Secure Shell Protocol and Public Key Infrastructure) function but intruders can attempt to break any of the existing security protocols and could hack the password. When Secure Shell Protocol is used, the client is asked to log into another computer at some remote location but with some password authentication, then only the files could move from one location to another. In this case association between client name and password is maintained by remote machine. When Public Key Infrastructure is used, the password authenticated key exchange provides the two computing devices with session key to implement an authenticated communication channel within which messages sent over the wire are cryptographically protected. But in both the protocols security of the password becomes the prime concern for every data communication over the public network.

In this research paper one more tier to the security protocol would be added by combining finger prints to the passwords for fortifying the transport layer. The password and finger prints together would be used for proving mutual authentication (the Client would authenticate Server and the Server would authenticate Client) and it would be the Ideal Password Authentication Scheme (Password along with Fingerprint) which would result in the fortification of the transport layer security protocol. Mutual authentication is required so that intruders could not practice IP or Server Spoofing, Smurf attack and DNS Poisoning etc. Phishing would be extremely difficult if mutual authentication is implemented well. So this research paper would use password and fingerprints for identity authentication (Ideal Password Authentication Scheme) of Client and Server both (Mutual Authentication) which would result in the fortification of the Transport Layer Security Protocol. And this Ideal Password

Authentication Scheme could be implemented in any organization with multi-server environment.

The structure of the remainder of the paper is as follows. In Section II review of literature is done with complete analysis of all existing password authentication schemes on the basis of security requirements and attacks. In Section III description of minutiae points of fingerprints used for proving mutual authentication. In Section IV proposed methodology for implementing this ideal password authentication scheme is discussed. In Section V fortification of Transport Layer Security Protocol is shown and Section VI concludes the paper.

2. REVIEW OF LITERATURE

Users generate strong passwords and at the back end password authentication schemes work for security and strength of the password. But these schemes are vulnerable to various attacks which results in insecurity.

Let us first discuss kind of attacks, for which scheme should not be vulnerable, and security requirements, which scheme should satisfy. In this research paper certain security requirements and attacks are finalized which are mandatory for all the password authentication schemes to withstand. Attacks such as:

Denial of service attacks (The goal of this attack is to deny legitimate users access to particular resources. False verification information of the legal user can be updated by the attacker for the next login phase. Later on the legal user would not be able to login successfully. A malicious user intentionally disrupts service to a computer or network resource)[3],

Forgery attacks (It is a kind of impersonation attack in which an attacker attempts to modify intercepted communications to masquerade the legal user and login the system to access the resources at the remote system.Remote user authentication is very important for security of systems which allows remote access over public (untrusted) network, on which forgery attacks become quite common), server spoofing attack)[4],

Parallel session attacks (When user and server communicate with each other, an attacker could create a valid login message out of some eavesdropped communication of the user and the server.For this attacker need not to know the user's password, one could easily masquerade legitimate user by creating a valid login. It occurs when two or more protocol runs are executed concurrently and messages, from one run (the reference session) are used to form spoofed messages in another run (the attack session)),

Password guessing attacks (In this attacker intercepts the authentication messages and stores them locally and then attempts are continuously made to guess password. Majority passwords have very low entropy and are very vulnerable to password guessing attacks. Attacker verifies the correctness of guess by using these authentication messages)[5],

Replay attacks (An attacker saves the previous communications of the legitimate user. Attacker intercepts the previous communications and can easily impersonate the legitimate user in order to login into the system. The attacker can replay all these intercepted messages and it would result in impersonation of legitimate user.

S.No	Security Requirements and Attacks	R	E	H
1	Denial of Service Attack	Y	Y	Y
2	DNS Poisoning	Y	Y	Y
3	Forgery Attack	Y	Y	Y
4	Man in the Middle Attack	Y	Y	Y
5	Forward Secrecy	Y	Y	Y
6	Ping of Death	Y	Y	Y
7	Mutual Authentication	N	N	Y
8	IP Spoofing	Y	Y	Y
9	Parallel Session Attack	Y	Y	Y
10	Ping Broadcast	Y	Y	Y
11	Password Guessing Attack	Y	Y	Y
12	Server Spoofing	Y	Y	Y
13	Replay Attack	Y	Y	Y
14	Session Hijacking	Y	Y	Y
15	Smart Card Loss Attack	Y	Y	N
16	Smurf Attack	Y	Y	Y
17	Stolen Verifier Attack	Y	Y	Y
18	Teardrop Attack	Y	Y	Y

R: RSA Based E: ElGamal Based H:Hash Based

Y: Supported N: Not Supported

Fig: 1.1 Analysis of all the existing password authentication schemes on the basis of attacks and security requirements.

