Volume 1, No. 2, September 2010
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

Cloud Software as a Service with Iris Authentication

D.Kesavaraja[*1], D.Sasireka[2], D.Jeyabharathi[3]

[*1] Department of Computer Science and Engineering, Dr Sivanthi Aditanar College of Engineering, Tiruchendur, Tamilnadu,India
Email: dkesavaraja@gmail..com[1]

[2] Department of Information Technology,PSN College of Engineering and Technology , Tirunelveli Tamilnadu,India
Email: edsasireka@yahoo.com[2]

[3] Department of Computer Science and Engineering,Einstein College of Engineering, Tirunelveli Tamilnadu,India
Email: bharathi.durai@gmail..com[3]

Abstract: Cloud computing provides amble opportunity in many areas. In our Cloud Data Server provides fast and reliable software service to its clients.In that service authentication for identifying authorized user as a major issue. So we proposed a novel security mechanism named as iris cloud verification. The Cloud Iris Verification System(CIVS) enables authorized user to access software as a service from cloud server. It is suggested in recent biometric literature that human irises might be as distinct as fingerprints for different individuals, leading to the idea that iris patterns may contain unique identification features. An CIVS compares a newly acquired iris pattern with a retrieved iris pattern from a data base to decide if they originated from the same eye. Iris patterns are collected from images of the eye. Our system proposes novel and efficient cloud iris recognition method that employs cumulative SUM based grey change analysis. Iris recognition includes security to cloud server from unauthorized access. We demonstrate the effectiveness and feasibility of our method on a thousands of eye images for defense forces. The efficiency ratio of this computation process is 93.17.

Keywords:Cloud Data Server,Cloud Iris Verification System,Iris,Security,Software As a Service

INTRODUCTION

With the fabulous growth of Cloud-based software as a services and sensitive information on Cloud, Cloud security is getting more important than ever. Cloud Based Applications has need in on a daily basis life. People use the Cloud to work, to exchange information, to make purchases, etc. This growth of the Cloud use has regrettably been accompanied by a growth of malicious activity in the Cloud. More and more vulnerabilities are discovered, and nearly every day, new security advisories are published [1][2].

Potential attackers are very numerous, even if they represent only a very small proportion among the hundreds of millions of Cloud users and clients.

In modern world cloud security is in critical need of finding accurate, secure and cost-effective alternatives to passwords and Cloud verification numbers (PIN) as financial losses increase dramatically year over year from computer-based fraud such as computer hacking and identity theft. Cloud Iris Verification system(CIVS) deal with these elementary problems because, an individual's biometric data is unique and cannot be transferred. Biometrics is an automated method of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic[3]. Examples of physiological characteristics include hand, finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits which can be learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics.

CIVS uses hardware to capture the biometric information, and software to maintain and manage the system. In general, the system translates these measurements into a mathematical, computer-readable format. When a user first creates a biometric profile, known as a pattern, that pattern is stored in a database. The CIVS then compares this pattern to the new image created every time a user accesses the service. For an enterprise server, CIVS provides value in two ways. First, a Cloud server automates entry into secure locations, relieving or at least reducing the need for full-time monitoring by personnel. Second, when rolled into an authentication scheme, Cloud server adds a strong layer of verification for user names and passwords.

CIVS adds a unique identifier to cloud authentication, which is tremendously difficult to duplicate. Smart cards and tokens also provide a unique identifier, but CIVS has an advantage over these devices: a user cannot lose or forget his or her fingerprint, retina, or voice. The practical applications for providing security to cloud service

Using iris recognition in cloud software, a client simply walks up to their system and looks in a sensor camera to access their service. The camera instantly photographs the iris of the clients [4]. If the client's iris pattern matches the record stored in the database access is granted. At the cloud software, a positive authentication can be read through glasses, contact lenses and most sunglasses. Iris recognition proves highly accurate, easy to use and virtually fraud proof means to verify the identity of the clients.

