# Enhanced Merged Security Levels of BSPS in WLAN

Avala Ramesh
Dept. of Computer Sc. & Systems Engg.
Andhra University College of Engineering,
Andhra University,
Visakhapatnam, India

S. Pallam Setty
Dept. of Computer Sc. & Systems Engg.
Andhra University College of Engineering,
Andhra University,
Visakhapatnam, India

## ABSTRACT

Security and quality of service are two major problems in wireless communications. This work concentrated on improving the security levels for Enhanced Bio-cryptic Security- Aware Packet Scheduling-Algorithm (EBSPS) and also the fast communication between Wireless Node (WN) and Advanced Radius authentication server (ARAS). This paper introduces a novel Enhanced Merged Bio-cryptic Security- Aware Packet Scheduling-Algorithm (EMBSPS). Simulations were conducted using the Matlab and EMBSPS is compared with the results of present EBSPS and BSPS. To accomplish better Quality-of-Service (QoS) in WLAN, it is substituted with the existing EBSPS with novel EMBSPS. This EMBSPS Algorithm assures the finest concert in improving the security levels and speeds up the authentication process. Lastly, simulation result proves that proposed model is performing finer than the present algorithm in terms of the quality of service.

## General Terms

Wireless communications and Security

## Keywords

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

## 1. INTRODUCTION

Quality of service in terms of quality of security and fast authentication process in Wireless Local area Network (WLAN) are two major problems arena of Information and Communication Technology because of its wide usages. For instance, recent implementations of WLANs range from little in-home networks to big campus-sized [1]. In addition gaining the pervasive usage and reputation of WLAN, it is less attenuated to the network congestion, fast transmission, power consumption, reliable communication and most importantly security [2]. In literature of WLAN 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]. According to the survey report 2013 on WLAN security in Kaohsiung metropolitan areas by the University of Kaohsiung. It is clearly observed that 56.24 % are the simple passwords and easily cracked by malicious behaviors [4]. X.800 Security services architecture was classified into five categories for both connection and connection less i.e. Data Confidentiality, Non-repudiation, Authentication, Access Control and Data Integrity. This work mainly concentrated on fast authentication mechanism in WLAN. In the network model Wireless Node (Node) can able to access the network after authentication. This authentication process will be permitted or denied by the Advanced Radius Authentication Server (ARAS) [3]. In authentication process, bio-cryptography will give the better solution than normal text or biometric based authentication. Bio-Cryptography strengthens the verification and validation process in the WLAN. Presently, the majority security applications are developed based on token or knowledge. There are primary flaws with these two types of security methods. Tokens like key or cards can be mislaid or stolen. Similarly, knowledge such as PINs and passwords can also be simply forgotten or guessed using psychological manipulation of people into performing action secret information Bio-cryptography is a branch of science and technology which combines biometrics with cryptography. It inherits the advantages of both and offer a strong means to protect against WLAN security attacks [4]. Another important aspect of this paper is each and every security level is well defined for every WN through ARAS. Finally, scheduling packet will arrive to Network switch (NS) with a packet delivery ratio [3].

The important contributions of this work consist of: (1) a analysis and requirements of merging of biometric images for wireless LAN; (2) a innovative Enhanced Merged bio-cryptic security-aware packet scheduling; (4) a new performance analysis of data packet fast transmission and performance; (5) a simulator where the EMBSPS algorithm is implemented and evaluated. The rest of the paper is organized in the fallowing way. Section 2 discusses previous works in the area of Bio-Cryptography Security Levels and ARAS. Section 3 describes the network system prototype 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 WORKS

Xiao Qin and team has came up with an idea security level. Their work explains the security aware packet scheduling (SPSS) concepts and the results were compared with the two baseline algorithms MAX and MIN. Where SPSS assigns security levels dynamically, MAX maintained with highest security level and MIN is assigned with minimum security level. Overall SPSS performs better than MAX and MIN in terms of security level and guarantee ratio [5]. But require amount of security level assignment is confusing due to load on the network switch (LNS).

Next, Rajesh Duvvuru et., has resolved security level assignment flaw was resolved by introduced Advanced Security-Aware Packet Scheduling (ASPS) for the desired WN. In this scheme, without hampering the rest of parameters like level of security and guarantee ratio, ASPS reduced the consignment on LNS using advanced radius authentication server (ARAS). It is observed that overall performance of ASPS is better than SPSS [3].

Later Rajesh Duvvuru and team introduced Bio-crypted Security-Aware Packet Scheduling-Algorithm (BSPS) is introduced in order to strengthen the authentication mechanism. This work integrated with the bio-encryption techniques for the security levels. The Quality-of-security (QoS) is good in BSPS rather than ASPS. But BSPS deals only with thumb and iris [6].

