Enhanced Security Levels of BSPS in WLAN

Rajesh Duvvuru[1], Sunil Kr. Singh[3]
[1,3] Dept. of Computer Sc. & Engg.
National Institute of Technology
Jamshedpur, India

P. Jagadeeswara Rao[2]
Dept. of Geo-Engg.
AU College of Engineering
Andhra University
Visakhapatnam, India

Ankita Sinha[4]
[4]SME, Trainee
Amdocs
Gurgaon, INDIA

ABSTRACT

Wireless Network security is a major confront for the past two decades. Most importantly secure communications in WLAN is still a big challenge. This work majorly concentrated on designing the enhanced security levels for Enhanced Bio-cryptic Security- Aware Packet Scheduling-Algorithm (EBSPS). To enhance exist Bio-cryptic Security- Aware Packet Scheduling-Algorithm (BSPS), it is added with two more security levels by applying the bio-cryption on the facial and hand images. Simulations were performed using the Matlab and NS-2 and later EBSPS compared with the results of present BSPS. To achieve the good Quality-of-Service (QoS) in WLAN, it is replaced with the existing BSPS with novel EBPS. This EBSPS Algorithm besides assuring the finest performance in escalating the security level to the desirable WN by applying Bio-cryptographic methods in each security level. Finally, simulation result proves that proposal is performing superior than existing algorithm in terms of the quality of security.

General Terms

Wireless communications and Security.

Keywords

Bio-Cryptography, Quality-of-Security, Biometrics, Security Level, Enhanced Bio-cryptic Security- Aware Packet Scheduling-Algorithm, Bio-cryptic Security-Aware Packet Scheduling-Algorithm.

1. INTRODUCTION

Security in Wireless Local area Network (WLAN) became the one of the important research area of Information and Communication Technology because of its extensive range of usage. For example, recent implementations of WLANs range from little in-home networks to big, campus-sized ones to completely mobile networks on trains and airplanes [1]. In addition gaining the widespread popularity and usage of WLAN, it is less defiant to the network traffic, power consumption, guarantee ratio and most importantly security attacks [2]. Many algorithms have discussed the securities issues in WLAN, even existing solution are not enough to deal with the risks and mitigations involved in it [3].

Security services (X.800) for both connection and connection less were classified into five categories i.e. Authentication, Access Control, Data Confidentiality, Data Integrity and Non-repudiation. This work mainly concentrated on three security services, firstly Authentication, where the WN should be validated by Advanced Radius Authentication Server (ARAS) and access is permitted or denied by the ARAS and finally wireless data packet (WDP) is sent confidentially on to the network [3]. In authentication mechanism, it is added with additional novel feature called bio-cryptography, which leads to the stronger verification and validation mechanism in the WLAN. A biometric system is essentially a pattern-recognition system that identifies a person based on a feature vector derived from a particular behavioral or physiological distinctive that the person possesses [4]. Bio-cryptography refers to the application of cryptography to encrypt/decrypt the biometric data for its security. The extracted templates need to be secured through encryption using any of the existing encryption algorithms. It is important to protect the biometric identity/data of a person from unauthorized access because they are critical to one’s identity. Another important aspect of this paper is providing specific security level for the each and every WN through ARAS. Lastly packet scheduling of arrived packets to Network switch (NS) with a guarantee ratio [3].

The key contributions of this work comprise: (1) a analysis and requirements of security for wireless LAN; (2) a new Enhanced bio-cryptic security-aware packet scheduling; and (4) a new performance metric integrating both security and performance; (5) a simulator where the BSPS algorithm is implemented and evaluated. The rest of this paper is organized as follows. Section 2 discusses previous works in the area of Levels of Security, ARAS and Bio-Cryptography. Section 3 describes the system model and architecture. In section 4, it is represented with the performance evaluation of our algorithm. Finally, it is concluded the paper with future work discussed in Section 5.

2. RELATED WORK

Xiao Qin et introduced Security level concept. Their work describes the security aware packet scheduling (SPSS) concepts and they have compared their algorithm SPSS with the two baseline algorithms MIN and MAX. SPSS assigns dynamic security levels. MIN is assigned with minimum security level and MAX maintained with highest security level. Overall performance of SPSS is evaluated by combining of security level and guarantee ratio. SPSS performed better than two standard algorithms [5]. But the necessary security level distribution is not clear due to that reflects on the load on the network switch (LNS).

