

## Improved Security to private cloud through Novel Chaotic based Bio-cryptic Cloud Security Mechanism

**Sudhakar Godi**

Department of Computer Science and Engineering,  
Swarnandhra College of Engineering & Technology  
Narasapur, West Godavari, A.P., INDIA  
[suda.godi@gmail.com](mailto:suda.godi@gmail.com)

**Rajasekhar Rao Kurra**

Department of Computer Science and Engineering  
Sri Prakash College of engineering ,Tuni  
East Godavari, A.P., INDIA  
[krr\\_it@yahoo.co.in](mailto:krr_it@yahoo.co.in)

**Abstract-** Reliability and confidentiality are two important parameters to secure the private cloud's data. For the past two decades, the cloud computing industry became more popular due to wide range of applications and its usage. In addition to its extensive applicability, the data storage, network maintenance and Quality-of-Security (QoS) are major challenges in cloud computing, especially in a private cloud. This paper describes in improving the QoS private cloud network through a novel Chaotic based Bio-cryptic Cloud Security (CBCS) algorithm. This paper also comprises of private cloud management, chaotic maps, Security Level (SL) and Bio-cryptic Security aware Packet Scheduling (BSPS) algorithm. This work describes the importance of the private cloud access and its secure concepts through CBCS algorithm for the different levels of user authentication. The CBCS approach designed for strengthening the authentication process between the client/server architecture to protect client own private data from unauthorized user. The simulation results were compared with the existing non-chaotic, based Private Cloud Security Level Algorithm (PCSLA). Finally, the proposed CBCS algorithm outperforms PCSLA in terms of Packet Size (PS), SL and Overall Performance (OP).

**Keywords:** Cloud Computing, Bio-cryptography, chaotic maps

### Introduction

Since the cloud computing paradigm was introduced in 1999 by Salesforce.com, numerous attempts were made to improve the QoS on Cloud databases [1]. However, Cloud servers are facing with severe attacks like session riding, virtual machine escape, unauthorized access, reliability and availability of service, Insecure cryptography, Data protection and portability, CSP Lock-in, illicit entry, Hijacking and Denial-of-service (DoS) and many more [2] [3]. Beside many applications and advantages with the cloud computing has taken a giant leap in the current software industry. Cloud computing can be categorized into public, private, community and hybrid types cloud consisting of three layers named Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) in

each [4]. Due to the extensive applications of cloud computing like easy access of data, low hardware cost, fast computing, comfort with software up-gradation, enormous storage, sensor cloud, e-commerce, Bigdata analytics, social networking collaborations, heterogeneous operating system, Geographic Information System and many more [5]. According to the North Bridge GIGAOM Research survey report 2014, where more than 1,358 respondents participated. The survey specifies that, 49% opted for revenue generating or product development, 35% cited competitive advantage or innovation and 45% already using cloud platform. Software as a Service (SaaS) there is a considerable improvement of amount with 72% users and vendors from 2013 to 2014. Also, there is significant improvement in the cloud transition with an 65% to 75%. The major point to be noted that Information Technology (IT) companies are allocating 80% of their annual budget on a cloud platform and its applications [6].

From the above specified survey reports, it is clearly specified that, there is huge demand for the cloud computing. As specified earlier the security attacks are increasing with respect to the demand. Especially the security, private cloud is always a major challenging task. Over the years, many researchers and practitioners proposed various solutions to protect private cloud data [7] [8]. Especially introducing security levels in private-cloud authentication using bio-metrics makes to think to for betterment [9]. At present a limited biometric authentication includes fingerprint, palm-print, face and iris patterns. Earlier numerous solutions were proposed in strengthening the authentication in Wireless Local Area Networks (WLAN) using Bio-cryptic security levels. The demand of Biometric usage is increasing day to day, especially in India like country. A unique, Identification project named AADHAR in India, where identification was done using biometric pattern recognition for each and every person, who are aged above 5 years [10].

The existing approach Private Cloud Security Level Algorithm (PCSLA) handles only a limited authentication process[9]. In PCSLA the biometric protection is concepts

not addressed. Further proposed solutions were discussed in the next sections.