Successively Rajesh Duvvuru et., has extended the version of BSPS, which is Enhanced Bio-crypted Security-Aware Packet Scheduling-Algorithm (EBSPS) is majorly concentrated only improvising the security level by adding two more security level. These two levels contain two more biometric encryption of palm and facial [7]. Secure bank transactions is the best example for the Biometric security. S.T. Bhosale et., explained card less automatic teller machine (ATM) by replacing the biometrics for authorization and authentication of the user [8]. A survey report was presented by Li Bin and team on diverse edge detection operators like Canny, Roberts, prewitt and sobel. In authors work it states that Canny operator detects weak edges better [9]. In our previous work, it is observed that, canny edge technique images will provide the stronger security than Laplacian and Zero cross edge technique images [21]. Sulakshana Bhariya et.al., described the importance of the bio-cryptography and discussed the Improving the Security of Image Encryption and Decryption procedure[10]. A survey report on biometric system were given by Christian Rathgeb et.al., [18]. Currently the system for intended and simulated for different security levels for authentication mechanism in WLAN through Advanced Radius Server Authentication (ARSA) [7].

# 3. ENHANCED MERGED BIOCRYPTICs SECURITY-AWARE PACKET SCHEDULING ALGORITHM (EMBSPS)

## 3.1 Assumptions and Notations

In EMBSPS it is assumed with a fixed number of security levels in a network. In addition to this it is also assumed five security levels.

### *3.1.1 Request IP address (RqIA) packets*

In Startup of WN, it will start searching for network. Then of request IP address packet was sent from WN to ARAS it contains set of field (IP Address of WN, NSIP). Where NSIP represents IP address of destination Network switch.

### *3.1.2 Response Authentication (RsA) packets*

According to the RqIA packet received by the ARAS, the ARAS verifies whether IP address is valid or not. RsA packets are of two types. The first one is RsANV, if the IP is not valid, ARAS issues RsANV packet with (Not valid message, IPWN). If RqIA is valid, then ARAS will issue the RsAV packet with (SL, text-pass, Biometric1 (optional), Bioemetric2 (optional), Bioemetric3 (optional), Bioemetric4 (optional), Bioemetric5 (optional), IPWN) or RsA packet. It present for each of these levels, each with different fields.

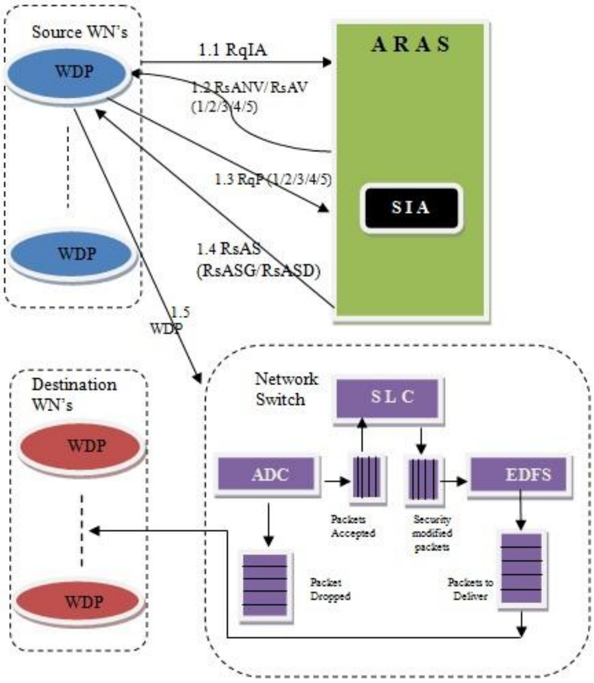


**Figure 1: Schematic Model of Network System**

- RsAV1 (Response for Authentication for security level 1) is a tuple of two fields (1, password, WNIP). 1 specifies security level 1 and contains a textual password.
- RsAV2 (Response for Authentication for security level 2) is a tuple of three fields (2, password, thumb, WNIP). 2 specifies security level 2 and also contains a textual password and Biometric1 (thumb).
- RsAV3 (Response for Authentication for security level 3) is a tuple of four fields (3, password, thumb, iris). 3 specifies security level 3 and it comprises of a textual password and added with Biometric1and 2 (thumb and iris).
- RsAV4 (Response for Authentication for security level 4) is a tuple of four fields (4, pass, thumb, iris, Palm print). 4 specifies security level 4 and it comprises of a textual password and includes with Biometric1, 2 and 3 (thumb, iris, thumb print).
- RsAV5 (Response for Authentication for security level 5) is a tuple of four fields (5, pass, thumb, iris, Palm print, facial).5 specifies security level 5 and it includes of a textual password and comprises with Biometric1, 2, 3 and 4 (thumb, iris, Palm print, facial).

Here WNIP represents with the IP address of the WN. It is a common field in both RsAV and RsANV.

### *3.1.3 Request Authentication (RqA)*

ARAS will sent RsAV1 or RsAV2 or RsAV3 or RsAV4 or RsAV5 to WN, according to the importance of the WN user. Then WN responds and afford the credentials accordingly and sent RqA to ARAS. Further RqA is also bifurcated into five types in accordance with the RsAV's. ARASIP is the common field in packet; it represents the IP address of ARAS.

- RqA1 (Request for Authentication for security level 1) is a tuple of two fields (1, password, ARASIP). 1 specifies security level 1 and cryptic password.