Later, it is was resolved by introduced Advanced Security-Aware Packet Scheduling (ASPS) for the desired WN. In this scheme, security is assigned automatically which is necessary for the WN with advanced radius authentication server (ARAS). Without hampering the rest of parameters like level of security and guarantee ratio, ASPS reduced the consignment on LNS [3].

Next it was concentrated on strengthen the authentication process by recommending Bio-crypted Security-Aware Packet

Scheduling-Algorithm (BSPS). This work incorporated with the bio-encryption techniques in the security levels. BSPS performed better than ASPS in terms of Quality-of-security (QoS). But its limits only to thumb and iris usage [6]. One of the important applications of biometric is secure bank transaction. S.T. Bhosale and B.S.Sawant explained the concept of card less automatic teller machine (ATM) by replacing the biometrics for valid authentication, which yield in high validation of the user [7]. Li Bin et has conducted survey on different edge detection operators like Roberts, sobel, prewitt and Canny. In authors work it is concluded that Canny operator detects better when noise is there in weak edges. [8]. Sulakshana Bhariya et described the importance of the bio-cryptography and discussed the Improving the Security of Image Encryption and Decryption [9]. Presently the system for designed and simulated for different security levels for authentication process in WLAN via Advanced Radius Server Authentication (ARSA) [3].

3 ENHANCED BIOCRYPTED SECURITY-AWARE PACKET SCHEDULING ALGORITHM (EBSPS)

3.1 Assumptions and Notations

In EBSPS it is assumed that there are fixed number of security levels in a network. In our work we have assumed five security levels.

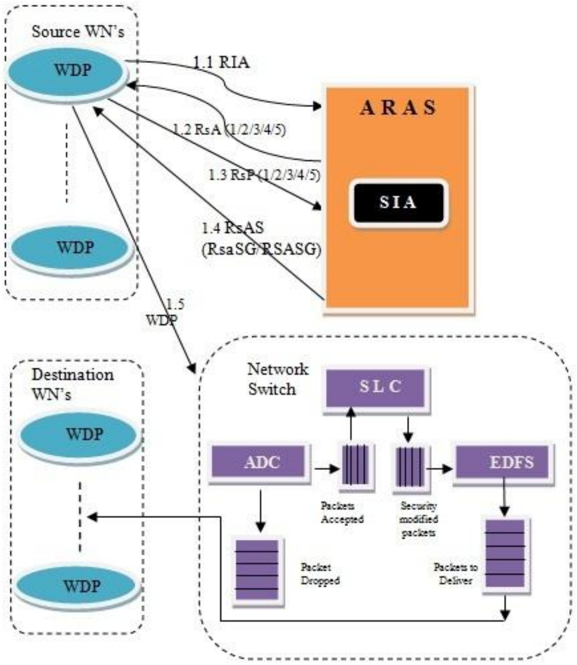

Figure 1: Schematic Diagram of Network System

3.1.1 Request IP address (RIA) packets

Initial packet sent from WN to ARAS it contains single field (IP Address of WN).

3.1.2 Response Authentication (RsA) packets

ARAS will responds to the RIA and dynamically issue RsA according to RIA. It present for each of these levels, each with different fields.

- RsA1(Response for Authentication for level 1) is a tuple of two fields (1,pass). 1 specifies security level 1 and contains a textual password.
- RsA2(Response for Authentication for level 2) is a tuple of three fields (2,pass,thumb).
- RsA3(Response for Authentication for level 3) is a tuple of four fields (3,pass,thumb,iris).
- RsA4(Response for Authentication for level 4) is a tuple of four fields (4,pass,thumb,iris,handprint).
- RsA5(Response for Authentication for level 5) is a tuple of four fields (5,pass,thumb,iris,handprint, facial).

3.1.3 Request Authentication (RqA)

RsA1 or RsA2 or RsA3 or RsA4 or RsA5 receiving from ARAS, WN will respond and provide the credentials accordingly and sent RqA to ARAS. Three different RqA packets have to be present for each of these levels, each with different fields.

3.1.4 Response Authentication Status (RsAS)

Finally ARAS will check the RqA and grant or reject the access to WN. These packets are designated 2 types:

- RsASG(Response for Authentication: Granted), and
- RsASD(Response for Authentication: Denied).