CLOUD CLIENT ATTACKS

Cloud client attacks intrudes cloud server and perform improper access in cloud service,The following figure describes the cloud client attacks in the cloud environment,

© JGRCS 2010, All Rights Reserved

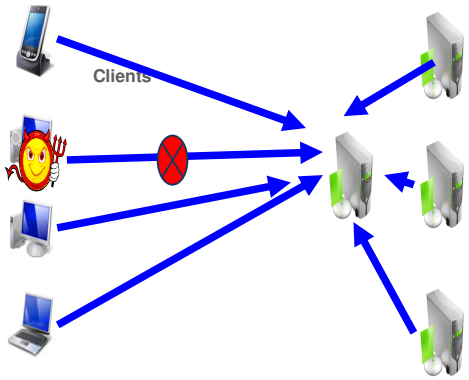


Figure 1:Cloud Client Attacks

Fig-2 gives the detailed structure of the Cloud Client Attacks. A dependable system is defined as one that is able to deliver a service that can justifiably be trusted. Attributes of dependability include availability, reliability, confidentiality, and integrity.
Security is the concurrent existence of Availability-Readiness for correct service ,Confidentiality - Prevention of unauthorized disclosure of information ,Reliability - Continuity of correct service ,Integrity -The absence of improper system state alterations.

HTTP WEB SERVER

Distributed Data backups are managed by Web Server and provide a reliable service to the user. Redundancy is used to increase system availability.

Most attacks take advantage of specific vulnerabilities in a particular OS, controller , or hardware platform, they are, in general, ineffective on others. So, the deployment of a redundant data management Web servers (hardware/OS/Virtual Controller) should allow the system to continue providing acceptable service to users, even if parts of the system are corrupted. The Web servers provide the same services but run different platforms.

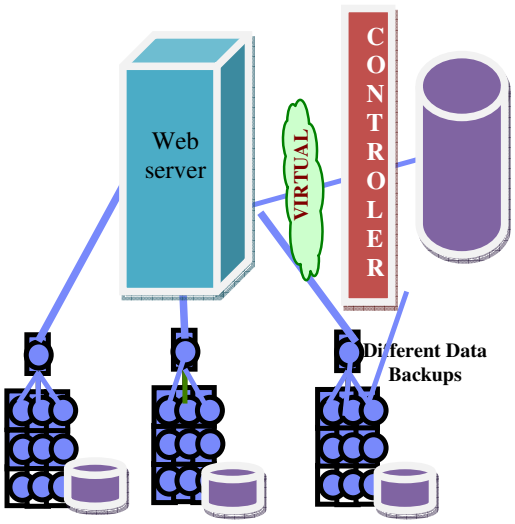


Figure 2: Distributed Web Server Architecture

Fig-2 gives the detailed structure of CIVS and how the virtual controller is connected with the CIVS .

ROBUST WEB SEVER

Adaptive Tolerant Web Server provides service taking care of security and persistent availability required for a web service. When the CIVS gets a HTTP request, instead of immediately providing the HTTP response it holds the request and connects to the virtual controller. When the virtual controller is connected, the CIVS is cut off from the cloud. After the Agreement protocol is satisfied the virtual controller is cut off and the HTTP response is sent to the user from the CIVS.
Thus the controller were the hash code resides is segregated from the cloud during the agreement protocol process ensuring inability to hack the system.

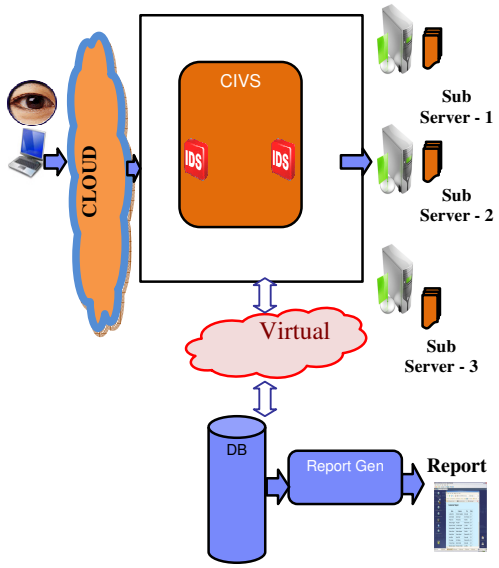


Fig 3 – Cloud Iris Verification System

SYSTEM MODEL

In our CIVS system having five set of stages described in fig 4. The stages are

1. Segmentation
2. Normalization
3. Enhancement
4. Feature Extraction
5. Storing/Verification

In iris image acquisition, an eye image of 320x240 size is obtained at a distance from a B/W CCD camera without any physical contact to the device. The eye is illuminated using near-infrared wavelengths and specular reflections are on the pupil area not to obscure iris regions.