- RqA2 (Request for Authentication for security level 2) is a tuple of three fields (2, password, thumb, ARASIP). 2 specifies security level 2 and also contains a cryptic password and Bio-cryptic (thumb image).
- RqA3 (Request for Authentication for security level 3) is a tuple of four fields (3, password, Merge {thumb, iris}, ARASIP). 3 specifies security level 3 and it comprises of a textual Cryptic password and added with Merge-Bio-Cryptic image (thumb and iris).
- RqA4 (Request for Authentication for security level 4) is a tuple of four fields (4, pass, merge {thumb, iris}, Palm print, ARASIP). 4 specifies security level 4 and it comprises of a textual cryptic password and includes with Merge-Bio-Cryptic image (thumb and iris) and Bio-Cryptic Palm print image.
- RqA5 (Request for Authentication for security level 5) is a tuple of four fields (5, pass, Merge {thumb, iris}, Merge {Palm print, facial}, ARASIP).4 specifies security level 5 and it includes of a textual password and comprises with Biometric1, 2, 3 and 4 (thumb, iris, Palm print, facial).

### *3.1.4 Response Authentication Status (RsAS)*

Lastly ARAS will validate the RqA's packet and decrypt the images and textual password. After decryption process, ARAS will verify it with its database. Later, it will 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

Wireless data packet (WDP) is comprises with a set of fields (ATi,PTi,SLi,Di)[8]. Where, PTi and ATi represents processing and arrival time of packet i and SLi and Di is denotes as security level and deadline of the packet i

Equation (Eq)-1 shows the calculation of deadline.

Di >= ITi– FTi (1)

Where ITi is the initial time of the packet send and FTi is the packet received at NS.

Where ARASTATi is the total request and response time is the communication between by the ARSA of packet i, to assign and verify the security level and WNTATi represents total time consumed at WN.

Computation time at WN can be defined as:

CTWi = TEDi +TRSAEi ---- (2)

Where TED is computation time for edge detection and TRSAE is computation for RSA encryption at WN. Also, Computation time at ARAS (CTARAS) is calculated as:

CTARASi = TRSADi +TPMi --- (3)

Here, TARSAD is computation time to decrypt the biometric samples at ARAS and TPM represents computation time for pattern matching in the database. Then computation time of TARASD is similar to TED and TPM is assumed as with the Radom probability distribution.

CT, can be obtained by adding the equations 2 and 3.

CTi = CTWi + CTARASi --- (4)

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

TATi = WNTATi + ARASTATi ----- (5)

Equation-5 has discussed clearly in the literature of Bio-cryptography [6].

## 3.3 The EMBSPS Algorithm

As discussed earlier the EMBSPS algorithm strengthens authentication process and shortens the authentication time of BSPS algorithm. In EMBSPS we are shortening the authentication time by merging the two biometric images into a single image. Merging of images depends upon the SL. For instance, it requires 50% left portion from thumb image and 50% right portion from iris image to merge to merge thumb-iris image. Figure 2 explains clearly the merging procedure. After merging we fallow the complete procedure of EBSPS. The rest of the working procedure of the EMBSPS is same as of EBSPS algorithm. The EBSPS algorithm explained in the preceding work [7] and EBSPS will follow the algorithm of BSPS [6]. Figure 1 demonstrates the complete procedure of the Network System.

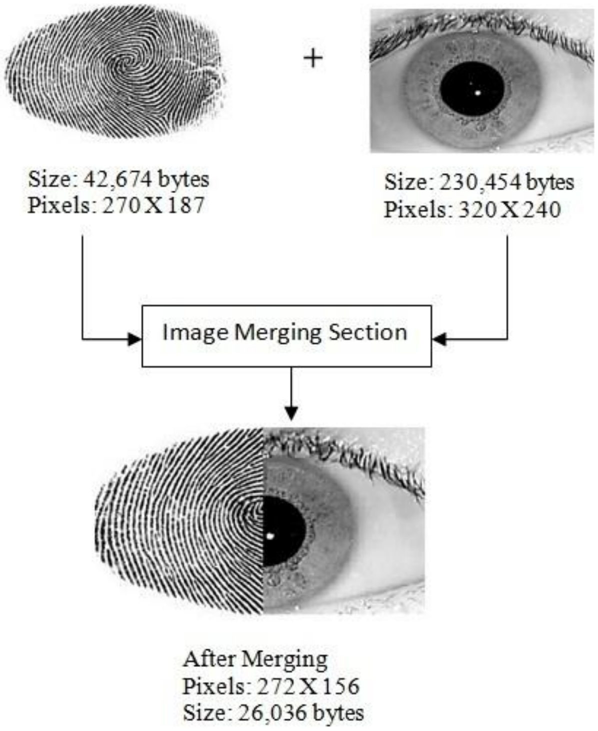


**Figure 2: Equal half Merging (50%-50%) of Thumb print and Iris biometric images.**

# 4. SIMULATIONS AND RESULTS

## 4.1 Merged-Bio-cryptography Simulations using Matlab

Merged-Bio-cryptography fallows three important steps. Initially, any of two biometric images were going merged. Secondly, canny edge operator is applied for feature extraction on biometric images and lastly encryption process is applied features extracted merged-biometric images by using RSA algorithm.

### *4.1.1 Merging of biometric images*

In this work, the very step was merging of images. Biometric images are going to made two equal half. For instance, suppose if merging of palm print-facial is taking place. We will take 50% left portion of palm print and 50% right portion of facial. Then these two equal halves are going to merge together. Three main advantages are there by using merging. They are:

- Size of the RqA will get reduced abruptly, which reflects in the speedy authentication process.
- Feature extraction will be applicable on fewer images and due to this edge detection time is minimized
- Encryption and decryption time also will get reduced, due to merging.