3.2 The Packet Model

WDP is represented with a set of fields (ATi,PTi,SLi,Di)[8]. Here SLi and Di is represented with the security level and deadline of the packet i. ATi and PTi denotes arrival and processing time of packet i.

Equation (Eq)-1 specifies the formula for the calculation of deadline.

$$DLi >= ITi– FTi \qquad (1)$$

To compute the ARAS time, we make use of equation-6

$$ARASTATi = ARASTRqAi + ARASTRsAi \qquad (2)$$

Where ARASTATi is the total request and respose time is the communication between by the ARSA of packet i, to assign and verify the security level, ARASTRqAi is represented as Total requests time by the ARAS and ARASTRsAi is represented as Total response time by the ARAS. Equation-2 has discussed clearly in our previous work[6].

Thus, is the total authentication time (TATi) is expressed as

$$TATi = WNTATi + ARASTATi \qquad (3)$$

3.3 The EBSPS algorithm

As discussed earlier the EBSPS algorithm strengthens authentication process of BSPS algorithm. The working procedure of the EBSPS is same as of BSPS algorithm. The BSPS algorithm explained in the preceding work [6].

4 SIMULATIONS AND RESULTS

4.1 Bio-cryptography Simulations using Matlab

Bio-cryptography fallows two important steps. Initially it is applied the canny edge operator for feature extraction on biometric images and next we have encrypted the extracted features images by applying the RSA algorithm.

4.1.1 Canny edge detection (CED) of Biometric images

CED is applied to the simple pattern extraction and not minutiae. In this work, threshold value is not considered. It is used an inbuilt function for the feature extraction using CED. i.e., edge(fin_his_eq,'canny'); from Matlab. By using edge functions it is found that the edges of the different biometric image like thumb, iris, palm and facial.

4.1.2 RSA Algorithm on feature exaction biometric images

Even RSA algorithm is older, but still RSA algorithm is an strong cryptographic algorithm. In this algorithm we have taken two distinct prime numbers p and q randomly, then computed the prime numbers p and q for the key generation. [11].Given m, can recover the original message M by reversing the padding scheme. Where, Cd using the pre-computed values. In Matlab image tool kit we applied the above equation used .i.e. cipher(j,k)= mod(M(j,k)^e,n); where M is the feature extracted biometric image. Using imread(), we read the image M (Image is already stored in WN).

4.2 Result and Analysis of Cyrpto-biometrics

As it is assigned with the different bio-cryptic security levels that were successfully encrypted using RSA algorithm. Figure 2 clearly gives the security assignment.

Figure 2 clearly explaining the security level 2 encryption processes with text based and thumb print. Firstly it is designed to take the plain text and converted equally to numeric form. Next it is considered the thumb print and submitted for the edge detection. Using Canny edge operator edges are detected in Matlab.

Later it is submitted to the numerical plain text and edge detected thumb print for encryption with RSA algorithm. The finally result, which was RsA2 packet, which contains cipher text and bio-cryptic thumb print. Later RsA2 will be sent from WN to ARAS for authentication. As it is taken plain text-'Password Text', then it is applied to the same procedure, i.e., SL-2. But the size of the RsA3 packet is bigger than RsA2 at the same time the security is stronger than RsA2. Simply, security of packet is proportionate to the packet size.

Once the RsA2 is received from WN, ARAS will admit the packet and check with the database. If the packet data is available with the database, it will issues RsASG or RsASD packets accordingly to WN.

Figure 3 describes the encryption procedure of the security level 3. As it is discussed earlier, SL3 has to use RsA3 packet for authentication. In addition to the RsA2, RsA3 is added with one more security layer in the form of Iris. In encryption process using RSA algorithm, we have used the common two primary numbers p and q.

All images and text will be encrypted with only one primary number. In figure 4, one more security level is added in the form of palm print to present RsA3.

The RsA4 represents the SL4, which comprises of the authenticated items like text based password, thumb, iris and palm prints. Palm print image segmentation is performed with the help of Region-of –Interest (ROI) segmentation process [13]. Instead of taking whole palm print it is considered only segmented part. Now, it is easy to recognize the pal more precisely.

We have taken different segments of single palm print for ease of operate. Once it is segmented the palm image, it finds the edges for that palm by applying Canny operator. Later it encrypts the palm segment and finally cryptic palm image will send to ARAS for authentication.

Figure 5 is designed the RsA5 packet. It comprises set of cryptic text password, thumb print, iris image, pal print and facial image. In facial encryption we have collected diverse angles of facial photo of human and applied for the edge detection and done encryption on the facial edge photo by using RSA algorithm.

