ROBAT-C2: ROBUSTNESS ORIENTED BIOMETRIC AUTHENTICATION TRYOUT ON CLOUD COMPUTING

R.Vijayalakshmi[1], T. Prasath[2], S. Sathiyadevi[3], S. Nagadivya[4], D. Rampriya[5]

[1]*Final Year M.Tech, (CSE), Christ College of Engineering and Technology Pondicherry,* ***viji.ramanidass@gmail.com***
[2]*Final Year M.Tech, (CSE), Christ College of Engineering and Technology Pondicherry,* ***prasath.27101987@gmail.com***
[3] *Final Year M.Tech, (CSE), Christ College of Engineering and Technology Pondicherry,* ***sathiyadevi5@gmail.com***
[4] *Final Year M.Tech, (CSE), Christ College of Engineering and Technology Pondicherry,* ***divyacse2008@gmail.com***
[5] *Final Year M.Tech, (CSE), Christ College of Engineering and Technology Pondicherry,* ***dspriya1021@gmail.com***

Abstract

Broadened service based computing in the cloud environment makes nowadays rapid computations easier. The cloud forms the structure for security and authentication mechanism which provides the privacy equipped cloud and storage that concentrates more on biometric authentication services which enhances the provable security in the persistence environment. In this paper the major focussing area is authentication based on biometric iris recognition which uses security levels based on iris. There are three phases that includes the secure based cloud storage service in the first phase the biometric authentication that uses the morphology identification server (MIS) divides the work path of iris identification at various levels such as segmentation, sectoring, normalization, generates iris code that which matches with the MIS data storage. The second phase the persistent environment provides provable security enhancement in storing the data at different storage medium to extend the service robustness in cloud. The third phase is detecting the dynamic worm in the travelling data via cloud environment and the detection lists the report and that yields the partial decrypted data to the user. The user then decrypts the message to get back the original encrypted file.

Index Terms: *Biometric authentication, persistent cloud storage, dynamic worm detection, security enhancement.*

---------- *** ----------

1. INTRODUCTION

Even though we use our own hard drives to store data and feel that capacity is enough, in some cases the need for the capacity occurs and the present hard disk memory does not satisfy the user at that situation, user need to expand here storage. To do so they involve in upgrading or replacing the drive with a large capacity one, or using an external storage device. The same problem occurs not alone in home drive but also in organization also. To overcome this most of the organization start to use the cloud storage service. Where the memory can be use based on our needs and pay for that and too expand the memory at more needs. The usage of tablets and ultra-books gets increased this driving a tendency that cloud storage not only tempting, but obligatory these devices limited GBs of memory for storage. This limited storage involves in detriment it during the ease and transportability. Cloud provides a logical solution through accessing the connection during the portability. Limitless volume, virtually universal access is some of the essential benefits of cloud data storage. Expanding the storage or upgrading it was the temporary solution where the size odds are not considered and use it for one day need not for longer and there is a risk in it. But in the case of cloud there is not any risk in filling it. Cloud provides higher capacity plan with less cost instead of spending more money in buying a new storage device. To plug a short period essential provisional capacity can added in cloud, and then change to the storage plan without burdened with drives that no extended need. Through the help of internet, cloud connection was made and the data was accessed or shared from anywhere in the world. More efficacy and creative opportunities in work are provided by cloud with the data in the PC.

The security concerns issues related to the cloud storage that focuses on reliability and security. The users of cloud are guaranteed to entrust the data that are stored via internet connectivity. The information that are provided can be accessed from anywhere at anytime.

Ensuring security some combinational techniques that are as follows with primary security features:

- Some complex based authentication security algorithms are used to encode and decode the files.

- The authentication process is required to create log on and log out session.
- The authorization task is ensured to access the information to store in the cloud infrastructure.

Replication of data that is copies of data are stored in different servers in the cloud for the robustness. This helps in retrieving of data as long as one storage server endures.

The current world with the promoting technologies, the need of security rises. The security authentication is focused in different fields such as government, commercial, military and research. In different sectors this system already implemented. But some issues occur on the existing system. Passwords and ID cards are commonly used in the traditional security systems. These are not given unique identification and not reliable for an particular since passwords may be forgotten and ID cards may be lost. To overcome these drawbacks, the biometric technique can be used.