### *4.1.2 Edge detection (ED) of Merged-Biometric images*

Edge detection is applied on to the pattern extraction and not minutiae. For simulation, it is considered inbuilt function for the feature extraction using Canny ED. i.e., edge(fin_his_eq,'canny'); from Matlab. By finding the edges for different merged-biometric images like thumb-iris and palm print-facial [11].

### *4.1.3 RSA Algorithm on feature extraction Merged-Biometric images*

In the literature of image encryption, there are different encryption schemes that are available like RSA algorithm, Elliptic curve cryptography (ECC) and Chaos-Based [19] [20]; We chosen, RSA algorithm for encrypted the merged-biometric images for easy implementation. In this algorithm we considered two distinct prime numbers p and q randomly and then computed the prime numbers p and q for the key generation. [12].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).

### *4.1.4 Simulation of EMBSPS*

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. By default, the IP address of ARAS is assumed as 127.1.1.11. Where the address is in the form of IPV4 and size is of 4 bytes.

Finger print, Iris and Palm print data samples were collected from the Biometrics Research Laboratory, Indian institute of Technology Delhi, IIIT Delhi [13][14][15]. Also Facial image data samples were gathered from the University of Massachusetts Amherrest , United States of America [16].

Security level 1 and 2 results same effect in EMBSPS, EBSPS and BSPS algorithm. So we present the simulation of Security Level 3, which will perform better than EBSPS and BSPS. In Figure 8, we considered the textual password, thumb print and Iris. First we will merge the thumbprint and iris images. Later edge detection is going to perform using canny operator. Then resulted merged-biometric edge image and textual password is subjected to RSA Encryption mechanism. Finally the resultant encrypted textual password and merged-bio-crypt image will be sent to the ARAS in the form of RqA3 packet for the verification and validation. At the destination side ARAS will decrypt the text password and merged-bio-crypt image and verify with its database. If the data is matched, RsASG else RsASD packets will be sent back to WN.

Next, the security level 4 was discussed precisely in figure 9. Here we had gone with the procedure of SL-3. But at this level one more biometric is going to be added i.e., palm print. In Palm print, image segmentation was done with the help of Region-of –Interest (ROI) segmentation process [17]. Palm segmentation is more efficient and easy to recognize the palm more precisely. At this SL, definitely EMBSPS performs better than EBSPS and BSPS. Figure 6 shows the detailed difference between EMBSPS, EBSPS and BSPS.

Finally, the simulation of security level 5 was shown in figure 10. Here, it is considered by default text password and remaining biometric options. Biometric utilities like thumb, Iris, Palm print and facial were used. Here, Biometric images were made into two groups randomly. It is assumed that thumb and iris as first group and second group as palm print and facial image. Once the groups were formed, then the merging was done using Equal half Merging. Equal half merging already discussed in previous section. Then biometric samples were sent to the image merging section. After that, the resultant images are thumb-iris image and palm print-facial images. Then rest of the procedure is as such of BSPS algorithm.

## 4.2 Result and Analysis of Merged-Bio-Cryptography

The analysis was made on the basis of the Matlab simulations.

### *4.2.1 Impact of Merging Vs Data Size*

First calculated size of the two individual images, after merging, it is calculated one more time. For instance, in thumb-iris test case, the thumb image size was 42,674 bytes and iris size was 230,454 bytes. Finally after merging the images, the total size was 26,036 bytes. It is observed that, while merging the biometric images, there is chance of compressing for merging. It may not happen frequently. Table number 1 is provided some important combinatorial test cases of merged biometric images.

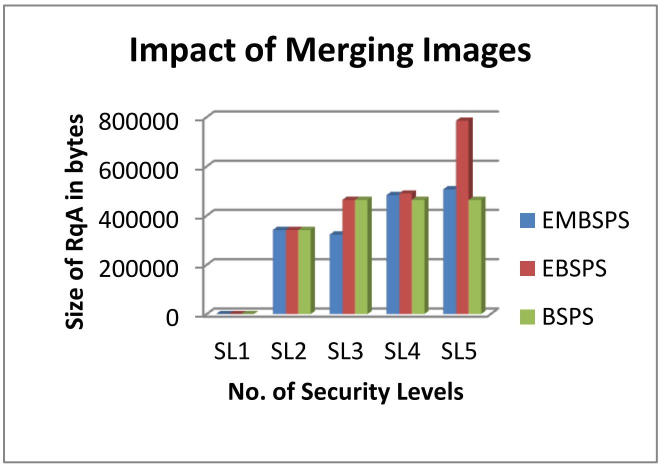


**Figure 3: Impact of Merging on EMBSPS, EBSPS and BSPS.**

It is that observed that the EMBSPS the performance is good, comparatively EBSPS and BSPS after merging the biometric images. Also in SL-4 and SL-5 it appears to be BSPS RqA packet size is performs better than EMBSPS and EBSPS, but the BSPS security is too weak comparatively EMBSPS and EBSPS. Figure No. 3 shows the impact of merging the images.