Figure 6 represents comparison of EBSPS with BSPS in terms of security level. We found EBSPS has five security levels, whereas BSPS contains only three security levels. Even security level of EBSPS is very stronger; it contains its own limitation with the authentication time, and packet size of the RsA packet.

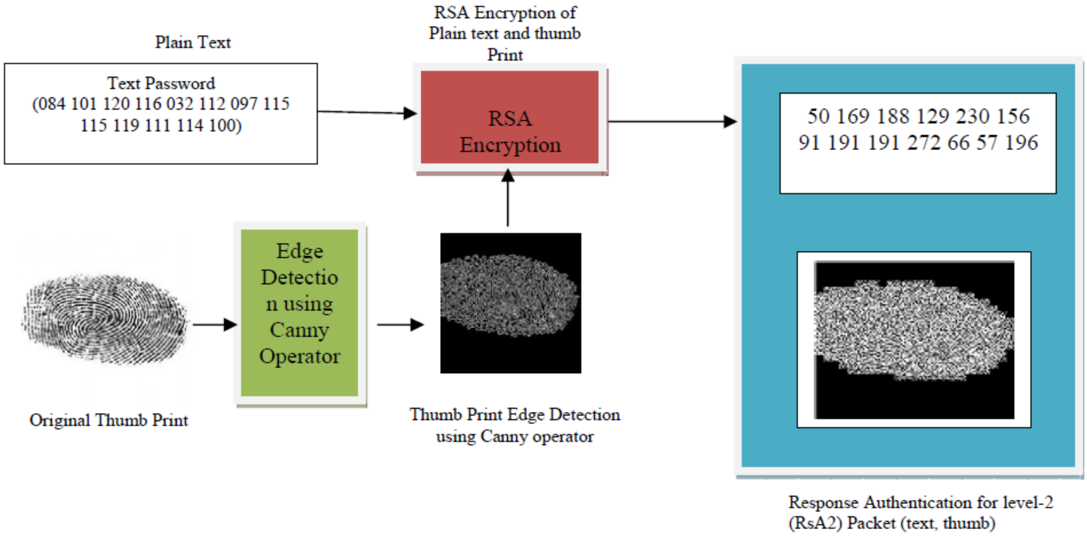
Plain Text
Text Password
(084 101 120 116 032 112 097 115 115 119 111 114 100)
RSA Encryption of Plain text and thumb Print
RSA Encryption
50 169 188 129 230 156 91 191 191 272 66 57 196
Edge Detection using Canny Operator
Original Thumb Print
Thumb Print Edge Detection using Canny operator
Response Authentication for level-2 (RsA2) Packet (text, thumb)