This attack involves capturing traffic and uses that to gain access to the systems. e.g Login information of the valid user is sniffed by the hacker. Now even if the information is encrypted, the hacker replays the login information and gains the access),

Smart card loss attacks (If the smart card of the legitimate user is lost or stolen the attacker can easily change the password of the smart card by using password guessing attacks, dictionary attacks and could impersonate the legitimate user in order to login into the system), and

Stolen-verifier attacks (The passwords are stored in the hashed code at the server. In this attack the attacker steals the passwords (hashed code) from the server and can easily impersonate the legitimate user to login into the system. Hashed code stolen is used by attacker as stolen verifier for impersonating legitimate user) and security requirements such as

DNS poisoning, forward secrecy (This is the security requirement that ensures that the previously generated passwords in the system are secure even if the system's secret key has been revealed in the public by accident or is stolen[6]. Key once used for transmission of data should not be used to derive any new key. But if the key is derived from some other material then that material should not be used to derive any more keys)[7],

Mutual authentication (In this the user and the server can authenticate each other. This means not only the server verifies the legitimate user but the user also verifies the legitimate server[8][9].

This security requirement helps to withstand server spoofing) etc. Current data security and cryptographic techniques or schemes for password authentication are: [10] **RSA based** (This is public key cryptosystem which was proposed by Rivest, Shamir and Adleman in 1978. It is used for encryption. Its security is based on factoring large or huge

numbers), [11][12] **ElGamal based** (It is proposed by ElGamal in 1985. It is public key cryptosystem used for encryption. In it discrete logarithms are calculated depending upon the finite numbers. This scheme is an alternative to RSA for public key encryption. As far as RSA is concerned its security lies in factoring large integers, but security of ElGamal algorithm depends on computing discrete logs of large prime numbers) and [13][14] **Hash based** (This scheme uses various types of hashing which would enhance the performance of the transmission).

Scheme	**Comparative Analysis Done on Schemes on the basis of Literature Review and it is derived that Hash Based scheme is suitable for Mutual Authentication**
RSA Based	It uses one way ciphers or trap door ciphers in which key for encoding (public key) is different from key for decoding (private key). It is vulnerable to and could not withstand the mutual authentication security requirement.Security certificate is required because public key could be used to forge a message. Certification code should be changed with each message.
ElGamal Based	It has the advantage that same plaintext gives a different ciphertext every time when it is encrypted but disadvantage with the scheme is that the ciphertext is twice as long as the plaintext. In this scheme different random number has to be chosen every time by the sender and the receiver, whenever they want to communicate, because of the security protocol at the transport layer. Encryption under this scheme requires exponentiations twice (these exponentiations are independent of message) but decryption only requires one exponentiation. But the scheme is vulnerable to and could not withstand the mutual authentication security requirement.
Hash Based	In it hashing could be done with hashfunction, hashset, hashmap. The said code would be used to encrypt the information to be said. Hashcode always returns same value for the same input, it is consistent method. A good hashcode method is efficient to compute, gives uniform distribution of values (better than RSA and ElGamal) and mathematical analysis is required to prove that the cost of inserting into hash table or searching value in the hash table is O(1). The scheme uses smart card and password for identity verification. The scheme is vulnerable to smart card loss attack but could very well withstand the requirement of mutual authentication.

Table 1: Comparative Analysis of Schemes on the basis of Literature Review

This complete analysis is shown in Fig: 1.1 of all the existing password authentication schemes on the basis of above mentioned attacks and security requirements. After analyzing the existing schemes through Table 1 a conclusion is drawn that hash based scheme is being used by majority of the organizations because it is more convenient to use and more secure than other schemes. But as this scheme is vulnerable to smart card loss attack so following steps would be used in the research paper:

- Hashed finger print would be used as a parameter rather than smart card,
- The scheme could withstand mutual authentication so for that one more tier of security would be added,
- for proving authenticity with hash based scheme passwords would be used along with hashed finger prints,
- Mutual authentication would be done, user id along with index finger print would be sent to client for authentication of client side and
- password along with middle finger print would be used for authentication of server side.

Above mentioned steps would help in the overall fortification of the transport layer security protocol.