© JGRCS 2010, All Rights Reserved

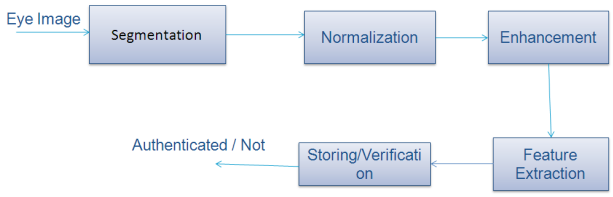


Figure 4: System flow of Iris verification

The eye image is shown in Fig. 5(a) and the iris diameter is above 170 pixels to provide good quality for iris recognition.

A. Segmentation

Iris region is isolated from eye image with the estimate that the shape of iris is circle. First we detect the edges in the iris pattern using Canny edge detection method. The canny edge detector provide the binary image of the given pattern. Using thresholding method we cover inner pupil and outer portion of image then we can get area of pupil , iris .From that we find radious of pupil and iris. From the radious the Circular hough transform gives the center points of iris and pupil. Using center points and radius of iris and pupil we can get segmented iris .

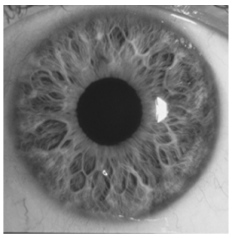


Figure5 (a): Sample eye images

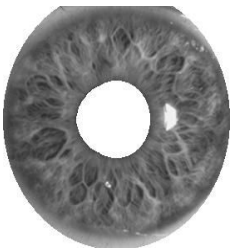


Figure5 (b): Images after iris segmentation.

The segmented Iris pattern is given to the process of normalization and enhancement.

B. Normalization

Eye image captured from different person & different environment may be in different size. So, normalization of irises of different size to same size is need for achieving more accurate recognition. The result of iris normalization is shown in Fig. 5(b) and the size of normalized image is 64X300. Eyelash and eyelid rarely occlude iris region. That's why only iris image data in right side [45°- 315^0] and left side [135^0 - 225^0] are transformed into rectangular coordinate system like Fig. 6(a).

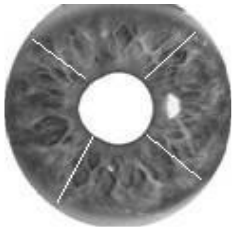


Fig 6(a) - Iris regions to be transformed into polar coordinate system.

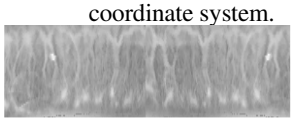


Fig 6(b) - Normalized iris image

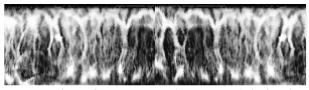


Fig 6(c) - Enhanced iris image.

C. Enhancement

It is necessary to improve the dissimilarity of normalized iris image for iris feature extraction since it has low contrast Fig. 6(b). Histogram stretching method is used obtain well-distributed iris image and the result is shown Fig. 6(c).

D. Iris feature extraction

It is important to analyze the changes of grey values patterns and extract features from iris image. Previous work is used Gabor transform and wavelet transform and In this paper, Cumulative sum based analysis method used to extract features from iris images. Cumulative sums calculated simply and do not need much processing burden.

1) Overall feature extraction processing is as following:

Stepl. Divide normalized iris image into basic cell regions for calculating cumulative sums. (One cell region is a m x n pixels size, and an average grey value is used as a representative value of a basic cell region to calculate the cumulative sum)

Step2. Basic cell regions are grouped in a horizontal direction and in a vertical direction as shown Fig. 3. (Five basic regions are grouped into group)

Step3. Calculate cumulative sums over the each group like equation (2).

Step4. Generate iris feature codes.

The cumulative sums are calculated as follows: Suppose that X1, X2, . .., X5 mean five representative values of each regions within a group.

X' = (X1+X2+...+X5)/5 .(1)

* First calculate the average 5

* Calculate cumulative sum from 0: S0 = 0

* Calculate the other cumulative sums by adding the difference between current value and the average to the previous sum,

i.e., Si = Si±l + (Xi -X) for i = 1,2,..., 5. (2)

© JGRCS 2010, All Rights Reserved

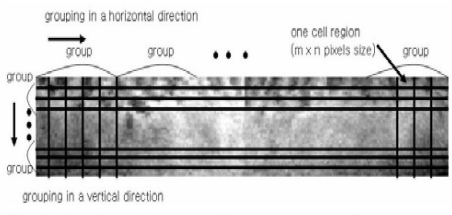


Figure 7: Divide normalized iris image into cell regions and grouping of cell regions.