Fig 2: Encryption procedure for the security level-2

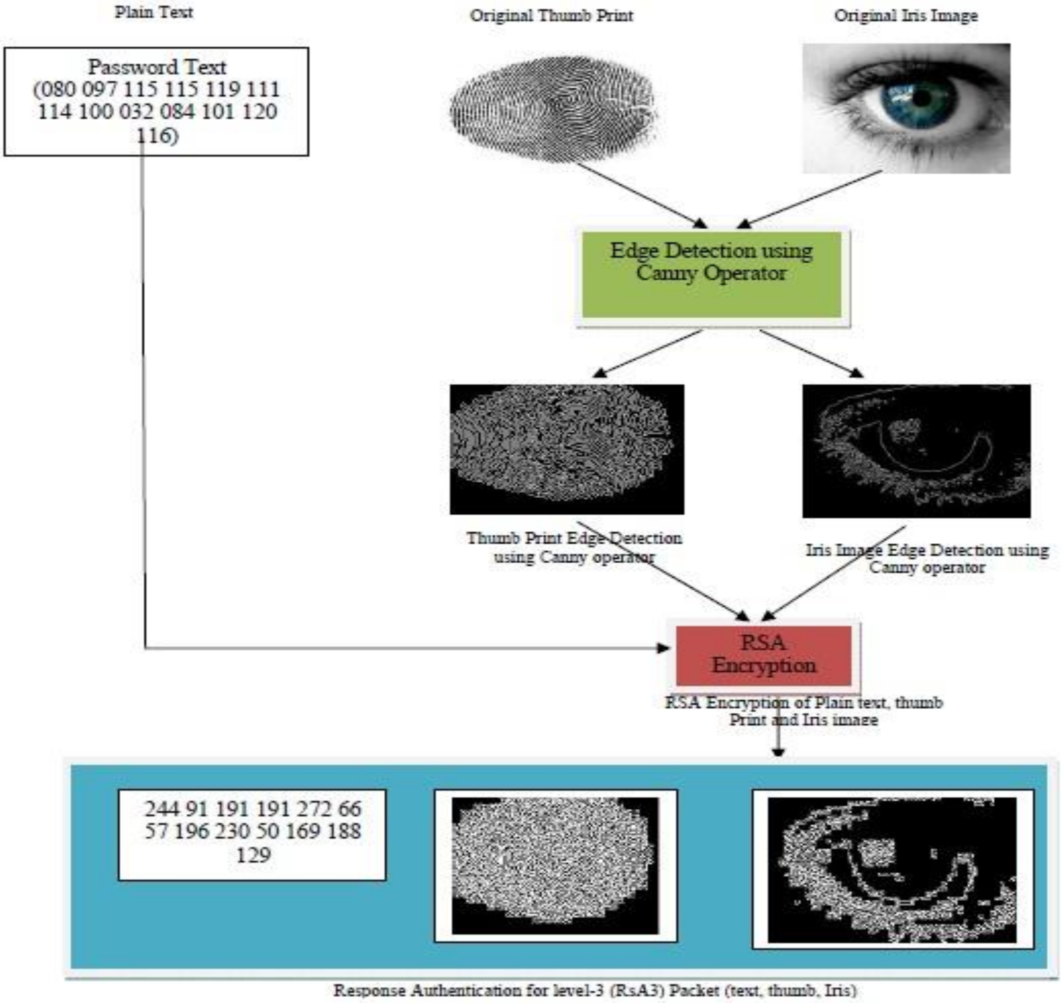
Plain Text
Original Thumb Print
Original Iris Image
Password Text
(080 097 115 115 119 111 114 100 032 084 101 120 116)
Edge Detection using Canny Operator
Thumb Print Edge Detection using Canny operator
Iris Image Edge Detection using Canny operator
RSA Encryption
RSA Encryption of Plain text, thumb Print and Iris image
244 91 191 191 272 66 57 196 230 50 169 188 129
Response Authentication for level-3 (RsA3) Packet (text, thumb, Iris)