3. MINUTIAE POINTS FOR MUTUAL AUTHENTICATION

Password along with fingerprints would be an ideal password authentication scheme which makes use of the combination of two identity authentication parameters. This ideal password authentication scheme would be able to withstand the above said security requirements and would not be vulnerable to various above stated attacks. Now for using finger print as a parameter detailed study of the types of fingerprint and technologies for finger print authentication is required. There are three basic types of fingerprints [15]: Arches (It may be plain (ridge enters from one side, make a wave in the center and flow in the opposite side) or tented (angle is there in the arch). Delta is not there in arch. Loops (ridge count is there). One core and delta is there in loop. Whorls (Any fingerprint that has two or more delta's is whorl). In it one ridge would be having 2 delta's. Everyone falls into one of the above said categories. Within these three categories there are thirty different minutiae points. This makes fingerprint unique because no one has the same number of minutiae points on the same place. Following are the technologies for finger print authentication [16]:

- Correlation (where image itself is used as a template): It is very easy to recreate fingerprint from templates, and which would give access to unauthorized users so it is not safe to use.
- Texture Descriptors (fingerprint texture is used): captures global and local features of a fingerprint in a compact fixed length vector which would be finger code. Correlation and Texture Descriptors give access to unauthorized users so third finger print authentication is used in the research paper which is Minutiae Descriptors.
- Minutiae Descriptors (set of unique features in finger print): Bio hashing is used to replace template based matching (Correlation).

In this research paper, minutiae descriptors would be used for fingerprint authentication. The motive is to create mathematical abstraction of the minutiae information of the fingerprint so that intruder could not get any relevant

information about the original fingerprint. If M is the minutiae point then position(x, y) of M would be required. M could be generated from sensitive fingerprint sensor along with the stated position values. Hash algorithm would be used to generate the hash code of the fingerprint values. There are various hash algorithms which are currently in use for converting fingerprints into hash code The existing hash algorithms are:

Grid hash algorithm [16]: Sometimes there may be a situation that partial fingerprints are provided, which means fingerprints are cut to an acceptable limit. So due to this reason grid algorithm is used because it gives matrices of equal sizes for each fingerprint.

Angle hash algorithm [16]: In this core and delta points are created by putting start of the ridge as core (cx, cy) and the point at the divergence of the ridge is delta(dx, dy). This algorithm divides the fingerprint into grid of squares and the number of minutiae in each square is counted and further they are stored in the form of a matrix at the server as hash code. Minutiae points are M with specified position (x,y).

Now if it is the ith minutiae point, then position of the point would be (xi,yi). Join core, delta with the minutiae point and it would take the form of a triangle. Then calculate the slope of the line. Formula for calculating slope of the line is:

$$M1 = y1 - cy / x1 - cx$$

$$M2 = y1 - dy / x1 - dx$$

Further calculate the angle for this with the use of following formula:

$$\alpha = \tan - 1\, M1 - M2 / 1 + M1.M2$$

And the hash code for the fingerprint would be all the angle calculations:

$$(\alpha 1, \alpha 2, \alpha 3, - - - - - - - - - -, \alpha n)$$

Minimum distance hash algorithm [9]: Sometimes it may happen, that only one global feature core or delta could be traced out. In this algorithm a line would be created from minutiae point to the global point (core or delta). Then distance between the both would be calculated. Suppose M is the minutiae point with (xi,yi) position and (tx,ty) if the value of the global point core or delta. Now distance between the ith minutiae point and global point would be di. The formula for calculating di is as follows:

$$di = \sqrt{((xi - tx)^2 + (yi - gy)^2)}$$

Now the minutiae point which would be having the least distance would be core and the process would carry on iteratively. And the algorithm would result in the network of connected line segments. Once this network is generated then by using the property of line segments such as length and the slope of line, hash code would be generated. Any fingerprint with M minutiae points would have hash code as:

$$(p1, p2, p3, - - - - - - - -, pm)$$

where p is the parameter which is used for hash code.

The research paper uses following steps for formulating a proof of fortification of the transport layer security protocol by use of ideal password authentication scheme (password along with fingerprint):

- Username would be given as input,
- Password along with finger print (ideal password authentication scheme) value would be used for proving mutual authentication,
- Minutiae descriptors would be used as a technology for finger print authentication.

Overall when this ideal password authentication scheme would be implemented then efficiency of the system would improve. And it would result in addition of one more tier to the security protocol (with the use of fingerprint), by which mutual authentication would be very well implemented and further which would fortify the transport layer security protocol.