After calculation cumulative sums, iris codes are generated for each cells using following algorithm after obtaining MAX and MIN values among cumulative sums.

if Si located between MAX and MIN index
if Si on upward slope
set cell's iris_code to "1"
if Si on downward slope
set cell's iris_code to "2"
else
set cell's iris-code to "0"

This algorithm generates iris codes by analyzing the changes of grey values of iris patterns. Upward slope of cumulative sums means that iris pattern may change from darkness to brightness. Downward slop of cumulative sums means the opposite change of upward slope.

E. Verification

In order to calculate the similarity of two iris codes, hamming distance method is used as equation (3) and the lower hamming distance means the higher similarity.

$$HD = \frac{1}{2N}\left[\left(\sum_{i=1}^{N} A_h(i) \oplus B_h(i)\right) + \left(\sum_{i=1}^{N} A_v(i) \oplus B_v(i)\right)\right]$$

here Ah(i) and A,(i) mean enrolled iris codes over the horizontal and vertical direction. And Bh(i) and B,(i) mean new input iris codes over the horizontal and vertical direction. And N is total number of cell .

Experimental Results

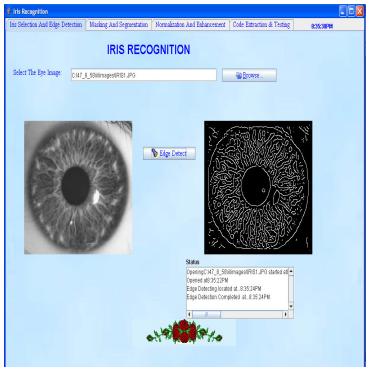


Figure 8: Iris normalization

Figure 8 describes the normalization process of the iris pattern in the Cloud Iris Verification System

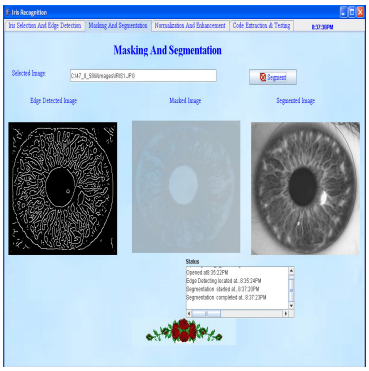


Figure 9 – Masking and SegmentationFig 9 describes the masking and segmentation process of the normalized iris pattern

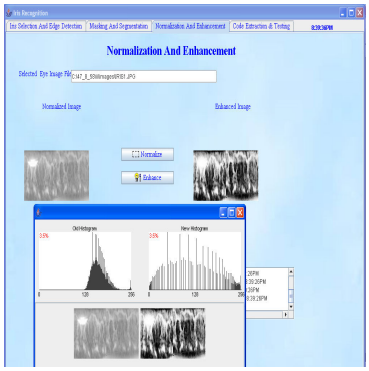


Fig 10 - Enhancement

Figure 10 describes the Enhanced iris image from the segmented iris pattern

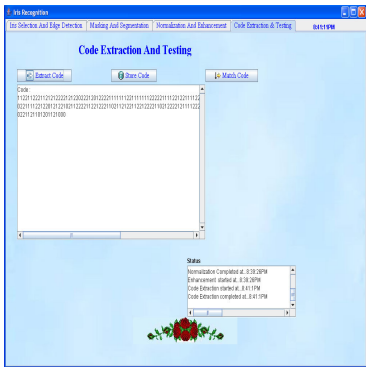


Fig 11 – Code Extraction

Figure 11 describes the unique code of the iris pattern in the CIVS

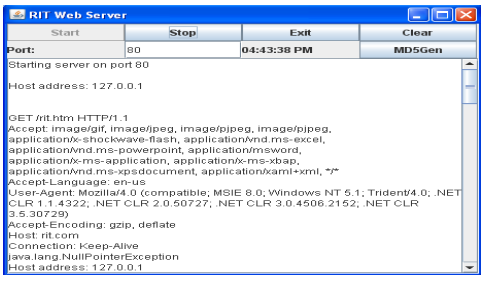


Figure 12 – CIVS Server

© JGRCS 2010, All Rights Reserved

PERFORMANCE ANALYSIS

(4)

r-Rank Correlation
d-differences in Rank
N-Number of Servers

Using the formula (4) Rank correlation is calculated. The Value of r=1.

