# Fortification of Transport Layer Security Protocol with Hashed Fingerprint Identity Parameter

**Kuljeet Kaur[1] and G Geetha[2]**

**[1] School of Computer Applications, Lovely Professional University, Phagwara
Phagwara, Punjab 144401, India**

**[2] School of Computer Applications, Lovely Professional University, Phagwara
Phagwara, Punjab 144401, India**

**Abstract**

Identity over the public links becomes quiet complex as Client and Server needs proper access rights with authentication. For determining clients identity with password Secured Shell Protocol or Public Key Infrastructure is deployed by various organizations. For end to end transport security SSL (Secured Socket Layer) is the de facto standard having Record and Handshake protocol dealing with data integrity and data security respectively. It seems secure but many risks lurk in its use. So focus of the paper would be formulating the steps to be used for the enhancement of SSL. One more tier of security to the transport layer security protocol is added in this research paper by using fingerprints for identity authentication along with password for enhancement of SSL. Bio Hashing which will be done with the help of Minutiae Points at the fingerprints would be used for mutual authentication. New hash algorithm RNA-FINNT is generated in this research paper for converting minutiae points into hashed code. Value of hashed code would be stored at the Database in the Multi Server environment of an organization. Research paper will perform mutual authentication in the multi server environment of an organization with the use of fingerprint and password both as identity authentication parameters. This will strengthen record and handshake protocol which will enhance SSL and further enhancement of SSL will result in the fortification of Transport Layer Security Protocol.

Keywords: *Mutual Authentication, Minutiae Points, Secured Socket Layer, Multi Server Environment, Hashed code*

## 1. Introduction

Convenient mechanism of proving authenticity over the public link is the use of Passwords. Communication over the public link starts by sharing a (short) password within a session which is created between Client and Server with Session key. Impersonation, forgery, parallel session attack, IP spoofing, ping of death, server spoofing, denial of service attacks etc is possible at the transport layer. So organizations deploy Secure Shell protocol and Public Key Infrastructure for security [1]. Even the protocols function well but intruders can attempt to break any of the existing security protocols and could hack the password. The major concern in implementation of secured shell protocol and public key infrastructure is the security of passwords.

i. In Secure Shell Protocol the client is asked to log into another computer at some remote location with some password authentication. After proper authentication with password is done then only the files could move from one location to another. In this case remote machine maintains the association between client name and password [1].

ii. In Public Key Infrastructure, the password authenticated key exchange provides the two computing devices. Session (It is created with the valid password authentication) key is there with the computing devices to implement an authenticated communication channel. Within this communication channel messages sent over the wire are cryptographically protected [1].

Again in both the cases password security is the prime concern. So, need of adding one more tier of security by using one more identity authentication parameter which is fingerprint along with password is generated.

Moreover for end to end transport security SSL (Secured Socket Layer) is the de facto standard. SSL (Secure Sockets Layer) is an Internet protocol that allows all the visitors of the particular website to connect to a secure and encrypted webpage. In the public link organizations create

their Virtual Private Network (VPN), also known as clientless VPN or web VPN.
SSL-VPN is an emerging technology that provides remote-access VPN capability by using the SSL function [2]. Now the webpage which is having SSL implemented is protected and quiet secure so any information like names, addresses, credit card data and survey answers submitted through that webpage are masked during the transmission. But generally for complete transmission to get started only passwords are used for identity authentication.
So for adding one more tier of security for mutual authentication fingerprint would be used along with password as identity authentication parameters. This tier of security would enhance SSL and result in fortification of Transport Layer Security Protocol.

The structure of the remainder of the paper is as follows. In Section II description of benefits and risks associated with the implementation of SSL and steps required for successful implementation of SSL for enhancing security. In Section III description of minutiae points of fingerprint identity parameter used for proving mutual authentication. Focus would be on the technology of minutiae descriptors for extracting fingerprint value. In Section IV new hash algorithm RNA-FINNT which will convert fingerprint value to hashed code for storing in database. In Section V enhancement of SSL with two identity parameters password and fingerprint which will result in fortification of Transport Layer Security Protocol and Section VI concludes the paper.

## 3. Benefits and Risks associated with SSL and steps required for successful implementation of SSL

SSL is an Internet Protocol which uses a combination of public-key and symmetric-key encryption. Public key encryption provides better authentication techniques but symmetric key encryption is much faster than public key infrastructure. Major advantageous associated with the SSL are [2]:

i. It provides a secure connection between remote users and internal network resources
ii. It has outbound connection security
iii. It does not require additional client software to be installed on the end point device.
iv. It builds trust relationship of client on your webpage
v. It minimizes disputes caused by credit card frauds

This protocol seems very secure as the connection between remote users and internal network resources is very authentic and protected but there are lot many risks which lurk in its use like [2]:

i. lack of required host security software on public machines
ii. physical access to shared machines
iii. keystroke loggers
iv. endpoints—loss of sensitive information and intellectual property
v. Man-in-the-middle attack etc.