The proposed approach comprises: (1) a study and analysis of private cloud data security; (2) Chaos based Bio-cryptic Cloud Security algorithm (CBCS); and (3) a novel measure by combining both security level and computation time; (4) a working model simulator where the CBCS algorithm was implemented and tested. The rest of the paper is organized as follows. Section 2 discusses related works in the arena of cloud computing, private cloud storage, and Chaos based algorithms. Section 3 describes the proposed architecture and CBCS algorithm. Simulation and results were discussed in Sections 4. Finally work concluded with brief pros and cons of CBCS and PCSLA with further scope in Section 5.

## Related Work

As specified in the earlier section, the cloud computing is a great invention in the information age. Cloud computing working as a base point to bring the Internet-of-Things (IoT) to this computation world. But secure cloud data storage and access is always a challenging task. Traditional authentication methods weakens the cloud computing mechanism by assigning common authentication to all the users. Various types of clients use the private cloud for their data storage and computation. People store data according to their need, some save highly confidential and few stores unimportant. But everyone expects confidentiality of their private cloud data, confidentiality can be achieved through a proper authentication mechanism.

In general, Lightweight Directory Access Protocol (LDAP) is used for the user authentication [11]. LDAP services belong to the Application Layer in TCP/IP protocol stack. Whereas in the cloud, the IaaS layer will take care of the authentication process in association with LDAP [12]. But Literature notifies different security levels in WLAN through various security level mechanisms. The WLAN authentication mechanism proposed by various researchers. Among them Security aware Packet Scheduling algorithm (SPSS) is an initial one proposed by Qin et al [13]. Later R Duvvuru et al extended and designed Automated Security aware Packet Scheduling algorithm (ASPS), Bio-cryptic Security aware Packet Scheduling algorithm (BSPS), Enhanced Bio-cryptic Security aware Packet Scheduling algorithm (EBSPS)[14][15][16]. These algorithms are a combination of the Bio-cryptic and text-cryptic authentication to the WLAN. Then R Avala and S P Setty inherited some properties from EBSPS and designed Enhanced Merged Bio-cryptic Security aware Packet Scheduling algorithm (EMBSPS) and Mult Merged Bio-cryptic Security aware Packet Scheduling algorithm

(MMBSPS) for fast packet transmission inside the WLAN beside assuring security [17][18][19]. Making one step forward Sanjay Kumar introduced a six level bio-cryptic security with Improved Bio-cryptic Security aware Packet Scheduling algorithm (IBSPS) [20]. Whereas Abdullah Sharaf Alghamdi et al., introduced Bio-Chaotic Stream Cipher-Based for cyrptic-Iris image. [21]. The Bio-Chaotic algorithm (BCA) model was adopted for extending the security of Cloud computing data. In addition to that Uma D G et al came up with a novel solution Multi Merged Biometric Water Marking Security Aware Packet Scheduling Algorithm using bio-watermarking for the protection of biometric templates [22]. Whereas we also successfully implemented and tested Double Biocrypted Security-Aware Packet Scheduling Algorithm (DBSPS) to strengthen the authentication process in WLAN using RSA and Selective encryption [23]. Due to the heavy demand of cloud computing, there is the need to maintain the Quality-of-Security (QoS). Once again Rajesh Duvvuru et al came up with a novel idea by introducing the security levels through PCSLA for cloud authentication [9]. Unfortunately the current proposed method PCSLA require improvements in order to achieve QoS. The proposed method CBCS algorithm adopted the advantages of PCSLA, CBSPS and DBSPS algorithms. The concept of Bio-cryptography comprises of securing the biometrics from Hackers or illicit users [24]. The CBCS algorithm designation details discussed in the next section.