Eye images for the experiment were acquired through a W CCD camera with two LED lamps around the lens. size of image is 320 x 240 with 8bit grey value. Experimental data are composed of 820 images acquired from 82 individuals and 10 eye images per person (left eye right eye). The performance evaluation of proposed method was measured by the two error rates such as FRR and FAR. The false acceptance rate (FAR) was computed as equation (5) the false rejection rate was computed as equation (6).

$$FAR(\%) = \frac{\#\text{ of false acceptances}}{\#\text{ of total imposter attempts}} \quad (5)$$

$$FRR(\%) = \frac{\#\text{ of false rejections}}{\#\text{ of total authentic attempts}} \quad (6)$$

Figure 13. shows hamming distance distribution for the same persons. Hamming distance values are located between 0 and 30. Figure 14. shows hamming distance distribution for the different persons. Hamming distance values for the imposters are distributed from 25 to 52. xset and y-axis indicate the number of data and hamming distance respectively. Figure 15 shows the FAR/FRR curves according to the hamming distance. False rejection rate is decreased when the hamming distance value is increased false acceptance rate is decreased when the hamming distance value is decreased respectively. So, two error curves have intersection point. By selecting the cross point two error curves as a threshold, two error rates minimized at the same time can be found. By experimental results, the recognition performance of proposed method is 99.0% to 99.2% when the threshold is 26. The experimental results show that the proposed method is a promising and effective approach in iris recognition.

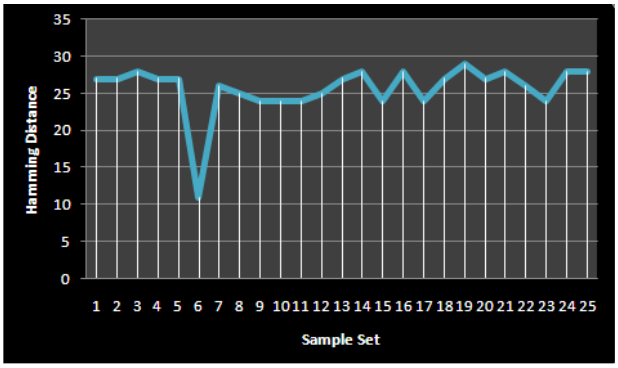


Figure 13. Hamming distance for the same persons

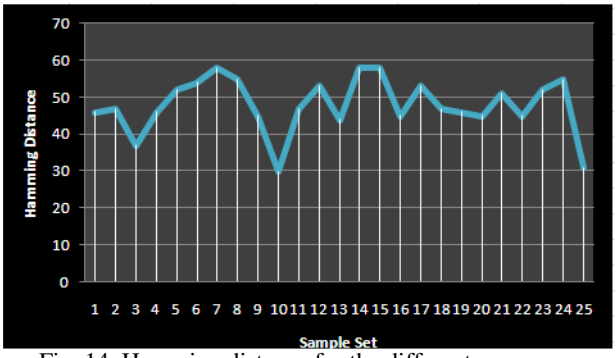
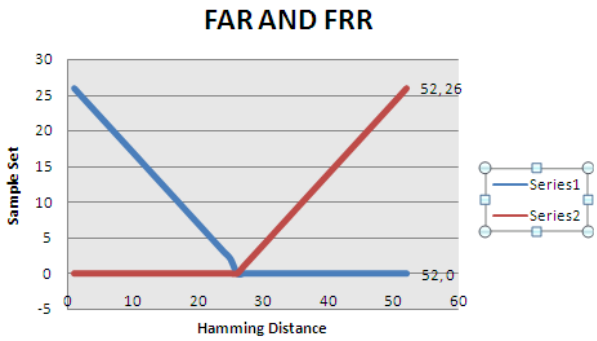


Fig. 14. Hamming distance for the different persons



Series 1 FAR and Series 2 FRR

Fig. 15. FAR/FRR curves according to hamming distance

Persistent service Availability

Persistent service Availability lies between 0 to 1. The relation between Cloud servers is measured it using Rank Correlation.