Because of these risks possibility of impersonation or forgery is there. SSL has two protocols: record and handshake. Record protocol focuses on format which is used to transmit data. And Handshake involves using SSL record protocol for message exchange. A session of
SSL always begins with exchange of messages which are called SSL Handshake. It allows the server to authenticate itself to the client but client optionally authenticates itself to server. So, overall complete mutual authentication is required in the SSL. This is done by adding one more tier of security by using fingerprint as identity parameter along with password. Both identity parameters would perform mutual authentication and enhance SSL.

Above this, few steps which are required for successful implementation of the SSL are [3]:

i. Strong user authentication is required for which security policies should be strengthened.
ii. Host should be verified at each login.
iii. System which you are using should not be publically accessed or should be secure.
iv. Cache should be regularly cleaned.
v. Continuous detection of keystroke loggers is required.
vi. Security awareness among the users is required and it could be done by educating them with security policies.
vii. Mutual authentication should be there.

With these steps SSL could be successfully implemented in the organization. And as discussed above by adding one more tier of the security with fingerprint as identity parameter along with password mutual authentication would be done.
Mutual authentication will strengthen record and handshake protocol of SSL which will enhance SSL and enhancement of SSL will result in the fortification of transport layer security protocol.

## 3. Minutiae Descriptors technology used for extracting Fingerprint value

Fingerprints are of three types [4]: Arches (It may be plain or tented and angle is there in the arch. Start of ridge in the arch is core and end of ridge is delta, but arches do not have delta value), Loops (One core and delta is there in the loop and ridge count is there) and Whorls (Number of delta's are two). Everyone falls into one of the above said categories. And the technologies which are used for extracting fingerprint value are as follows [6]:

- **Correlation** (Image of the fingerprint is used as a template. It gives access to unauthorized users because recreating fingerprint from image is very easy.)
- **Texture Descriptors** (Texture of the fingerprint is used as a template. For using texture certain global and local features of a fingerprint are captured as a compact fixed length vector. It gives access to unauthorized users so it is not safe to use.)
- **Minutiae Descriptors** (These are set of unique features in a fingerprint. Template based matching is replaced with this bio hashing.)

Within the three categories of fingerprint arches, loops and whorls, there are thirty different minutiae points. These minutiae points makes fingerprint unique because no one has the same number of minutiae points on the same place. So in this research paper minutia points would be used to extract the fingerprint value. And with the help of following steps SSL would be enhanced with fingerprint identity parameter for fortifying transport layer security protocol:

- Hashed finger print would be used as a identity parameter (New Hash Algorithm RNA-FINNT mentioned in Section IV would be used to save value of hashed fingerprint into the database)
- By using fingerprint value one more tier of security is added and mutual authentication would be done
- for proving authenticity in tiers passwords would be used along with hashed finger prints (value would be extracted through minutiae points over the fingerprints)
- 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 [5].
- Different servers would be used to store these values of User ID, fingerprints. It will create a Multi Server Environment.

Above mentioned steps would perform mutual authentication in the multi server environment of an organization and would enhance SSL which will help in the overall fortification of the transport layer security protocol.

## 4. New Hash Algorithm RNA-FINNT for converting Fingerprint value to Hashed code

In this research paper, minutiae descriptors would be used for fingerprint authentication. Mathematical abstraction of the minutiae points of the fingerprint is done so that intruder could not get any relevant information about the original fingerprint. Any sensitive fingerprint sensor could be used to scan the fingerprint. Extracted value would be M which is the minutiae points along with the stated position values (x, y) at the fingerprint.

New hash algorithm RNA-FINNT would be used to generate the hash code value which would be stored in the database. There are various hash algorithms which are currently in use for converting fingerprints into hash code. The existing hash algorithms are [6]:

**Grid hash algorithm** (Partial fingerprints are provided and it gives matrices of equal sizes for each fingerprint),

**Angle hash algorithm** (In this algorithm core and delta points would be joined with the minutiae points and it would take the form of a triangle. X and Y are the positions of M, CX and CY are the positions of Core and DX and DY are the positions of Delta. Then slope of line would be calculated (from position values of X, Y, CX, CY and DX, DY) and angle would be stored as a hashed code value in the database and

**Minimum Distance Hash Algorithm**

(Only one global feature would be considered in this algorithm. Line would be drawn from position (TX and TY) of one global feature to M and the distance between the points would be calculated. Same value would be stored in the database as a hashed code).