Fig 3: Encryption procedure for the security level-3

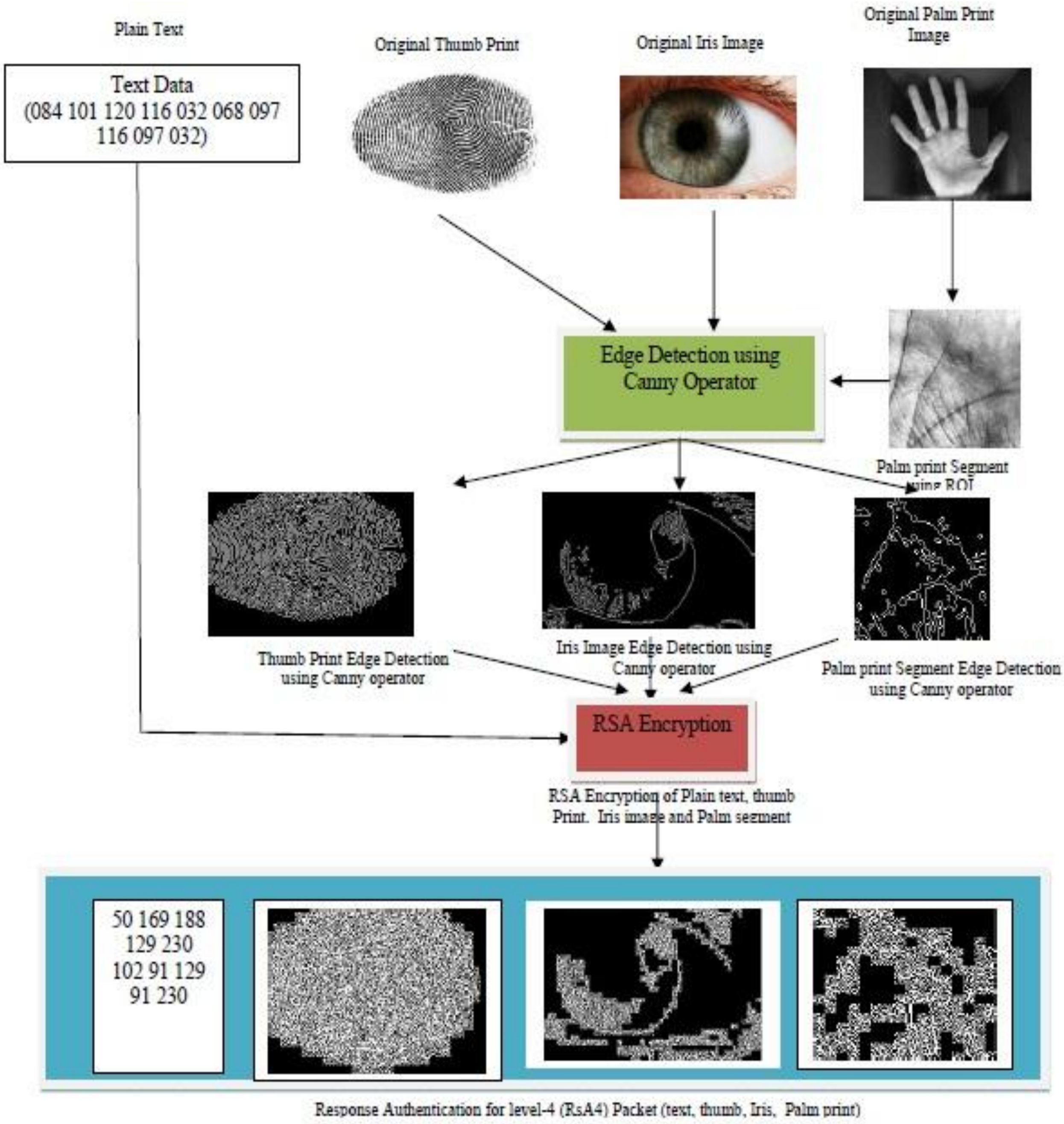
Plain Text
Text Data
(084 101 120 116 032 068 097 116 097 032)
Original Thumb Print
Original Iris Image
Original Palm Print Image
Edge Detection using Canny Operator
Palm print Segment using ROI
Thumb Print Edge Detection using Canny operator
Iris Image Edge Detection using Canny operator
Palm print Segment Edge Detection using Canny operator
RSA Encryption
RSA Encryption of Plain text, thumb Print. Iris image and Palm segment
50 169 188 129 230 102 91 129 91 230
Response Authentication for level-4 (RsA4) Packet (text, thumb, Iris, Palm print)

Fig 5: Encryption procedure for the security level-4

4.3 Performance evaluation

The overall performance of EBSPS is better than BSPS because enhancement in the security level. The overall performance is articulated in our previous work [6]. Performance measurement is based on mainly five parameters they are Guarantee ratio (GR), level of security (LS), overall performance (OP), Load-on-Switch (LOS) and total authentication time (TATi). Overall performance can be designed by following Eq-4:

OP= (GR * LS) + LOS + TATi ---- (4)

