Journal of Information Security, 2013, 4, 197-202
http://dx.doi.org/10.4236/jis.2013.44022 Published Online October 2013 (http://www.scirp.org/journal/jis)

Diminution in Error Approximation by Identity Authentication with IPAS for FTLSP to Enhance Network Security

Kuljeet Kaur, Geetha Ganesan
School of Computer Applications, Lovely Professional University, Phagwara, India
Email: jeetbrar17@gmail.com

Received July 6, 2013; revised August 7, 2013; accepted August 15, 2013

ABSTRACT

In this paper, we have proved the diminution in error approximation when identity authentication is done with Ideal Password Authentication Scheme (IPAS) for Network Security. Effectiveness of identity authentication parameters for various attacks and security requirements is verified in the paper. Result of analysis proves that IPAS would enhance the transport layer security. Proof of efficiency of result is generated with drastic diminution in error approximation. IPAS would have advanced security parameters with implemented RNA-FINNT which would result in fortification of the transport layer security protocol for enhancement of Network Security.

Keywords: Fingerprint; Error Approximation; Network Security; Fortification; Transport Layer

1. Introduction

Identity Authentication could be done with Password, Smart Cards and Fingerprints. As the Smart card loss is very common attack on the network so this identity authentication parameter is not completely reliable. Password faces the dictionary attacks, stolen verifier attack, and man in the middle attack etc in common. So it states that there should be an Ideal Password Authentication Scheme which should have an assimilation of most effective identity authentication parameters. Survey on user's choice was done and it concluded that fingerprint would be the most acceptable identity authentication parameter in future along with password [1]. So assimilation of password and fingerprint would generate an ideal password authentication scheme [2].

Fingerprint could be extracted on the basis of template, texture and minutiae points. Amongst the three minutiae points, it is the most effective as no one has the same number of points on the same place. Minutiae points give uniqueness to the fingerprint. There are various algorithms for extracting minutiae points like grid hash, angle hash and minimum distance hash. But we derived a new algorithm RNA-FINNT for extracting the minutiae point's values of the fingerprint [3]. This paper has validation of diminution in error approximation in terms of percentage. IPAS which is generated with assimilation of password and fingerprint is used to validate the results. RNA-FINNT is used to extract values of minutiae points [3]. Calculations with respect to various fingerprint extraction algorithms are done by assimilating them with Password. Comparative analysis of all these calculations validates that the percentage of error would reduce when password is assimilated with fingerprint in which extraction of minutiae points is performed by RNA-FINNT.

Remainder sections of the paper prove this validation. Section 2 proposes methodology for proving the diminution in error approximation, Section 3 states the effectiveness of Identity Authentication Parameters for various Attacks and Security Requirements, Section 4 generates a proof of Diminution in Error Approximation and Section 5 suggests the advanced security parameters of ideal password authentication scheme which results in fortification of transport layer security protocol for enhancement of network security.

2. Proposed Methodology for Proving the Diminution in Error Approximation

To prove diminution in error approximation we have used a comparative study in which assimilation of existing fingerprint extraction algorithms is dome with password. Our new algorithm RNA-FINNT is also assimilated with password which generates an ideal password authentication scheme. Multi server environment is required for implementation of IPAS [4]. Methodology proves that IPAS results in diminution in error approximation. Flowchart defines the proposed methodology (**Figure 1**).

2.1. Mentioned below Is the Stepwise Process for Proving Diminution in Error Approximation

Step 1: Calculate the total number of Attacks and Security Requirements possible on each Identity Authentication Parameter. This implies for password, fingerprint (extraction with Grid Hash Algorithm) [5], fingerprint (extraction with Angle Hash Algorithm) [5], fingerprint (extraction with Minimum Distance Hash Algorithm) [5] and fingerprint (extraction with RNA-FINNT Hash Algorithm) [3].

Step 2: Calculate the total number of Attacks and Security Requirements possible if password is assimilated with on each Identity Authentication Parameter. This implies for password assimilation with fingerprint (extraction with Grid Hash Algorithm), fingerprint (extraction with Angle Hash Algorithm), fingerprint (extraction with Minimum Distance Hash Algorithm) and fingerprint (extraction with RNA-FINNT Hash Algorithm) respectively.