### 4.2.2 Impact of Computation Time

Secondly, calculated whole procedure of the EMBSPS, like edge detection and encryption will consume some specific amount of time. For example, palm print-facial test case will consume 1.40774 sec, whereas thumb-iris will take 0.46717 sec. Some important test cases were mentioned in figure No.7 and 8. When EMBSPS is compared with the EBSPS algorithm, in the view of Computation time (CT), it is observed that EMBSPS has consumed less time than EBSPS procedure in every test case due to merging of merging of biometric images.

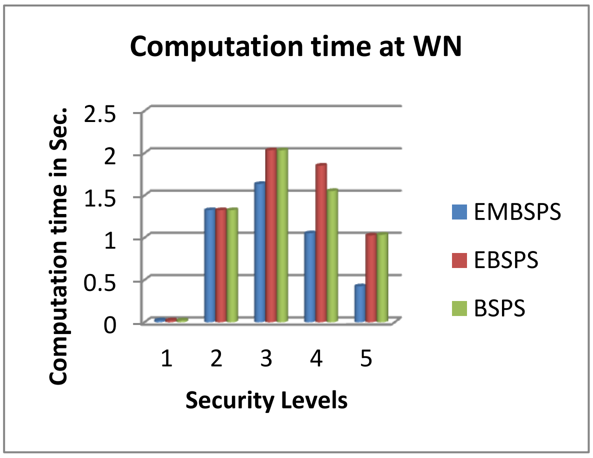


**Figure 4: Computation time at WN between EMBSPS and EBSPS algorithms.**

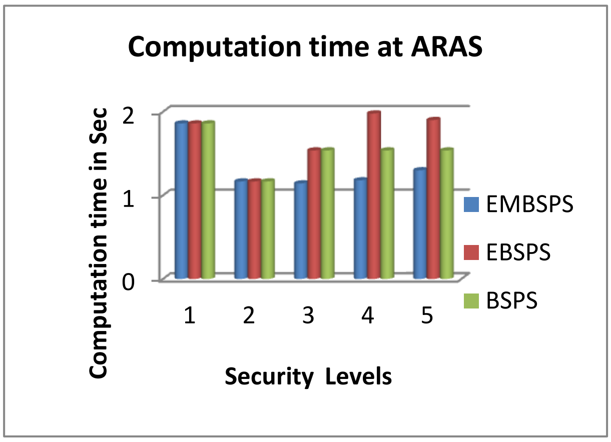


**Figure 5: Computation time at ARAS between EMBSPS and EBSPS algorithms.**

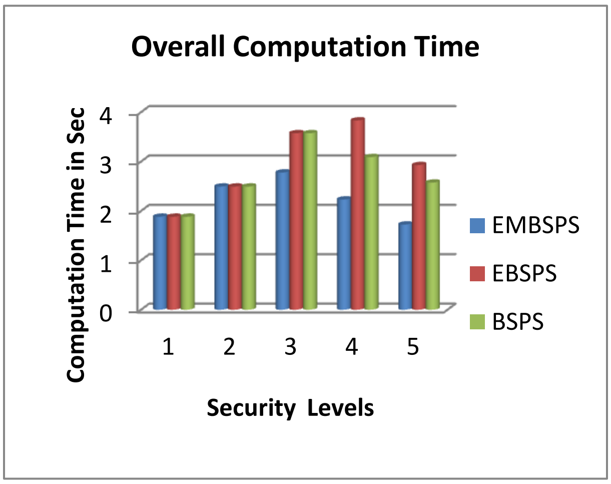


**Figure 6: Total Computation time at ARAS between EMBSPS and EBSPS algorithms.**

### 4.2.3 Impact of Data Size Vs Data rate

Lastly, when the data size is small, the data transmission is fast either in wired or wireless communications. The general phenomenon is data size is directly proportionate to data transmission in wireless network. The results were discussed in the previous work [5].

### 4.2.4 Impact of Security Levels

Figure 7 represents comparison of EBSPS with BSPS in terms of security level. It is found that EMBSPS and 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.