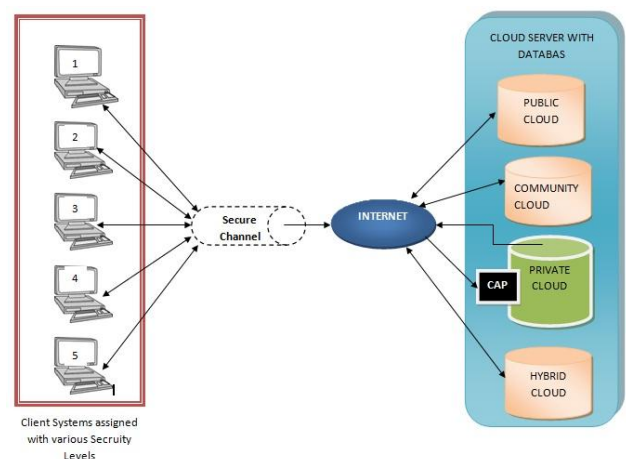


Fig.1. Architecture of proposed Client-Server Cloud network with limited number of client systems

## The Chaotic Based Bio-Cryptic Cloud Security (CBCS) Algorithm

### A. Assumptions and Notations

This cloud security model assumed with a limitation of five level security. The network model comprised of various security client systems assigned to a static Security Level (SL). Clients System will communicate with the server to

access the cloud through HTTPS and TCP/IP protocols (internet) in a secure channel. Cloud Authentication Point (CAP) verifies the credentials of the client and grant or rejects access to the private Cloud Data (CD). Whereas, Network Delay (ND) is assumed with the Random Probability Distribution (RPD). Also, it is presumed that, the Gurantee Ratio (GR) access to the private cloud, is Random Probability Distribution (RPD). Whereas Packet Size (PS) plays a vital role in the bandwidth utilization, If packet size is small, more packets will be sent over the network. PS varies from the level to level. The security level assignment was done according to the users need. A fixed number security level is assumed to the each and every client system, depending on Medium Access Control(MAC) address in the cloud server.

The logistic map technique considered for the Bio-Chaotic encryption [25]. The computations of a logistic map can articulate in Equation-1:

$$LM = x_{n+1} = ax_n (1 - x_n) \quad -- (1)$$

Where  $x = \{1,2,3 \dots n\}$  are pixel coordinates, which magnify the population of 741 and 'a' is chaotic behavioral variable value ranges in between 3.5 to 4.

#### B. The packet prototype

CBCS works Client-Server(CS) handshaking mechanism. This mechanism contains request packets and response packets. Request packets are Initial Request (IRq) and Secure cloud authentication Packet (ScaP). Whereas response packets are Initial Response (IRs) and Authentication Status (AS) packet. Here, IRq and IRs are used for initial request and response the cloud data (for instance website) to access respectively. Where ScaP data packets are used for communication between client and server through discrete bio-cryptic data and AS packets responds to the client from the server by verifying the credentials of the ScaP. IRq, IRs and AS packets are inherited from the general CS architecture. The details are as follows:

- IRq represents with a set of fields (CIP, D, SIP, AT, C<sub>S</sub>). Where CIP is the clients IP address, C<sub>S</sub> is a client sequence number and the D denotes payload.
- IRs notifies with a set of attributes (CIP, AD, SIP, AT, S<sub>S</sub>). Where CIP is the clients IP address, S<sub>S</sub> is a server sequence number and the AD denotes authentication payload, it contains various biometric input fields. IRs is classified into five types IRs1 to IRs5
  - IRs1 have (CIP, AD1, SIP, AT, S<sub>S</sub>), where AD1 is the Input payload request for cryptic-text-password fields.

- IRs2 with (CIP, AD2, SIP, AT, S<sub>S</sub>), where AD2 is the Input payload request for cryptic-text-password and cryptic-thumb-print attributes.
- IRs3 contains (CIP, AD3, SIP, AT, S<sub>S</sub>), where AD3 is the Input payload request for cryptic-text-password, cryptic-thumb-print and cryptic-Iris tuples.
- IRs4 includes (CIP, AD4, SIP, AT, S<sub>S</sub>), where AD4 is the Input payload request for cryptic-text-password, cryptic-thumb-print, cryptic-Iris and cryptic-palm-print templates.
- IRs5 comprises (CIP, AD3, SIP, AT, S<sub>S</sub>), where AD5 is the Input payload request for cryptic-text-password, cryptic-thumb-print, cryptic-Iris, cryptic-palm-print and cryptic-face records.
- AS comprises of group of tuple (CIP, Stat, Session, SIP, AT). Where CIP is the clients IP address, Stat field represent ACCEPTED or DENIED access to the server and Session bit denotes session establishment between cloud's CS.