4. PROPOSED METHODOLOGY FOR IMPLEMENTING THIS IDEAL PASSWORD AUTHENTICATION SCHEME

The methodology which this research paper has used for implementing this ideal password authentication scheme is as follows:

1. Analysis of Existing Password Authentication Schemes as done in Fig: 1.1,Defining and Comparing the Attacks and Security Requirements as done in Fig: 1.1,

2. Generating an Ideal Password Authentication Scheme with the steps as follows:

   - Hash code value of the password would be stored at the server (database),
   - Fingerprint of index finger and middle finger would be taken with the help of sensors like veridicom sensor and optical digital biometrics sensor etc,
   - Both password and fingerprint would be used for identity authentication of client and server (mutual authentication).

So this scheme would withstand mutual authentication security requirement, initially organization which is having multi-server environment would store these values on different servers so that phishing could almost diminish. Very first time when user would insert these values (password, middle finger fingerprint, index finger fingerprint), it would be stored in the database as mentioned above in Fig: 1.2. Every time when user want's to prove authenticity, this ideal password authenticity scheme would be used for mutual authentication. Ideal password authentication scheme would use password and fingerprint which would enhance security as one more tier is added to the security protocol.

3. Matching of password and fingerprint with the values stored at server for identity authentication, check the authenticity of the scheme by implementation it in the organization with multi-server environment (Fig: 1.2) and dealing with e-payments and e-communication,

4. Generate a proof of fortification of Transport Layer Security Protocol which is discussed in details in Section V,
5. Validation of the results which is done as follows: A Simulator would be framed with the help of C#.Net and SQL Server which would generate a multi server environment.

The following steps would be followed to validate the results: A form would be created with the help of C#.Net which would ask user for initial input values which are username, image of the choice of user, password, fingerprint of index and middle finger, Database would be created in SQL Server which would store initial input of the Username, Image (Selected by the User), Password and hashed finger print values of Index and Middle finger of the legitimate user, So the database would have username stored in the text format, image only jpeg format, password in hashed code and index and middle finger fingerprints in the hashed code format.

Organizations would use the multi-server environment as follows:

User ID	
Image (Selected by Legitimate User)	Server 1
Password (Hash Code)	
Middle Finger (Hash Code)	Server 2
Index Finger (Hash Code)	Server 3

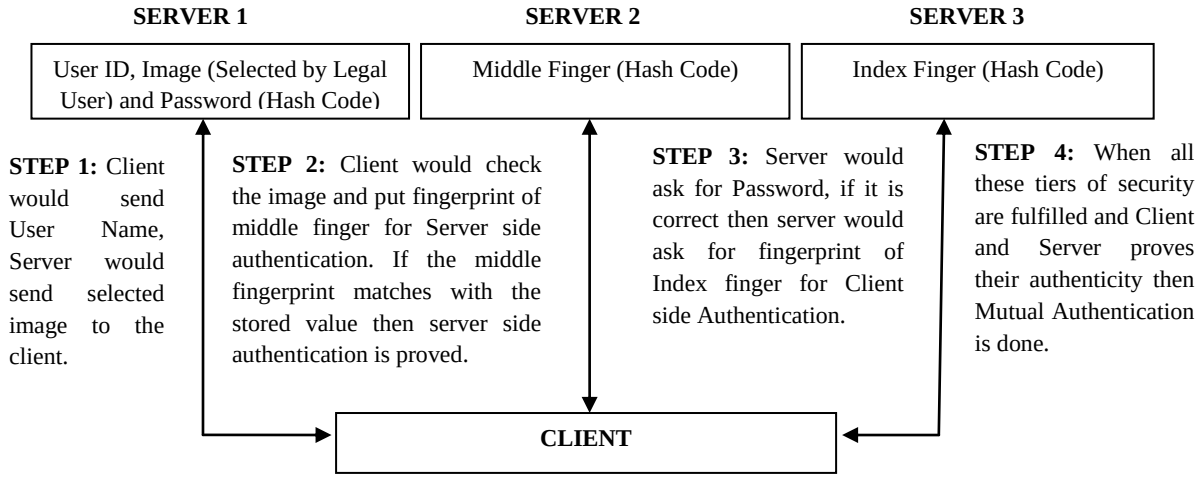

Fig: 1.2 Proposed Methodology for Multi Server Environment for this ideal password authentication scheme.

Then steps for mutual authentication would be followed which are:

STEP 1 Client would send User Name, Server would send selected image to the client.

STEP 2 Client would check the image and put fingerprint of middle finger for Server side authentication. If the middle fingerprint matches with the stored value then erver side authentication is proved.

STEP 3 Server would ask for Password, if it is correct then server would ask for fingerprint of Index finger for Client side Authentication.