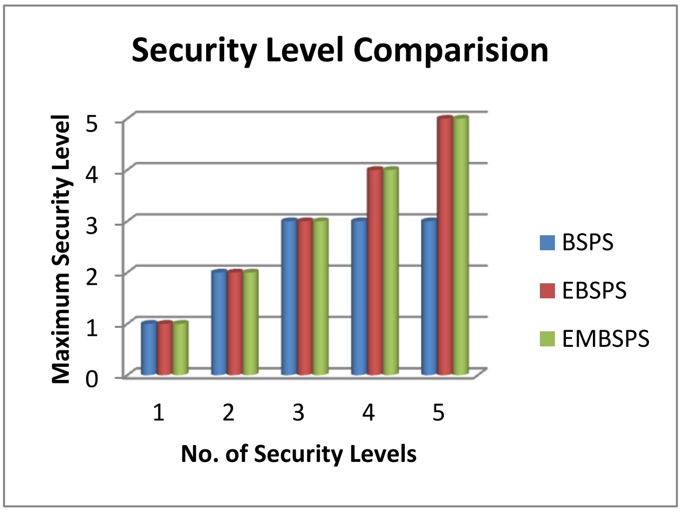
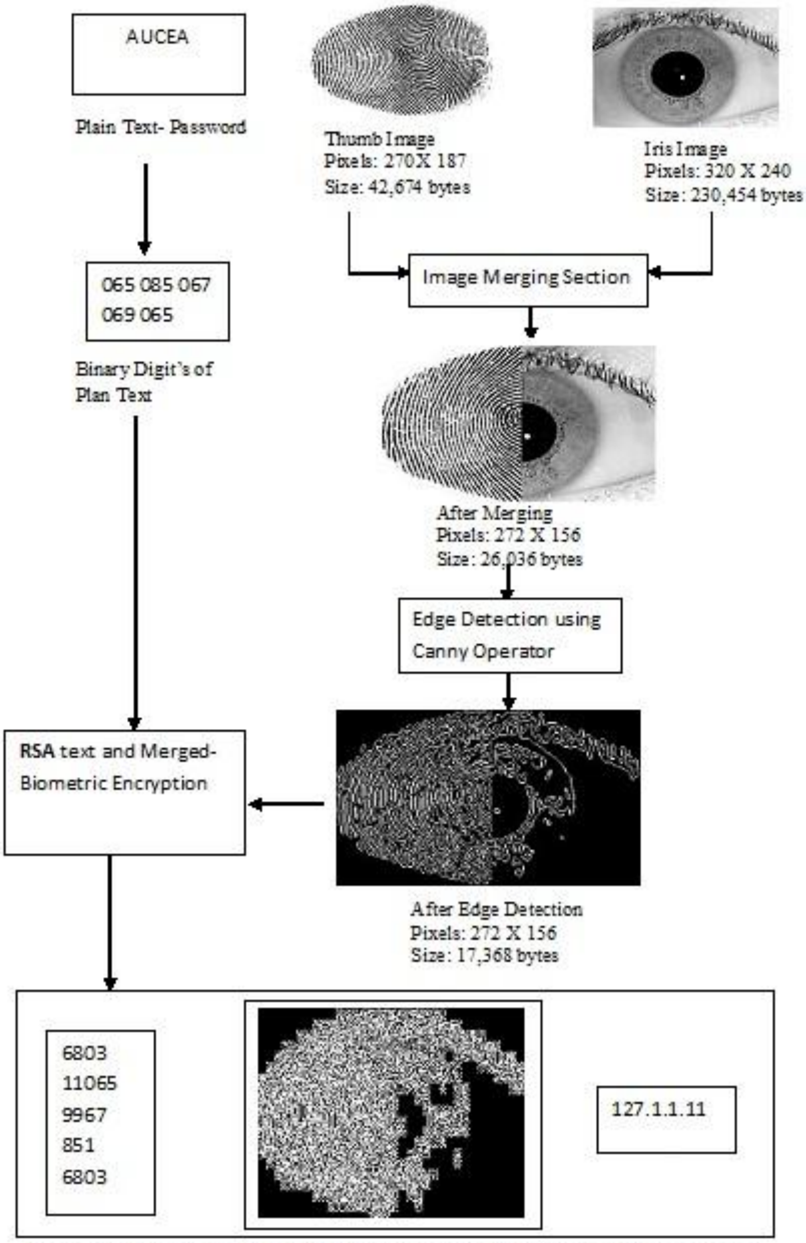


**Figure 7: Impact of Security Levels on EMBSPS, EBSPS and BSPS algorithms.**

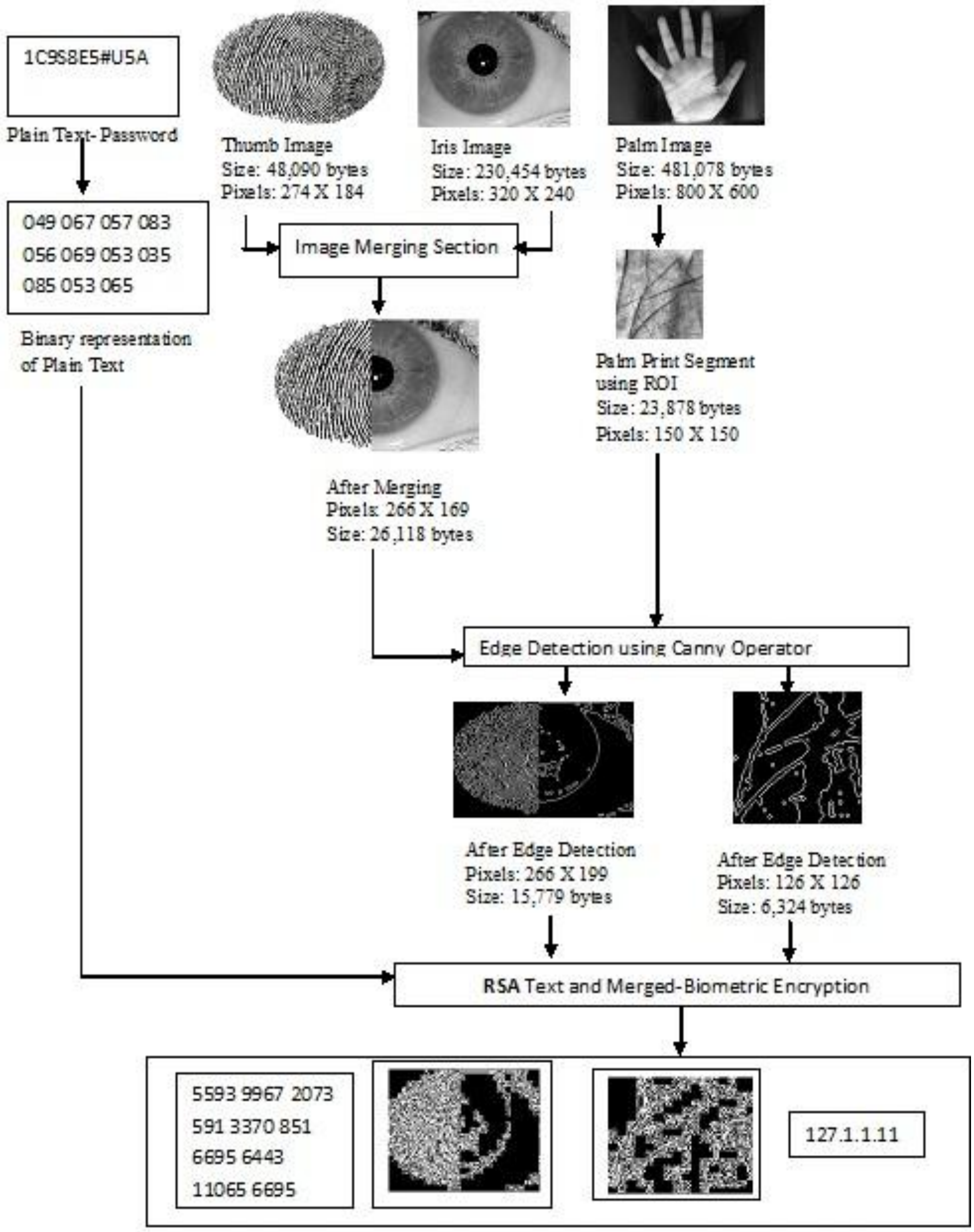
**Table 1. SL Comparison table for EMBSPS, EBSPS and BSPS**