The ScaP is categorized into five types and the description is as follows:

#### Secure cloud authentication Packets (ScaP)

The ScaP contains Biometric templates of users in encrypted form. CAP will validate the ScaP and allows to access CDB or rejects to resend the ScaP with valid data. With reference to the earlier discussion, ScaP can be categorized into five types. They are (1) Secure cloud authentication Packet with the first level of security (ScaP1). (2) Secure cloud authentication Packet with the second level of security (ScaP2). (3) Secure cloud authentication Packet with the third level of security (ScaP3). (4) Secure cloud authentication Packet with the fourth level of security (ScaP4) (5) Secure cloud authentication Packet with the fifth level of security (ScaP5). The detailed new ScaP data packets are discussed below:

- ScaP1, comprises a set of four fields (1, Cryptic-text Password, SIP, AT). 1 cites as the first level of security and cryptic password.
- ScaP2, is a tuple of five fields (2, Cryptic-text Password, Cryptic-thumb-print, SIP, AT). 2 stipulates second level of security and Cryptic-thumb-print.
- ScaP3, contains a record of six fields (3, cryptic-text Password, Cryptic-thumb-print, Cryptic-Iris, SIP, AT). 3 designates the third level of security, Cryptic-thumb-print and Cryptic-Iris.
- ScaP4, includes of seven fields (4, Cryptic-text Password, Cryptic-thumb-print, Cryptic-Iris, Cryptic-Palm-print, SIP, AT). 4 specifies the fourth level of security, Cryptic-thumb-print, Cryptic-Iris and Cryptic-Palm-print.

- ScaP5, contains a record of eight fields (5, Cryptic-text Password, Cryptic-thumb-print, Cryptic-Iris, Cryptic-Palm-print, Cryptic-face, SIP, AT). 5 specify security level 5, Cryptic-thumb-print, Cryptic-Iris, Cryptic-Palmprint and Cryptic-face

Where *SIP* is the Internet Protocol Address of Server and *AT* is the arrival time of respective packet, these are common fields in every ScaP. *AT* assumed with the Random probability distribution function. The proposed CBCS Algorithm deals with the Application security of private cloud's, IaaS layer.

### C. The CBCS Algorithm

This algorithm mainly focused on the Quality-of-Security (QoS) to the private cloud. The Bio-Chaotic approach is used with the help of Logistic map. This algorithm is specially meant for designation of Security levels. The problem solving approach step-by-step is as follows:

*Step1:* Initially the request packet *IRq* is sent over the internet through HTTP from the client system to cloud server.

*Step2:* Once the server receives *IRq* from the client, the *CAP* will issue *IRs* packet to the client over the internet .

*Step3:*The *IRs* packet contains *AD* attribute, it acts according to the MAC address and Security Level of Client.

*Step3.1:* IF *IRs1*, then Client Sent *ScaP1* to CS

ELSE IF *IRs2*, then Client Sent *ScaP2* to CS

ELSE IF *IRs3*, then Client Sent *ScaP3* to CS

ELSE IF *IRs4*, then Client Sent *ScaP4* to CS

ELSE Client Sent *ScaP5* to CS

*Step4:* The CS receives ScaP, then the CAP unit decrypts the biometric templates and check credentials with the stored templates.

*Step5:* IF *CAP* == *ScaP*, then AS is activated and AS packet with stat attribute as 'ACCEPTED' is sent to the client and GOTO Step6.

ELSE then AS is activated and AS packet with stat attribute as 'DENIED' is sent to the client.

*Step6:* Session is established between the client and CS for further client operations.