TABLE 2 : PERSISTENT SERVICE AVAILABILITY

Sl No	Name of the Web page	Persistent service Availability (Rank Correlation)	
		Average Delay Time	Average Speed
1	CIVS	37	17
2	Web Server-1	94	39
3	Web Server-2	101	45

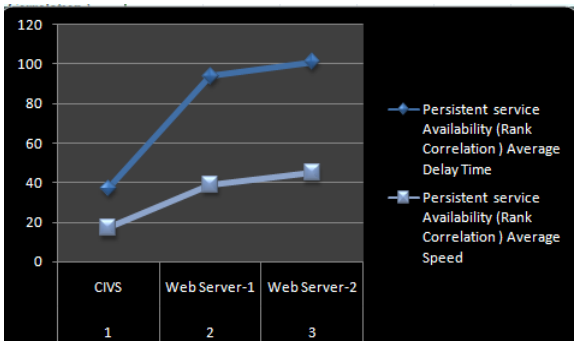


Figure 16 : Evaluation of persistence availability

© JGRCS 2010, All Rights Reserved

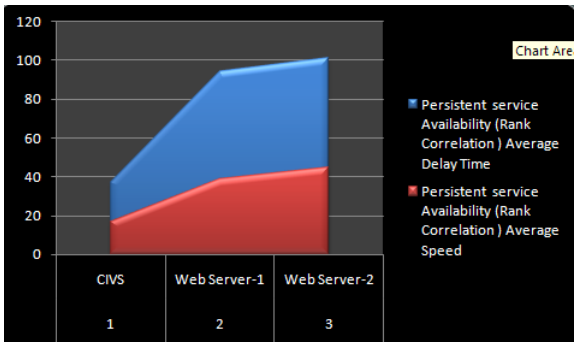


Figure 17 : Evaluation of Persistance service availability

Table 1 shows the Persistent service Availability of various servers.

APPLICATIONS

It can be applied in areas were continual reliable service is required.

Example Cash Transaction, Online Shopping and E-Governance, Web pages are "location aware" and Can only be executed in /data or /system, Any changes on file permissions succeed there.

A recent Survey during November 2009 predicts that around 698 websites have vanished due to improper security features. Using CIVS the security provided increases in large fold.

Another recent event "Chinese hacked PMO computers, says Narayanan" on Tuesday, Jan 19, 2010. Using VWS the security provided to that server is increases in large fold.

CONCLUSION

CIVS server was tested against webs servers with password security in order to rate it. From the analysis result it has been found that CIVS Server stands unique in providing secure service to the user compared to the other web servers. A new mechanism named Iris data security has been introduced to provide increased security. The virtual controller increases the reliability for using disconnected method. The Activity Analyser helps the administrator time to time in knowing about the intrusion caused and its counter measures.

In this paper, we implement the Cloud Verification Server. This method in use iris feature extraction that uses cumulative sum based change analysis. In order to extract iris features, normalized iris image is divided into basic cells. And iris codes of these cells are generated by proposed code generation algorithm, which uses cumulative sums of each cell. Proposed CIVS method is relatively simple and secure against existing methods. And the experimental result show that the proposed approach has a good credit performance Our proposed scheme provides highly reliable and secure service to its clients, It is efficient to a mark of 93.17% comparing others.

REFERENCES

[1] Implementation of a Cloud Data Server (CDS) for Providing Secure Service in E-Business By D.Kesavaraja , R.Balasubramanian And D.Sasireka, International Journal of Database Management Systems (IJDMS),(ISSN: 0975-5705)

[2] Wood, N.M. Orlans, and P.T. Higgins, Biometrics, The McGraw-hill company, Berkeley, California, 2002.

[3] Kronfeld, Gross Antomy and Embryology of the Eye, The Eye, Academic Press, London, 1962.

[4] John G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Trans. On Pattern Analysis and Machine Intelligence, 15(11), pp. 1148- 1161, 1993,

[5] "The Design Of A Generic Intrusion Tolerant Architecture For Web Servers " By Ayda Saidane, Vincent Nicomette, And Yves Deswarte, Member, IEEE ,IEEE transactions on dependable and secure computing, vol. 6, no. 1, january-march 2009

[6] "Data Fusion And Cost Minimization For Intrusion Detection " By Devi Parikh, Student Member, IEEE, and Tsuhan Chen, Fellow, IEEE, IEEE Transactions On Information Forensics And security, vol. 3, no. 3, september 2008