| | SL1 | SL2 | SL3 | SL4 | SL5 |
|---|---|---|---|---|---|
| **EMBSPS** | Text | Text +Thumb | Text + Merge (Thumb,Iris) | Text + Merge (Thumb,Iris) + Palm print | Text + Merge (Thumb,Iris) + Merge (Palm print ,Face+ |
| **EBSPS** | Text | Text +Thumb | Text + Thumb + Iris | Text + Thumb + Iris +Palm print | Text + Thumb + Iris +Palm print + Face |
| **BSPS** | Text | Text +Thumb | Text + Thumb + Iris | Text + Thumb + Iris | Text + Thumb + Iris |



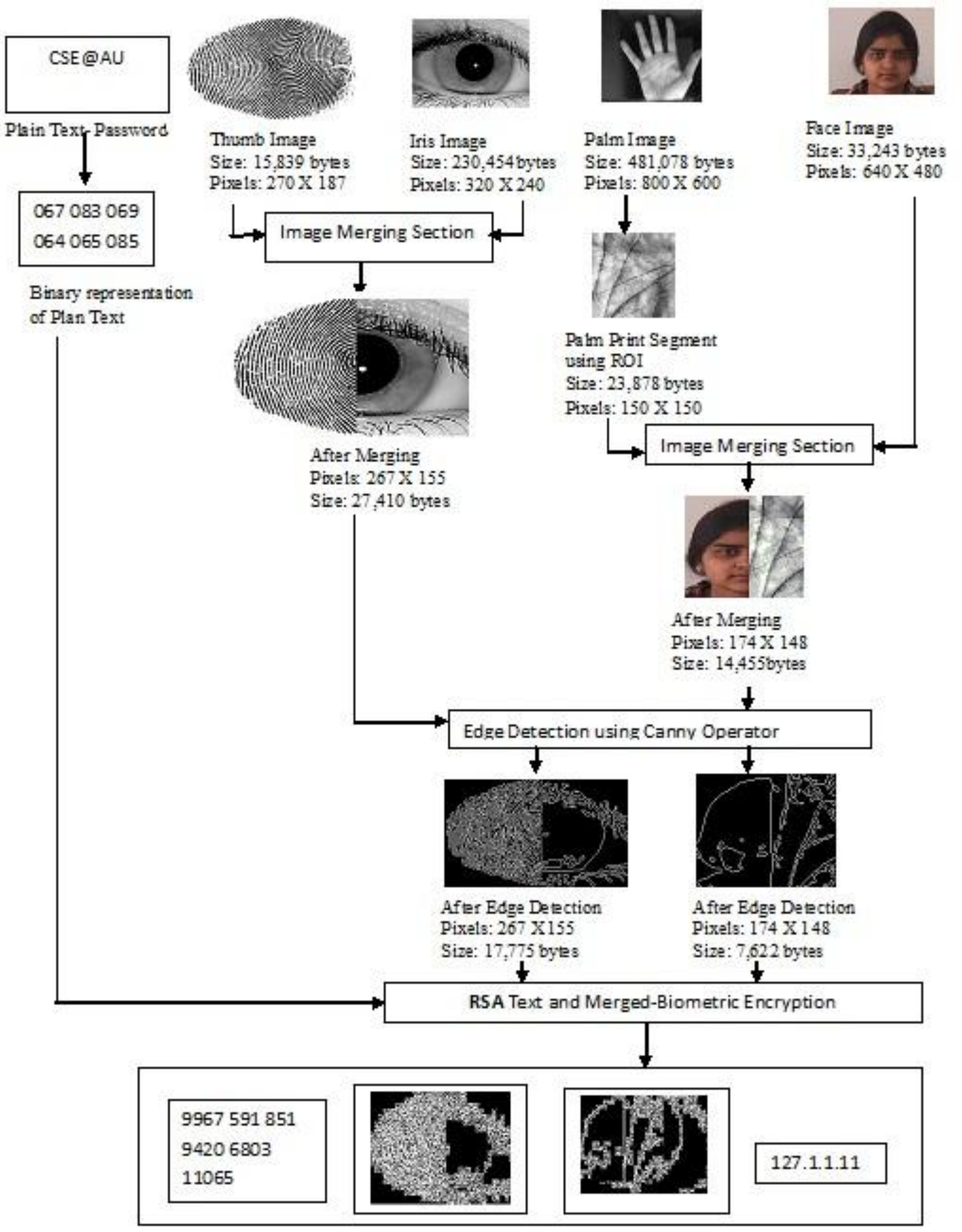
RqA3 (Request for Authentication for Security level 3) consist of encrypted tex t (20 bytes), merged thumb-iris (322,901 bytes) and ARAS IP Address (4 bytes).