*Step7:* Stop

## Simulations and Results

Simulation of CBCS performed using a Chaotic logistic map. Matlab software is used for the encryption and decryption of Biometric templates. In the simulation we only worked with the cryptic biometric templates and the rest of the parameters of CBCS are assumed, discussed in the earlier section.

### A. Simulation of ScaP1

The ScaP1 contains the only cryptic text password based on the RSA algorithm encryption. The implementation was done on Matlab software. The two big numbers are considered with a small key, taking big key make more complex, which is not feasible. The algorithm tested more than 67times with various combinations of keys, prime numbers and cipher texts. The rest of simulation result for an instance are as follows:

The value of (N) is: 594437

The public key (e) is: 5

The value of (Phi) is: 592896

The private key (d)is: 474317

Enter the message: cloud

ASCII Code of the entered Message: 99 108 111 117 100

Cipher Text of the entered Message: 97373 581439 75912 454923 380786

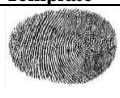
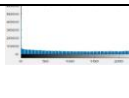

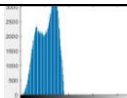
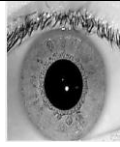
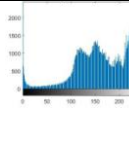
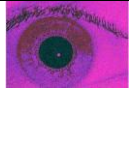
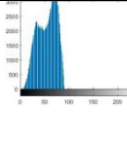
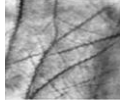
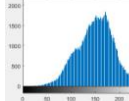

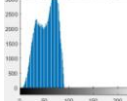

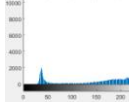

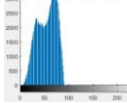
Decrypted ASCII of Message: 99 108 111 117 100

Decrypted Message is: cloud

### B. Simulation of ScaP2 to ScaP5

As specified in the earlier section ScaP encompasses of Bio-Chaotic Logistic Map encryption performed using three related functions *Hundungen()*, *Keygen()* and *LogisticMap()*. The related simulation details can be found in the literature [21]. Table-1 shows the simulation result of ScaP5, Where encryption to the thumb-print and Iris samples. The Biometric Database samples were collected from the popular biometric research databases like IIT Delhi, University of Massachusetts Amherrest and IIT Delhi[26][27][28] [29].

TABLE.1. Procedure of Bio-Chaotic Logistic Map Encryption

Original Biometric Template	Original Histogram	Key Size (bit)	chaotic Biometric Template	Bio-cryptic Histogram
		64		
		64		
		64		
		64		

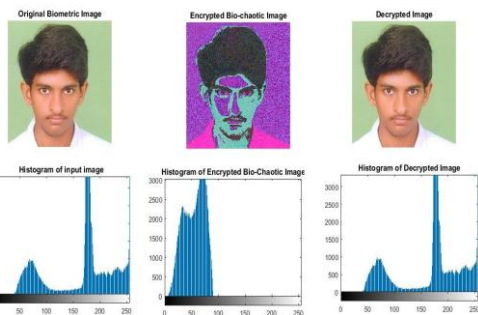






Fig. 2. Simulation of Bio-Chaotic approach in CBCS algorithm

TABLE.2 is ScaP5 with all attributes

Security Level	Cryptic-text	Cryptic-thumbprint	Cryptic-Iris	Cryptic-Palm-print	Cryptic-face	Server IP	A/T
5	97373581 43975912 45492338 0786					198.51. 100.2/4	R P D

C. Impact of Packet Size

The packet size varies from one security level to next level security level. But the results obtained through simulation states that, PCSLA PS is comparatively less than CBCS algorithm. Figure 3 shows the graphical representation of PS, where X-axis and Y-axis are PS and SL respectively.