[7] "An Architecture For An Adaptive Intrusion-Tolerant Server "By Alfonso Valdes, Magnus Almgren, Steven Cheung, Yves Deswarte ,Bruno Dutertre, Joshua Levy, Hassen Sadi, Victoria Stavridou, and Tomas E. Uribe

[8] "Graphical Inferences For Multiple Intrusion Detection " By Tung Le , Student Member , IEEE , and Christoforos N.Hadjicostis , Senior Member , IEEE

[9] "Random-Forest-Based Network Intrusion Detection Systems " By Jiong Zhang , Mohammad Zulkernine , and Anwar Haque

[10] William Stallings, "Cryptography and Network Security Principles and Practices", Third Edition, Prentice Hall, 2003.

[11] Java 2: The Complete Reference, Patrick Naughton and Herbert Schildt, Tata McGraw Hill, 1999.

[12] The Java Language Specification, 2nd ed, JamesGosling, Bill Joy, Guy Steele & Gilad Bracha, Sun Microsystems, 2000.

[13] ISS X-Force - www.iss.net/threats/ThreatList.php

[14] CERT - Carnegie Mellon University's Computer Emergency Response Team. www.cert.org/

[15] Boles, W.W. and Boashash, B., "A Human Identification Technique Using Images of the Iris and Wavelet Transform", IEEE Trans. on Signal Processing, 46(4), pp. 1185-1188, 1998.

[16] Li Ma, T. Tan, "Personal Identification Based on Iris Texture Analysis", IEEE Trans. on Pattern Analysis and Machine Intelligence. Vol.25, NO.12, 2003 persons [6] S. Lim, K. Leei, 0. Byeon, and T. Kim, "Efficient Iris Recognition through Improvement of Feature Vector and Classifier", ETRI J. vol. 23, No. 2, pp. 61-70, 2001

[17] Y. Wang, J. Han, "Iris Recognition using Independent Component Analysis", Int. Conf on Machine Learning and Cybernetics, pp. 18-21, 2005.

[18] E.Rydgren et.al. "Iris Features Extraction using wavelet packet", IEEE, ICIP, 2004.

[19] Y. Wang, J. Han, "Iris Recognition Using Support Vector Machines", ISNN, LNCS 3174, PP.622-628, 2004.

[20] R.W. Ives, A.J. Guidry and D.M.Etrer, "Iris Recognition using Histogram Analysis", Signals, System and Computers, 2004.

© JGRCS 2010, All Rights Reserved

AUTHORS

D.Kesavaraja has completed his B.E Degree from the Department of Computer Science and Engineering from Jayaraj Annapackiam CSI College of Engineering, Nazareth, Under Anna University, Chennai in 2005.He has completed his M.E Degree from the Department of computer science and Engineering from Manonmaniam Sundaranar University , Tirunelveli in 2010.He is a co-author of a book titled "Fundamentals of Computing and Programming" ,ISBN 978-81-8472-099-0. He is currently working as a Lecturer at the Department of Computer Science And Engineering, in DrSivanthi Aditanar College of Engineering, Tiruchendur. He has total of five years of Teaching Experience .He has presented papers in many conferences and published three international journals and also felicitated many Guest Lectures. His research interests include Intrusion Detection, Pervasive computing, Parallel Image Processing, Web Development ,Grid and Cloud Computing , Developing Applications of these technologies in Real Time .

D.Sasireka has completed her B.Tech Degree from the Department of Information Technology from, Dr Sivanthi Aditanar College of Engineering, Tiruchendur , Under Anna University, and Chennai in 2008. She is currently pursuing the Masters in Information Technology at Manonmaniam Sundaranar University , Tirunelveli .She is currently working as a Lecturer at the Department of Information Technology in PSN College of Engineering Technology Melathedioor , Tirunelveli. She has published papers in one International Level Journal and many National Level Conferences. Her research interests include Intrusion Detection and Network Security.

D.Jeyabharathi has completed her B.E Degree from the Department of Computer Science And Engineering from, Jayaraj Annapackiam CSI College of Engineering, Nazareth, Under Anna University,Chennai in 2009. She is currently pursuing the Masters in computer science and engineering at Manonmaniam Sundaranar University , Tirunelveli . She is currently working as a Lecturer at the Department of Computer Science And Engineering, in Einstein College of Engineering. Her research interests include Image Processing, Network Security.

© JGRCS 2010, All Rights Reserved