STEP 4 when all these tiers of security are fulfilled and Client and Server prove their authenticity then Mutual Authentication is done. It will result in the fortification of the Transport Layer Security Protocol.

6. Suggesting measures for future Ideal Password Authentication Scheme which is discussed in Section VI.

Above suggested is the proposed methodology for implementing this ideal password authentication scheme of password and fingerprint as identity parameters.

Password and fingerprint assimilated together would result in Ideal Password Authentication Scheme. This scheme would be implemented at the login phase for mutual authentication of client and server.

IP Spoofing or Server Spoofing will almost diminish with this Ideal Password Authentication Scheme. Suggested methodology would result in fortification transport layer security protocol.

5. FORTIFICATION OF TRANSPORT LAYER SECURITY PROTOCOL

This research paper results in generating an ideal password authentication scheme (password along with fingerprint) which would fortify the transport layer security protocol. The following objectives would be met if this ideal password

authentication scheme would be implemented in the multi server environment:

- Identification of the Risks associated with SSL VPN,
- Accumulation of one more tier to the Security Protocol,
- Non vulnerability and withstanding of Ideal Password Authentication Scheme to the defined attacks and security requirements,
- Withstanding of the Mutual Authentication Security Requirement,
- Less scope of IP or Server Spoofing,
- Implementation of the Ideal Password Authentication Scheme in Server side SSL,
- Accomplishment of the Goals of Ideal Password Authentication Scheme,
- Fortification of the Transport Layer Security Protocol,
- Scope of research paper in organizations dealing with e-payments or e-communication etc.

There are many password authentication schemes like RSA-based Password Authentication Schemes, ElGamal based Password Authentication Schemes and Hash-based Password Authentication Schemes. In this research paper hash based scheme is used to store fingerprint as hash code in the server.
These password authentication schemes secure transport layer from Denial of Service Attacks, Forgery Attacks (Impersonation Attacks), Forward Secrecy, Mutual Authentication, Parallel Session Attacks, Password Guessing Attacks, Replay Attacks, Smart Card Loss Attacks and Stolen-verifier Attacks. Adding more tiers of security strengthen the record and handshake protocol of Secured Socket Layer. And enhancement of SSL results in the fortification of transport layer security protocol.

With the implementation of ideal password-authentication scheme in multi-server environment of any Organization, the proof is generated that mutual authentication enhances the integrity and security which is part of record and handshake protocol of SSL, and by strengthening SSL, transport layer is fortified.

This ideal password authentication scheme would not be vulnerable to attacks and would be able to withstand the security requirements. When the security requirements are fulfilled then transmission or communication results in data integrity and security which would further result in the fortification of transport layer. The major security requirements which, this ideal password authentication scheme would fulfill are: Confidentiality, Integrity, Authentication, Non-Repudiation, Availability, Anonymity, and Traffic Analysis.

This research paper states that ideal password authentication scheme would enhance the transport layer security protocol. This scheme visualizes the following benefits which far sure make the communication process at the transport layer more secure:

- Two parameters are used in the ideal password authentication scheme, which are password and fingerprint to enhance security,
- This ideal password authentication scheme would withstand mutual authentication security requirement,
- Client will authenticate Server and Server would authenticate Client,
- Login process would be complete after proving authenticity in three phases so intruders could fail at one or another step,
- By adding tiers security is enhanced and possibility of intruder getting failed on any of the tier is very large,
- IP or Server spoofing is not possible with the implementation of ideal password authentication scheme,
- Malicious attempts and phishing by the intruders is not possible with this Ideal Password Authentication Scheme,
- Mutual authentication is done at the login phase for identification of client and server,
- This Ideal Password Authentication Scheme results in fortification of the transport layer security protocol.

So adding more tier to the security protocol enhances the process of security. This ideal password authentication scheme with two parameters password and fingerprint executed together, would overall result in the fortification of the transport layer security protocol.

6. CONCLUSION

While verifying the goal accomplishment of the ideal password authentication scheme there would be certain constraints in meeting goals of all the security requirements of security protocol. Although this ideal password authentication scheme claims:

- to fulfill all the specified goals and not to be vulnerable to attacks ,
- to include two parameters to add more security,
- for mutual authentication,
- to withstand security requirements and
- to fortify the transport layer security protocol.

But certain constraints may exist while executing the process. So all the constraints are to be mentioned when and where they exist and measures are to be suggested for mitigation upon the risks involved in implementation of the ideal password-authentication scheme.