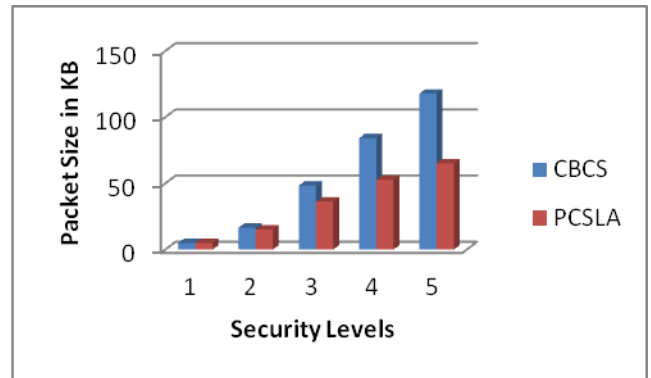


Fig. 3. Impact of PS on SL

D. Impact of Security Levels

The CBCS consists of good quality of security with Logist Map encryption, when compared to an existing PCSLA algorithm. PCSLA used biometric templates for authentication but, without security. CBCS besides assuring the security, it maintained five levels of security.

E. Overall Performance impact

The Overall Performance is calculated with the following equation-2

$$OP = LT + (GR * SL) + ND + PS \dots (2)$$

Where GR,SL, NT, PS and ND is assumed with certain probability distribution and LT is an operation time of the Logistic map with Biometric images. Figure 4 shows the graphical execution of OP at every SL, where X-axis and Y-axis plotted with SL and OP respectively. The OP clearly shows CBCS performance is better than PCSLA, except at SL-1. On an average CBCS algorithm performed approximately 15% to 20% better than PCSLA.

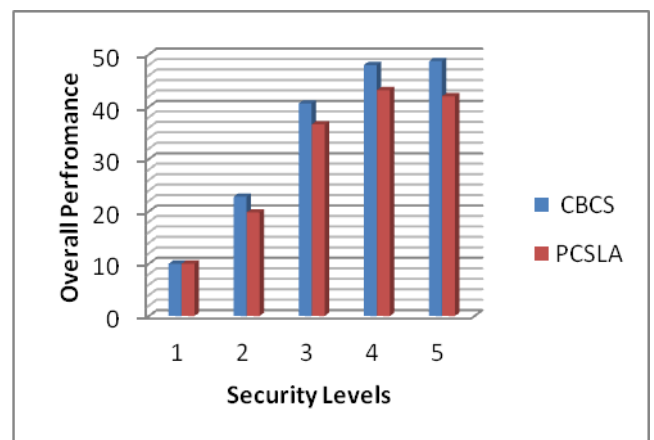


Fig. 4. Overall Performance graph between CBCS and PCSLA.

## Conclusions and Future Scope

Presently Cloud computing business is considered as a high priority industry, rather than all other software business. Due to many useful applications, users are comfortable with the cloud computing. But cloud computing is facing many major security threats. It results in poor services on the cloud server. Especially providing secure and safe authentication to the Private CS is a challenging task for the researcher and practitioners. This paper introduces a novel CBCS algorithm to strengthen the authentication process of Private CS. The CBCS comprises with Bio-Chaotic approach with various levels of security to different people, which will improve the secure access to the CS. Existing approaches PCSLA doesn't satisfy the security related issues, even it have Biometric SL. The CBCS simulated and tested successfully, the outcomes are compared with the PCSLA. The Overall Performance of CBCS is approximately 20% better than PCSLA.

In future, there is a need to improve the security authentication process to the clients via, many chaotic approaches.