**Figure 8: EMBSPS procedure at security level-3**



RqA4 (Request for Authentication for Security level 4) consist of encrypted text (39 bytes), merged thumb-iris (246,851 bytes), merged Palm-face (227,084 bytes) and ARAS IP Address (4 bytes).

**Figure 9: EMBSPS procedure at security level-4**



RqA5 (Request for Authentication for Security level 5) consist of encrypted text (23 bytes), merged thumb-iris (283,573 bytes), merged Palm-face (283,573 bytes) and ARAS IP Address (4 bytes).

Figure 10: EMBSPS procedure at security level-5

### 4.3 Performance evaluation

The overall performance of EMBSPS is better than EBSPS and BSPS because enhancement and Merge in the security level. The overall performance is articulated in our previous work [6]. The 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-6:

OP= (GR * LS) + LOS + TATi ---- (6)

## 5. CONCLUSIONS AND FUTURE SCOPE

Bandwidth and speedy access are two important aspects besides assuring the security for good Quality of Service in wireless networks. In the present work, it was achieved all the three aspect by introducing the novel EMBSPS. The algorithm mainly consist three steps. Firstly we merge the biometric images. Next, merged-biometric images are supplied for the pattern extraction using canny edge operator.

Finally the pattern extracted images are sent for encryption using RSA. Through EMBSPS procedure, the data size of the image is reduced. Once the data size is reduced the data rate is fast in the network. It will reflect in fast authentication, to access the WLAN with the permission of ARAS. Simulations were performed to encrypt text, thumb, Iris, palm and facial images using the MATLAB. The proposed EMBSPS compared with EBSPS and BSPS in terms of security and fast authentication. It is observed that, approximately 20% improvement in the fast authentication and 40% improvement in security level of EMBSPS compared to BSPS. The results show that without hampering LS, GR and LOS, the overall performance of the EMBSPS is good. In future it is possible to reduce the time for authentication process and more over it is possible to encrypt with the rest of cryptic mechanisms like ECC and Chaos-Based.

# 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 Kote, 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] Rajesh Duvvuru, P. Jagadeeswara Rao, Sunil Kumar Singh and Ankita Sinha, "Enhanced Security levels of BSPS in WLAN", Published In the International Journal of Computer Applications, Volume 84 - Number 2, pp. 33-39, December 2013

[8] 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

[9] 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.

[10] 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.

[11] 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

[12] 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 .

[13] Sankaran, M. Vatsa, and R. Singh, Hierarchical Fusion for Matching Simultaneous Latent Fingerprint, *In Proceedings of International Conference on Biometrics: Theory, Applications and Systems*, 2012.

[14] Ajay Kumar and Arun Passi, "Comparison and combination of iris matchers for reliable personal authentication," Pattern Recognition, vol. 43, no. 3, pp. 1016-1026, Mar. 2010

[15] Ajay Kumar, Sumit Shekhar, "Personal Identification using Rank-level Fusion," IEEE Trans. Systems, Man, and Cybernetics: Part C, pp. 743-752, vol. 41, no. 5, Sep. 2011

[16] Vidit Jain and Amitabha Mukherjee, "The Indian Face Database",2002,(http://vis-www.cs.umass..edu/$\sim$vidit/{I}ndian{F}ace{D}atabase).

[17] 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.

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

[19] Zhongjian Zhao and Xiaoqiang Zhang. "ECC-Based Image Encryption Using Code Computing.." Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering Advances in Intelligent Systems and Computing, Volume 181, Springer, pp 859-865, 2013

[20] Yaobin Mao and Guanrong Chen. "Chaos-Based Image Encryption." Applications in Pattern Recognition, Computer Vision, Neuralcomputing, and Robotics, Springer, pp 231-265, 2005.

[21] Avala Ramesh and S. Pallem Setty, "Analysis on Biometric Encryption using RSA algorithm," Published In the IJMER, Volume 2, Issue 11(2), pp. 302-307, October 2013.