Step 3: Proof would be derived from the result of Step 2 that less number of attacks are possible if password is assimilated with fingerprint (extraction with RNA-FIN-

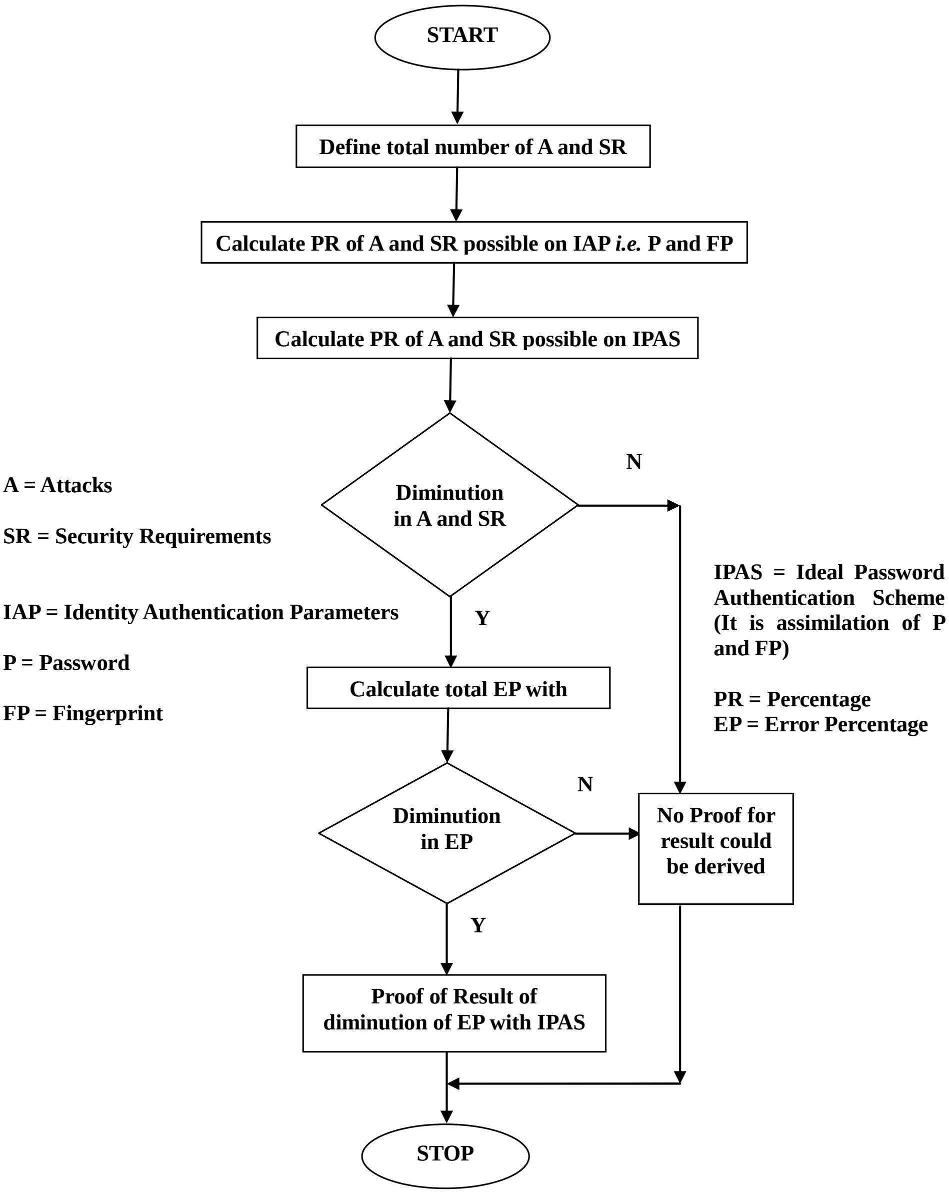
START
Define total number of A and SR
Calculate PR of A and SR possible on IAP i.e. P and FP
Calculate PR of A and SR possible on IPAS
Diminution in A and SR
N
Y
A = Attacks
SR = Security Requirements
IAP = Identity Authentication Parameters
P = Password
FP = Fingerprint
IPAS = Ideal Password Authentication Scheme (It is assimilation of P and FP)
PR = Percentage
EP = Error Percentage
Calculate total EP with
Diminution in EP
N
Y
No Proof for result could be derived
Proof of Result of diminution of EP with IPAS
STOP

Figure 1. Proposed methodology for proving diminution in error approximation.

NT Hash Algorithm) which is an Ideal Password Authentication Scheme.