## References

- [1] <http://www.computerweekly.com/feature/A-history-of-cloud-computing> (Accessed on 02/11/2014)
- [2] [https://downloads.cloudsecurityalliance.org/initiatives/top\\_threats/The\\_Notorious\\_Nine\\_Cloud\\_Computing\\_Top\\_Threats\\_in\\_2013.pdf](https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf) (Accessed on 16/10/2014)
- [3] <http://www.cloudcomputing-news.net/news/2014/nov/21/top-cloud-computing-threats-and-vulnerabilities-enterprise-environment/> (Accessed on 17/03/2015)
- [4] Armbrust, Michael, et al. "A view of cloud computing." *Communications of the ACM* 53.4 (2010): 50-58.
- [5] Velte, Toby, Anthony Velte, and Robert Elsenpeter. *Cloud computing, a practical approach*. McGraw-Hill, Inc., 2009.
- [6] <http://mjskok.com/resource/2014-future-cloud-computing-4th-annual-survey-results> (Accessed on 03/03/2015)
- [7] Feng, Deng-Guo, et al. "Study on cloud computing security." *Journal of software* 22.1 (2011): 71-83.
- [8] Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and Atanu Rakshit. "Cloud security issues." In *Services Computing, 2009. SCC'09. IEEE International Conference on*, pp. 517-520. IEEE, 2009.
- [9] Rajesh Duvvuru et al, "Improving Security in Private Cloud through Cryptographic and Biometrics", In *NCCS-2012, Pune, India*.
- [10] <https://eaadhaar.uidai.gov.in/> (Accessed on 05/09/2014)
- [11] Howes, Tim. "The string representation of LDAP search filters." (1997).
- [12] Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34, no. 1 (2011): 1-11.
- [13] 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.
- [14] 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.
- [15] Duvvuru, Rajesh, P. Jagadeeswara Rao, and Sunil Kumar Singh. "Improving Security levels in WLAN via Novel BPS." *Emerging Trends in Communication, Control, Signal Processing & Computing Applications (C2SPCA), 2013 International Conference on. IEEE, 2013*.
- [16] Duvvuru, Rajesh, et al. "Enhanced Security levels of BPS in WLAN." *International Journal of Computer Applications* 84.2 (2013): 33-39.
- [17] Ramesh, Avala, and S. Pallam Setty. "Enhanced Merged Security Levels of BPS in WLAN." *International Journal of Computer Applications* 88.7 (2014): 26-34.
- [18] Ramesh, Avala Ramesh and S. Pallam Setty. "Enhanced Authentication Mechanism in WLAN via MBSPS", In *IJMER, Special edition*, April 2014.
- [19] Ramesh, Avala, and S. Pallam Setty. "A Comparative Study on Security Levels in WLAN." *International Journal of Computer Applications* 93.8 (2014): 11-17.
- [20] Kumar, Sanjay. "Enhancing the Security Levels in WLAN via Novel IBSPS." *Advanced Computing, Networking and Informatics-Volume 2*. Springer International Publishing, 2014. 351-359.
- [21] Alghamdi, Abdullah Sharaf, Hanif Ullah, Maqsood Mahmud, and Muhammad Khurram Khan. "Bio-chaotic stream cipher-based iris image encryption." In *Computational Science and Engineering, 2009. CSE'09. International Conference on*, vol. 2, pp. 739-744. IEEE, 2009.
- [22] Geddada, Uma Devi, and Kaligithi Rajesh Kumar. "MMBWS FOR STRENGTHENING AUTHENTICATION PROCESS IN WIRELESS LOCAL AREA NETWORKS." *International Journal of Computer Engineering and Applications, Volume VIII, Issue I, Part I, 174-184, October 14*.

- [23] Godi, Sudhakar. "Improved Security Levels of Wireless LAN through DBSPS." *International Journal of Computer Applications* 106.14 (2014).
- [24] Ratha, Nalini K., Jonathan H. Connell, and Ruud M. Bolle. "Enhancing security and privacy in biometrics-based authentication systems." *IBM systems Journal* 40, no. 3 (2001): 614-634.
- [25] Pareek, Narendra K., Vinod Patidar, and Krishan K. Sud. "Image encryption using chaotic logistic map." *Image and Vision Computing* 24, no. 9 (2006): 926-934.
- [26] Ajay Kumar, "Incorporating Cohort Information for Reliable Palmprint Authentication," *Proc. ICVGIP, Bhubneshwar, India*, pp. 583-590, Dec. 2008
- [27] 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.
- [28] D. Yadav, N. Kohli, R. Singh, and M. Vatsa, Revisiting Iris Recognition with Color Cosmetic Contact Lenses, 6th IAPR International Conference on Biometrics, June, 2013.
- [29] A. 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.