If the above stated ideal password authentication scheme executed properly would surely enhance security, would make e-payments or e-communication more authentic. Organizations which have multi-server environment could successfully implement this ideal password authentication scheme.
This ideal password authentication scheme would be generated with two parameters for identity authentication which are password and fingerprint to add more tiers to the security which would result in diminishing the possibility of phishing, IP or Server Spoofing.
So overall it would result in the fortification of transport layer security protocol. In the future, fortification of Transport Layer Security Protocol could be done:

- By generating a new hash algorithm for converting input of fingerprint minutiae points to hash code.
- This could be very well implemented in the multi-server environment of any organization.
- Mutual Authentication could be done with Password and Fingerprints but hash code values could be

generated by making use of any new hash algorithm which will make the execution faster.

- One more identity parameter could be used for authentication which is Smart Card.
- Collectively three identity parameters Password, Smart Card and Fingerprint could be used for generating an Ideal Password Authentication Scheme.
- New Hash Algorithm could be suggested which would convert fingerprint into hashed code much faster than existing algorithms.
- Assimilation of this new hash algorithm with three identity parameters could enhance security at the transport layer.

This ideal password authentication scheme with two identity parameters password and fingerprint would meet all the security requirements and would achieve all the goals. There may be a possibility of generating a future ideal password authentication scheme by making use of three identity authentication parameters like Password, Smart Card and Fingerprint etc for mutual authentication in a multi server environment. And further this ideal password authentication scheme in multi server architecture would help in fortification of Transport Layer Security Protocol.

7. REFERENCES

[1] E. Bresson, O. Chevassut, and D. Pointcheval," Security Proofs for an Efficient Password-Based Key Exchange," in 10th ACM Conference on Computer and Communications Security, pp. 1-2,October 27, 2003, Washington, DC, USA.

[2] Peter Buhler, Thomas Eirich, Michael Steiner and Michael Waidner," Secure Password-Based Cipher Suite for TLS", in Network and Distributed Systems Security Symposium(NDSS 2000),San Diego, California, February 2000.

[3] Craig A. Huegen, "Network-Based Denial of Service Attacks," www.pentics.net/ denial-of-service/presentations/.../19980209_dos.pp...

[4] David A. McGrew and Scott R. Fluhrer ,"Multiple forgery attacks against Message Authentication Codes," eprint.iacr.org/2005/161.pdf ,Cisco Systems, Inc., May 31, 2005

[5] Vipul Goyal, Virendra Kumar, Mayank Singh, Ajith Abraham and Sugata Sanyal ," CompChall: Addressing Password Guessing Attacks," http://eprint.iacr.org /2004/136.pdf , 2003

[6] Kim Davis," DNS Cache Poisoning Vulnerability Explanation and Remedies," www.iana.org/about/.../davies-viareggio-entropyvuln-081002.pdf,Viareggio Italy October 2008,

[7] DongGook Park, Colin Boyd and Sang-Jae Moon ,"Forward Secrecy and Its application to Future Mobile Communications Security," www.dgpark6.com/ Down/pkc2000_FwdSec.pdf

[8] "Mutual Authentication," en.wikipedia.org/wiki/Mutual_authentication

[9] Rajaram Ramasamy, Amutha Prabakar Muniyandi ,"New Remote Mutual Authentication Scheme using Smart Cards," Transactions on Data Privacy ,Volume 2, p-141—152,2009

[10] Tom Davis," RSA Encryption," http://www.geometer.org/mathcircles,October 10, 2003

[11] Brent Waters, Allison Bishop, El Gamal Encryption CS395T Advanced Cryptography, Lecture 3,27th January 2009

[12] "ElGamal Encryption Example," www.informatics.indiana.edu/markus/i400/ lecture7.ppt

[13] Kumar Mangipudi and Rajendra Katti,"A Hash-based Strong Password Authentication Protocol with User Anonymity," International Journal of Network Security, Vol.2, No.3, PP.205–209, May 2006 (http://isrc.nchu.edu.tw/ijns/)

[14] Hanjae Jeong, Dongho Won and Seungjoo Kim ,"Weaknesses and Improvement of Secure Hash-Based Strong-Password Authentication Protocol," Information Security Group, Journal Of Information Science and Engineering 26, 1845-1858 (2010)

[15] "Basic Types of fingerprints," http://www.odec.ca/projects/2004/fren4j0/public_html/ fingerprint_patterns.htm

[16] Sahil Goyal and Mayank Goyal," Generation of hash functions from fingerprint scans," October 2011