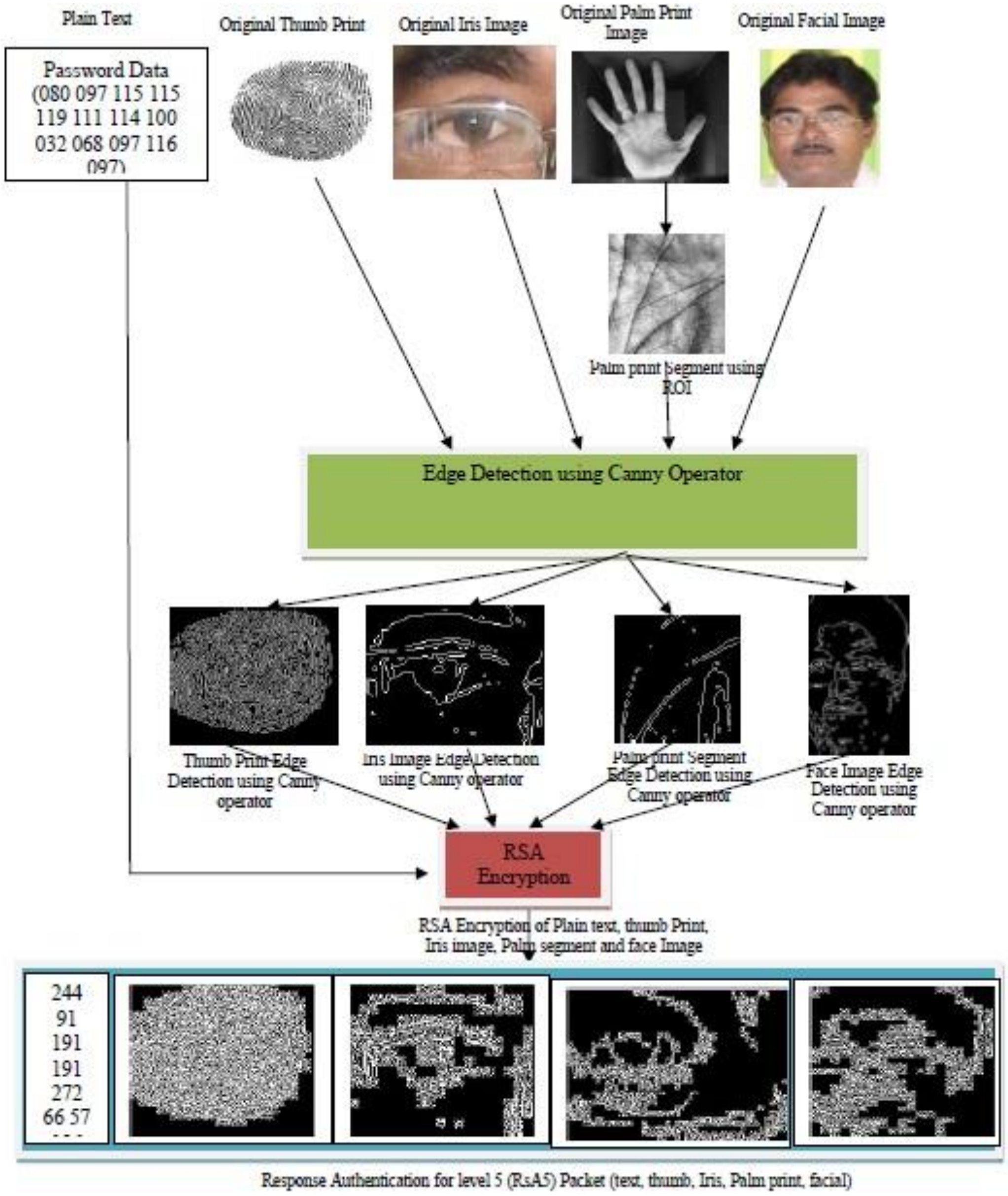
Plain Text
Password Data
(080 097 115 115
119 111 114 100
032 068 097 116
097)
Original Thumb Print
Original Iris Image
Original Palm Print Image
Original Facial Image
Palm print Segment using ROI
Edge Detection using Canny Operator
Thumb Print Edge Detection using Canny operator
Iris Image Edge Detection using Canny operator
Palm print Segment Edge Detection using Canny operator
Face Image Edge Detection using Canny operator
RSA Encryption
RSA Encryption of Plain text, thumb Print, Iris image, Palm segment and face Image
244
91
191
191
272
66 57
Response Authentication for level 5 (RsA5) Packet (text, thumb, Iris, Palm print, facial)

Fig 5: Encryption procedure for the security level-5

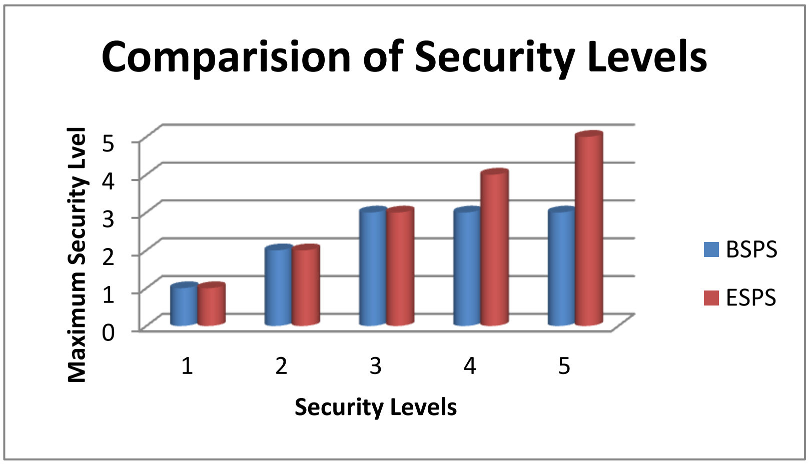

Fig 6: Comparison of Security levels EBSPS and BSPS

Table 1 compares the different security levels in EBSPS. In SL1 is designated as lower and SL5 as highest. Finally we have achieved 40% more security that BSPS.