Step 4: Calculate the total error percentage if password is assimilated with on each Identity Authentication Parameter. This implies for password assimilation with fingerprint (extraction with Grid Hash Algorithm), fingerprint (extraction with Angle Hash Algorithm), fingerprint (extraction with Minimum Distance Hash Algorithm) and fingerprint (extraction with RNA-FINNT Hash Algorithm) respectively.

Step 5: Proof would be derived from the result of Step 4 that less number of error would be there if password is assimilated with fingerprint (extraction with RNA-FINNT Hash Algorithm) which is an Ideal Password Authentication Scheme.

Error Approximation = e

Password = p

Total Number of defined Attacks and Security Requirements = n

Number of Attacks on p = t (p)

Error Approximation in p = p (e)

Fingerprint Extracted Value through Grid Hash Algorithm = f (g)

Number of Attacks on f (g) = t (f (g))

Error Approximation in f (g) = f (g) (e)

Fingerprint Extracted Value through Angle Hash Algorithm = f (a)

Number of Attacks on f (a) = t (f (a))

Error Approximation in f (a) = f (a) (e)

Fingerprint Extracted Value through Minimum Distance Hash Algorithm = f (m)

Number of Attacks on f (m) = t (f (m))

Error Approximation in f (m) = f (m) (e)

Fingerprint Extracted Value through RNA-FINNT Hash Algorithm = f (r)

Number of Attacks on f (r) = t (f (r))

Error Approximation in f (r) = f (r) (e)

Total Number of Attacks and Security Requirements possible if:

1) *p is assimilated with f (g) = p (f (g))*
2) *p is assimilated with f (a) = p (f (a))*
3) *p is assimilated with f (m) = p (f (m))*
4) *p is assimilated with f (r) = p (f (r))*

Total Error Percentage when p is assimilated with f (g) = te (pg)

Total Error Percentage when p is assimilated with f (a) = te (pa)

Total Error Percentage when p is assimilated with f (m) = te (pm)

Total Error Percentage when p is assimilated with f (r) = te (pr)

Total Number of defined Attacks and Security Requirements are n but if:

1) *p is assimilated with f (g) = n (p (f (g)))*
2) *p is assimilated with f (a) = n (p (f (a)))*
3) *p is assimilated with f (m) = n (p (f (m)))*
4) *p is assimilated with f (r) = n (p (f (r)))*

2.2. Proposed Methodology for Validating Results

Step 1: Calculate the total number of Attacks and Security requirements possible on each Identity Authentication Parameter.

$$p(e) = \left(t(p) \div n \times 100\right)$$

$$f(g)(e) = \left(t\left(f(g)\right) \div n \times 100\right)$$

$$f(a)(e) = \left(t\left(f(a)\right) \div n \times 100\right)$$

$$f(m)(e) = \left(t\left(f(m)\right) \div n \times 100\right)$$

$$f(r)(e) = \left(t\left(f(r)\right) \div n \times 100\right)$$

Step 2: Calculate the total number of Attacks and Security requirements possible if *p* is assimilated with each Identity Authentication Parameter.

$$p\left(f(g)\right) = t(p) + t\left(f(g)\right) - \left(t(p) \cup t\left(f(g)\right)\right)$$

$$p\left(f(a)\right) = t(p) + t\left(f(a)\right) - \left(t(p) \cup t\left(f(a)\right)\right)$$

$$p\left(f(m)\right) = t(p) + t\left(f(m)\right) - \left(t(p) \cup t\left(f(m)\right)\right)$$

$$p\left(f(r)\right) = t(p) + t\left(f(r)\right) - \left(t(p) \cup t\left(f(r)\right)\right)$$

Step 3: Proof is derived from Step 2 that less number of attacks are possible if p is assimilated with f (r) *i.e.* an Ideal Password Authentication Scheme.

Proof: *p* (*f* (*r*)) is best for Identity Authentication.

Step 4: Calculate the Total Error Percentage if *p* is assimilated with each Identity Authentication Parameter.

$$te(pg) = p(e) + f(g)(e) - n\left(p\left(f(g)\right)\right)$$

$$te(pa) = p(e) + f(a)(e) - n\left(p\left(f(a)\right)\right)$$

$$te(pm) = p(e) + f(m)(e) - n\left(p\left(f(m)\right)\right)$$

$$te(pr) = p(e) + f(r)(e) - n\left(p\left(f(r)\right)\right)$$

Step 5: Proof is derived from Step 4 that less number of error would be there if assimilation of *p* with *f*(*r*) is implemented *i.e.* Ideal Password Authentication Scheme.