**RNA-FINNT Hash Algorithm (Reduced Number of Angles-Fingerprint Hash Algorithm)**

In this research paper new hash algorithm is generated which results in reduced number of angles, would increase the efficiency of the system, would enhance the security at the transport layer and execution of which would be much faster than the already existing hash algorithms.

The algorithm would execute in the following manner (Fig. 1):

1. Sensor (veridicom sensor and optical digital biometrics sensor etc) would be used to take fingerprint of the user for first time.

2. Fingerprint would be divided into grid of squares and the number of minutiae points in each square is counted.

3. If the number of minutiae points in a specific square of a grid is less than or equal to 2 then the same count value would be the hashed code and would be stored in the matrix.

4. But if the number of minutiae points in a specific square of a grid is more than 2 then any one minutiae point would be picked at random.

5. Global feature core or delta would not be included rather one of the minutiae point would act as central point and connection between all the minutiae points in specific square of the grid would be generated.

6. All minutiae points would be connected and slope of line would be calculated (as mentioned in Eq. (1)). And from slope of line angles would be calculated (as mentioned in Eq. (2)).

7. This would result in RNA (reduced number of angles) as global features are not used.

8. Angle from each square of a grid would be stored in the database in row matrix and it is the hashed code for the fingerprint.

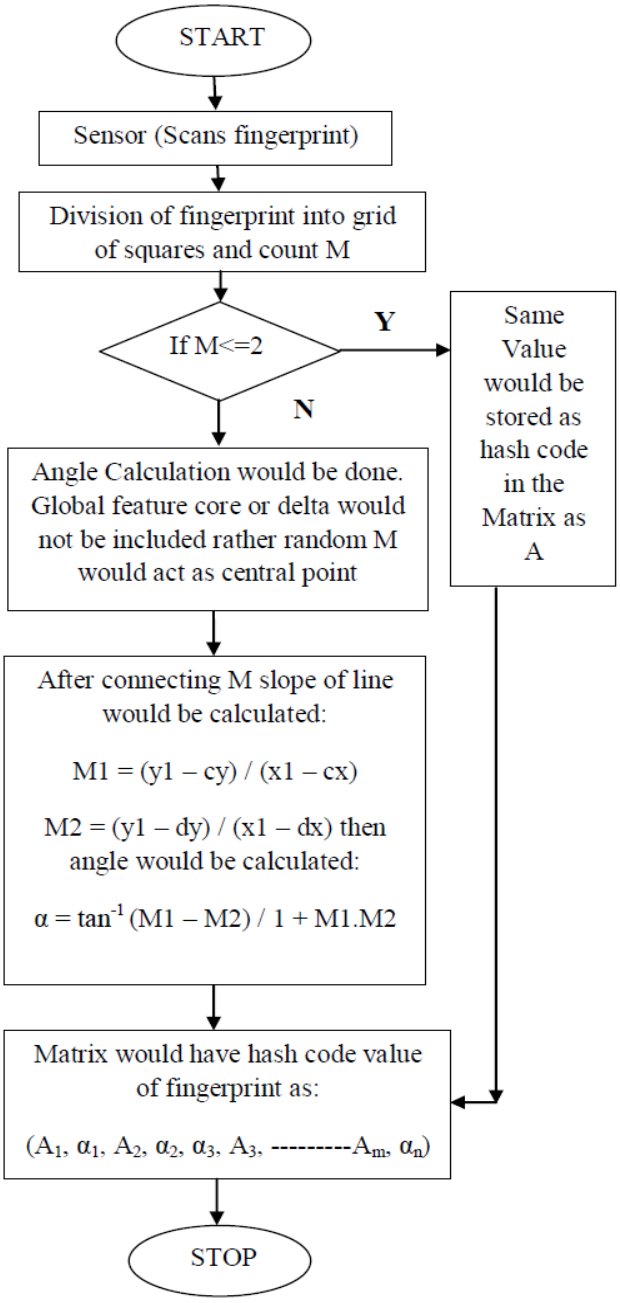


Fig. 1 New Hash Algorithm for converting fingerprint into hashed code: RNA-FINNT Hash Algorithm

**Example:**
Let the number of M in a square of a grid is 3. Position of one of the minutiae points M would be (x, y), second M would be (cx, cy) and the third minutiae point would be (dx, dy). Join all the M and pick one of the M as central point.

Slope of line would be calculated as follows:

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

$$M2 = y1 - dy / x1 - dx \quad (1)$$

After calculating slope of line, angle would be calculated with the use of following formula:

$$\alpha = \tan^{-1} M1 - M2 / 1 + M1.M2 \quad (2)$$

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

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

This output would be stored as the row matrix into the database.

This new hash algorithm would give output as a matrix which would have different values for each square of the grid (as mentioned in Eq. (3)). Either the square of the grid would have minutiae count as hash code value or the angle of the minutiae point would be the hash code.