Table 1. Statics for the EBSPS

	Text	Thumb	Iris	Palm	Face
SL1	Yes	No	No	No	No
SL2	Yes	Yes	No	No	No
SL3	Yes	Yes	Yes	No	No
SL4	Yes	Yes	Yes	Yes	No
SL5	Yes	Yes	Yes	Yes	Yes

5 CONCLUSION

In proposed approach it enhances the security in BSPS by introducing the two more bio-encrypted approaches i,e. Later it was focused mainly on enrichment of level of security in wlan. In EBSPS authentication, to access the wlan with the permission of ARAS we improved security level from SL3 to SL5. Simulations were performed to encrypt text, thumb, Iris, palm and facial images using the MATLAB. We compared proposed EBSPS with BSPS in terms of security. It is observed that, 40% improvement in the security level of EBSPS compared to BSPS. The results state that without hampering LS, GR and LOS, the overall performance of the EBSPS is good. But EBSPS has its own limitation with increase in the size of RsA packet in accordance with the SL.

6 REFERENCES

[1] http://www.ieee-globecom.org/2012/private/T10F.pdf

[2] Anastasios N. Bikos, Nicolas Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks," IEEE Security & Privacy, vol. 11, no. 2, pp. 55-62, March-April 2013, doi:10.1109/MSP.2012.136.

[3] Rajesh Duvvuru, Sunil Kumar Singh, G. Narasimha Rao, Ashok Kote4, B.Bala Krishna and M. Vijaya Raju, “Scheme for Assigning Security Automatically for Real-Time Wireless Nodes via ARSA,” In Proc. Of QSHINE 2013, LNICST 115,Springer, pp. 185–196, January, 2013.

[4] Mohamad El-Abed, et, “Evaluation of biometric systems: a study of users' acceptance and satisfaction,” International Journal of Biometrics , Volume 4, Issue 3, pp. 265-290, July 2013.

[5] Xiao Qin, et, “Improving Security of Real-Time Wireless Networks Through Packet Scheduling,” *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 9, pp.3273-3279, September 2008.*

[6] Rajesh Duvvuru, P. Jagadeeswara Rao and Sunil Kumar Singh, “Improvizing Security levels in WLAN via Novel BSPS”, In Proc. Of IEEE International conference on Emerging Trends in Communication, Control, Signal Processing & Computer Applications 2013(C2SPCA-2013), pp. 71, October 10-11, 2013

[7] S.T. Bhosale and B.S.Sawant, “ Security in e-banking via card less biometric atms,” International Journal of Advanced Technology & Engineering Research, Volume 2, Issue 4, July 2012

[8] Li Bin and Mehdi Samiei yeganeh, “Comparison for Image Edge Detection Algorithms,” IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278 - 0661 Volume 2, Issue 6, pp. 01-04, (July-Aug. 2012),

[9] Sulakshana Bhariya, Guide Jagveer, “A Bio-Cryptography Approach for Improving the Security of Image Encryption and Decryption,” International Journal of Technology, Vol. 2: Issue 1, pp. 01-04, 2012.

[10] Bing Wang, ShaoSheng Fan, "An Improved CANNY Edge Detection Algorithm," Second International Workshop on Computer Science and Engineering, 2009,IEEE, iwcse, vol. 1, pp.497-500, 2009

[11] Samoud Ali and Cherif Adnen, “RSA algorithm implementation for ciphering medical imaging,” International Journal of Computer and Electronics Research ,Volume 1, Issue 2, August 2012 .

[12] Christian Rathgeb and Andreas Uhl, “A survey on biometric cryptosystems and cancelable biometrics”, Journal on Information Security 2011, Springer, pp.1-25, 2011.

[13] Kai-Wen Chuang, Chen- Chung Liu, Sheng-Wen Zheng, “A Region-of-Interest Segmentation Algorithm for Palmprint Images,” In Proc. of The 29th Workshop on Combinatorial Mathematics and Computation Theory”, pp. 96-102, April, 2012.