When the above mentioned steps are executed in the sequential order then the resulted output shows the error diminution. This process is implemented through the framework specifically designed to prove the result [6]. Through the framework fingerprint extraction is done through RNA-FINNT and is assimilated with the Password. This assimilation is IPAS which is an Ideal Password Authentication Scheme and results in the diminution of error percentage while matching the fingerprint. Section 4 validates the result with exact data for proving the diminution in the error approximation.

3. Effectiveness of Identity Authentication Parameters for Various Attacks and Security Requirements

As mentioned in Section 2 flowchart (**Figure 1** and **Table 1**) comparative study of the attacks and security requirements in context to the existing and new fingerprint algorithms is to be done for proving diminution in error approximation. Standard attacks and security requirements are denial of service [7], DNS poisoning [8], forgery attack [9], man in the middle attack [10], forward secrecy [11], ping of death [12], mutual authentication [13], IP spoofing [14], parallel session [15], ping broadcast [16], password guessing [17], server spoofing [18], replay [15], session hijacking [19,20], mutual authentication [13], smart card loss [21], smurf [22], stolen verifier [21] and tear drop [23].

Table 1. Comparative study of attacks and security requirements on identity authentication parameters.

S. No	Security Requirements and Attacks	p	$f(g)$	$f(a)$	$f(m)$	$f(r)$
1	Denial of Service Attack [7]	Y	Y	Y	Y	Y
2	DNS Poisoning [8]	Y	N	N	N	N
3	Forgery Attack [9]	Y	Y	Y	Y	Y
4	Man in the Middle Attack [10]	Y	Y	Y	Y	N
5	Forward Secrecy [11]	Y	Y	N	Y	N
6	Ping of Death [12]	Y	Y	Y	Y	Y
7	Mutual Authentication [13]	N	Y	Y	Y	Y
8	IP Spoofing [14]	Y	Y	Y	Y	N
9	Parallel Session Attack [15]	Y	Y	Y	Y	Y
10	Ping Broadcast [16]	Y	Y	Y	Y	Y
11	Password Guessing Attack [17]	Y	N	N	N	N
12	Server Spoofing [18]	Y	Y	Y	Y	N
13	Replay Attack [15]	Y	Y	Y	Y	N
14	Session Hijacking [19,20]	Y	Y	Y	Y	Y
15	Smart Card Loss Attack [21]	N	N	N	N	N
16	Smurf Attack [22]	Y	Y	Y	Y	N
17	Stolen Verifier Attack [21]	Y	Y	Y	Y	N
18	Teardrop Attack [23]	Y	Y	Y	Y	Y
	Total Number of Attacks	16	15	14	15	8

Password = p

Fingerprint Extracted Value through Grid Hash Algorithm = $f(g)$

Fingerprint Extracted Value through Angle Hash Algorithm = $f(a)$

Fingerprint Extracted Value through Minimum Distance Hash Algorithm = $f(m)$

Fingerprint Extracted Value through RNA-FINNT Hash Algorithm = $f(r)$

Proof of Validation

Total Attacks = 18

$p = 16$, $f(g) = 15$, $f(a) = 14$,

$f(m) = 15$, $f(r) = 8$

Out of total 18, number of attacks possible on password is 16, fingerprint (extraction with Grid Hash Algorithm) is 15, fingerprint (extraction with Angle Hash Algorithm) is 14, fingerprint (extraction with Minimum Distance Hash Algorithm) is 15 and fingerprint (extraction with RNA-FINNT (Reduced Number of Angles Fingerprint) Hash Algorithm) is 8. This implies that only 8 attacks or security requirements are possible on IPAS (Ideal Password Authentication Scheme).

4. Proof of Diminution in Error Approximation

While validating the diminution in error approximation, RNA-FINNT is implemented in IPAS [24]. In RNA-FINNT number of minutiae points extracted is more than 12 so the overall reduction of error while extracting fingerprint is 4 [25]. On the basis of result of Section 3 (number of attacks) the steps of Section 2 are followed and below mentioned is the validation of the result. Below mentioned steps proved that as only 8 attacks are possible on RNA-FINNT so it result in diminution of error approximation.