**RNA-FINNT gives the following benefits:**

1. It has resulted in **RNA** (reduced number of angles) as global features core and delta are not used for calculations.

2. There is **no dependency** in the algorithm as any minutiae point could be picked at random for angle calculation.

3. All the squares of grid run in **parallel** so execution of the algorithm is much **faster** than the existing hash algorithms.

4. It has resulted in the **increased efficiency** of the system while execution.

5. All minutiae points in each square are being considered so it will result in **error reduction**.(Discussed in Section V Point 6)

6. Two parameters password and fingerprint are used to **enhance SSL resulting in the fortification of Transport Layer Security Protocol** by adding one more tier of security.(Discussed in Section III)

So this research paper focuses on minutiae descriptors as the technology for extracting fingerprint value and RNA-FINNT converts the extracted fingerprint value to the hashed code.

And same hash code is stored in the database. Intruder could not get any relevant information about the original fingerprint so for that mathematical abstraction of M is done. Password and fingerprint as the two security tier would enhance the mutual authentication process at transport layer.

## 5. Enhancement of SSL with two Identity Parameters resulting in Fortification of Transport Layer Security Protocol

If fingerprint is added as an identity parameter it would enhance SSL and the following benefits are visualized which far sure make the communication process at the transport layer more secure:

1. Two parameters (Password and Fingerprint) are used for login process.

2. Mutual Authentication is done as discussed in Section III (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).

3. Possibility of the failure of intruder would be at each step as the Login process is in phases.

4. IP or Server spoofing is not possible with the implementation of tiers to the security of Transport Layer.

5. Less number of angles is generated in the RNA-FINNT Hash Algorithm which resulted in the increased efficiency of the system.

6. For fingerprint authentication general rule is that 8 to 12 minutiae points should be considered before identification can be positive [7]. So the error approximation rate is high. But RNA-FINNT considers are the minutiae points which

would be part of the square of a grid of the fingerprint so it results in error reduction.

Authentication is done in phases and by assimilating fingerprint one more tier to security of transport layer is added. Mutual Authentication is done in the login process which will strengthen data security and integrity in the record and handshake protocol of SSL. Strengthening of both record and handshake protocol would result in enhancement of SSL. When SSL is enhanced the outcome would be fortified transport layer.

## 6. Conclusion

When we are using public links then security of the communication is the prime concern. This paper has stated that authentication should be done in tier. Client and Server both should authenticate each other by mutual authentication so that IP or Server Spoofing could not be there. Organizations, who have implemented SSL, could enhance SSL by using the steps mentioned in this paper in Section V. One more tier of security is added by assimilating fingerprint as an identity parameter along with password in the Multi Server Environment of any organization. RNA-FINNT is used to convert the extracted fingerprint value from minutiae points to hashed code. Proposed scheme of implementing security in tier with two identity parameters password and fingerprint would strengthen the record and handshake protocol of SSL. By strengthening these protocols SSL would be enhanced and result would be the fortification of transport layer security protocol.
For future there may be a possibility of implementing security in tier by using three identity parameters Password, Smart Card and Fingerprint for mutual authentication in a multi server environment of any organization.

## 7. References

[1] "Secured Shell Protocol and Public Key Infrastructure", http://www.ietf.org/rfc/rfc4716.txt

[2] "SSL Essentials: Technology, Applications, Advantages, Disadvantages", http://apps1.eere.energy.gov/buildings /publications/pdfs/ssl/dowling_ssl_essentials_07-16-07. pdf

[3] "SSL VPN Security", http://www.cisco.com/web /about/security/intelligence/05_08_SSL-VPN- Security.html

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

[5] 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)

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

[7] "Fingerprint Matching", http://members.fortunecity.com/julzjerg/finger.htm

**First Author** Asstt.Prof. Kuljeet Kaur is heading the domain of Systems and Architecture in the School of Computer Applications at Lovely Professional University, India. She is research scholar of PhD in Lovely Professional University, India. She has successfully implemented 5 projects. She has published 11 research papers in refereed Journals and Conferences. She serves as Reviewer in the International Journal of Research in Computer Science. She has attended 3 International Workshops and Faculty Development Programs. Her interest areas are Network Security, Identity Authentication and Systems Architecture. She is an active member of CSTA, ISCA, CSI and ISTE.

**Second Author** Prof.G.Geetha is heading School of Computer Science and Applications, Lovely Professional University, India. Her research interest includes Cryptography, Information security and Image Processing. She has published more than 50 research papers in refereed Journals and Conferences. She serves as Editorial Board member and reviewer in various Journals and Conferences. She is presently the President of Advanced Computing Research Society. She is an active member of various professional organizations like ISCA, ISTE, CRSI etc.