Proposed Methodology for Validating Results

Step 1: Calculate the total number of Attacks and Security requirements possible on each Identity Authentication Parameter

$$p(e) = \left(t(p) \div n \times 100\right) = 16 \div 18 \times 100 = 88.8 = 89$$

$$f(g)(e) = \left(t\left(f(g)\right) \div n \times 100\right) = 15 \div 18 \times 100 = 83.3 = 83$$

$$f(a)(e) = \left(t\left(f(a)\right) \div n \times 100\right) = 14 \div 18 \times 100 = 77.7 = 78$$

$$f(m)(e) = \left(t\left(f(m)\right) \div n \times 100\right) = 15 \div 18 \times 100 = 83.3 = 83$$

$$f(r)(e) = \left(t\left(f(r)\right) \div n \times 100\right) = 8 \div 18 \times 100 = 44.4 = 44$$

Step 2: Calculate the total number of Attacks and Security requirements possible if *p* is assimilated with each Identity Authentication Parameter.

$$p\left(f\left(g\right)\right)=t\left(p\right)+t\left(f\left(g\right)\right)-\left(t\left(p\right)\cup t\left(f\left(g\right)\right)\right)=16+15-18=13$$

$$p\left(f\left(a\right)\right)=t\left(p\right)+t\left(f\left(a\right)\right)-\left(t\left(p\right)\cup t\left(f\left(a\right)\right)\right)=16+14-18=12$$

$$p\left(f\left(m\right)\right)=t\left(p\right)+t\left(f\left(m\right)\right)-\left(t\left(p\right)\cup t\left(f\left(m\right)\right)\right)=16+15-18=13$$

$$p\left(f\left(r\right)\right)=t\left(p\right)+t\left(f\left(r\right)\right)-\left(t\left(p\right)\cup t\left(f\left(r\right)\right)\right)=16+8-18=6$$

Step 3: Proof is derived from Step 2 that only 6 numbers of attacks are possible if p is assimilated with f (*r*) *i.e.* an Ideal Password Authentication Scheme.

Proof: *p* (*f* (*r*)) is best for Identity Authentication.

Step 4: Calculate the Total Error Percentage if *p* is assimilated with each Identity Authentication Parameter.

$$te\left(pg\right)=p\left(e\right)+f\left(g\right)\left(e\right)-n\left(p\left(f\left(g\right)\right)\right)=89+83-100=72$$

$$te\left(pa\right)=p\left(e\right)+f\left(a\right)\left(e\right)-n\left(p\left(f\left(a\right)\right)\right)=89+78-100=67$$

$$te\left(pm\right)=p\left(e\right)+f\left(m\right)\left(e\right)-n\left(p\left(f\left(m\right)\right)\right)=89+83-100=72$$

$$te\left(pr\right)=p\left(e\right)+f\left(r\right)\left(e\right)-n\left(p\left(f\left(r\right)\right)\right)=89+44-100=33$$

Step 5: Proof is derived from Step 4 that only 33% of error would be there if assimilation of *p* with *f*(*r*) is implemented *i.e.* Ideal Password Authentication Scheme.

When password is assimilated with fingerprint (extraction with Grid Hash Algorithm) or fingerprints (extraction with Angle Hash Algorithm) or fingerprints (extraction with Minimum Distance Hash Algorithm) or fingerprint (extraction with RNA-FINNT Hash Algorithm) the error approximation is 72, 67, 73 and 33 respectively. Result derived is that in IPAS number of minutiae points extracted are more than12 so the error percentage drastically gets reduced to 4 [25] and IPAS error approximation on the basis of attacks and security requirements over the transport layer is just 33.

5. Advanced Security Parameters of IPAS Results in FTLSP for Enhancement of Network Security

When only limited attacks or security requirements could be practiced by intruders over the network then data would remain more secure. These attacks hinder the data communication on the transport layer. RNA-FINNT resulted to generate an ideal password authentication scheme which has password assimilated with fingerprint. Extraction process with the help of RNA-FINNT has improved and this would enhance the security at the network layer. With IPAS intruder cannot impersonate a legal user by stealing the user's ID and PW from the password table whenever user accesses data from remote server because storage at the server is done with hash code values. Along with this mutual authentication is implemented in the multi server environment so that IP or Server Spoofing could be eliminated. The organization which would be using this IPAS should have Secured Socket Layer implemented in the Virtual Private Network because it enhances the security of a message transmission on the internet.

6. Conclusion

Conclusion is that implementation of ideal password authentication scheme results in the diminution of error approximation, fortifies the transport layer (Secured Socket Layer implemented in the Virtual Private Network of an organization) and enhances the network security.

REFERENCES

[1] K. Kaur and G. Geetha, "Survey for Generating an Ideal Password Authentication Scheme Which Results in Fortification of Transport Layer Security Protocol," *International Journal of Computer Science and Information Technologies*, Vol. 3, No. 2, 2012, pp. 3608-3614. http://www.ijcsit.com/ijcsit-v3issue2.php

[2] K. Kaur and G. Geetha, "Fortification of Transport Layer Security Protocol by Using Password and Fingerprint as Identity Authentication Parameters," *International Journal of Computer Applications*, Vol. 42, No. 6, 2012, pp. 36-42.

[3] K. Kaur and G. Geetha, "Fortification of Transport Layer Security Protocol with Hashed Fingerprint Identity Parameter," *International Journal of Computer Science Issues*, Vol. 9, No. 2, 2012, pp. 188-193.

[4] K. Kaur and G. Geetha, "Generating Multi Server Environment for implementation of Ideal Password Authentication Scheme," *International Journal of Advances in Computer Networks and Its Security*, Vol. 2, No. 3, 2012, pp. 2250-3757.

[5] S. Goyal and M. Goyal, "Generation of Hash Functions

from Fingerprint Scans," 2011.

[6] K. Kaur and G. Geetha, "Framework for Proving Fortification of TLSP with IPAS," *International Journal of Computer Engineering and Technology*, Vol. 3, No. 2, 2012, pp. 499-505.

[7] C. A. Huegen, "Network-Based Denial of Service Attacks". www.pentics.net/ denial-of-service/presentations/.../1998-0209_dos.pp...

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

[9] D. A. McGrew and S. R. Fluhrer, "Multiple Forgery Attacks against Message Authentication Codes," Cisco Systems, Inc., San Jose, 2005. eprint.iacr.org/2005/161.pdf

[10] A. Ornaghi and M. Valleri, "Man in the Middle Attacks Demos," BlackHat Conference, USA, 2003.

[11] D. G. Park, C. Boyd and S.-J. Moon, "Forward Secrecy and Its Application to Future Mobile Communications Security". www.dgpark6.com/ Down/pkc2000_FwdSec.pdf

[12] R. Bidou, "Ping of Death". www.iv2-technologies.com/ DOSAttacks.pdf

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

[14] C. Hofer and R. Wampfler, "IP Spoofing". rvs.unibe.ch/teaching /cn%20applets/IP_Spoofing/IP%20Spoofing.pdf

[15] A. Yasinsac and S. Goregaoker, "An Intrusion Detection System for Security Protocol Traffic," Department of Computer Science, Florida State University, Tallahassee, 1996, p. 12.

[16] "Ping Broadcast". en.wikipedia.org/wiki/Broadcast_radiation

[17] V. Goyal, V. Kumar, M. Singh, A. Abraham and S. Sanyal, "CompChall: Addressing Password Guessing Attacks," 2003. http://eprint.iacr.org /2004/136.pdf

[18] L. Seltzer, "Spoofing Server-Server Communication: How You Can Prevent It," 2009. www.verisign.com/ssl/ssl.../ssl.../whitepaper-ev-prevent-spoofing.pdf

[19] S. Kapoor, "Session Hijacking Exploiting TCP, UDP and HTTP Sessions". infosecwriters.com/text_resources/.../SKapoor_SessionHijacking.pdf

[20] R. Ramasamy and A. P. Muniyandi, "New Remote Mutual Authentication Scheme Using Smart Cards," *Transactions on Data Privacy*, Vol. 2, No. 2, 2009, pp. 141-152.

[21] H. Jeong, D. H. Won and S. Kim, "Weaknesses and Improvement of Secure Hash-Based Strong-Password Authentication Protocol," *Journal of Information Science and Engineering*, Vol. 26, No. 5, 2010, pp. 1845-1858.

[22] "Smurf Attack". http://en.wikipedia.org/wiki/Smurf_attack

[23] "Teardrop Attack Detection". https://www.daxnetworks.com/Dax/Products/Switch/DTS_T5C_24G_24GT.htm

[24] K. Kaur and G. Geetha, "Implementing RNA-FINNT in Ideal Password Authentication Scheme Results in Fortification of Transport Layer Security Protocol," *International Journal of Advances in Computer Science and Its Application*, Vol. 2, No. 3, 2012, pp. 201-205.

[25] K. Kaur and G. Geetha, "Validation of RNA-FINNT for Reduction in Error Percentage," *International Journal of Advances in Computer Science and Its Application*, Vol. 3, No. 1, 2013, pp. 22-26.