Biometrics is the verification and identification of human sameness. It can be sorted into two classes are Physiological and Behavioural. The physiological characteristics are palm-prints, fingerprints, hand geometry and Iris recognition and Behavioural characteristics are the voice-prints, gesture, signature, etc. which are unique to every person. Iris recognition is best for other biometrics technique because two human's Iris will not be same, even if they are twins. Also the right and left of an individual's Iris differ which paves way for reliability.

A worm is a self-imitating virus that does not revise files but subsist in dynamic memory and reproduce itself. Every time a contaminated computer program is used then Computer virus or Worm can reach to hard disk. Viruses or Worms are shifted among computer systems using various technique; AN active worm are called spiteful software program that spread itself on the Internet to pass on a harms to other computers, These worms consist of "Code-Red" worm in2001 [8], "Slammer" worm in 2003 [9], and "Witty"/"Sasser" worms in 2004 [10]. Normal Worms are produce set of general network traffic. So traditional worms will be easily identifiable using overall traffic of the network .antivirus software is used to clean a worm affected system. but it is not possible to clear if the operating system of a system gets changes by worms. A dynamic Worm is unusual from normal worms because of its capacity to smartly operate its scan traffic volume over time. Dynamic worm activities are unseen and its development is totally maintaining a secret. Normal worm detection process is not possible to sense dynamic worm. So we use unique method called spectrum based analysis method to sense the worm. It contains two techniques namely 1. Power Spectral Density (PSD) 2 Spectral Flatness Measure (SFM) .PSD is a provision of a scan traffic volume and SFM used to separate the dynamic worm from normal worm

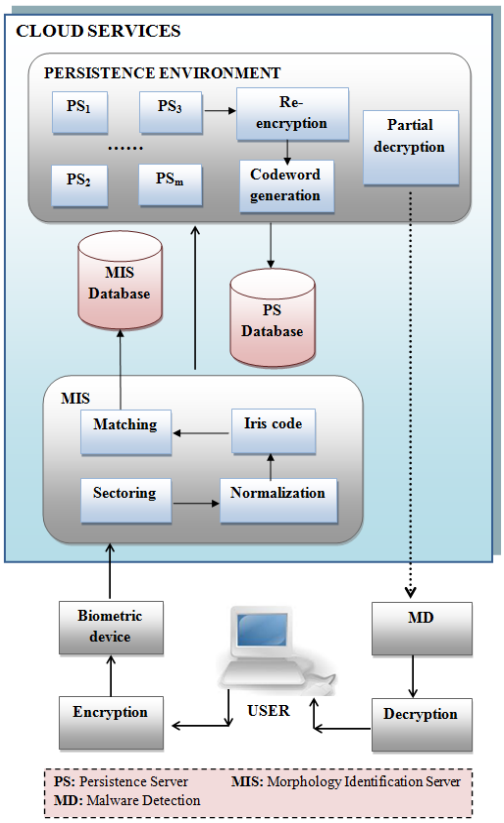

Fig1-: Biometrics Oriented Device authentication and worm detection in Cloud Service.

The above diagram is categorized into three phases. The first phase describes that the biometric device oriented authentication process takes place with the Morphology Identification Server which checks the iris code that matches to authenticate with the existing user and that is stored in the data storage.

The Second phase is the persistence environment that accumulates incoming data and when demand arises the partial decryption takes place.
The third phase enhances the detection of dynamic worm and decrypts the worm free data.

2. MORPHOLOGY IDENTIFICATION SERVER

There are various significant factors that restrict the advancement of Iris Recognition Systems. First, the identification of execution is highly affected by the accuracy

and robustness of iris segmentation. Second, sectoring the iris regions on the right and left sides in different angle based on the iris image. Third, normalization based on sectored iris. Fourth, generating the iris code only for the sectored part of the iris. Finally, the hamming distance method is used to check the similarities between two iris codes. All of these provocation call for the exertion towards developing accuracy, high-precision, robust and time complexity.

2.1 IRIS Segmentation

The eye image is separated into Iris region with the approximation that iris shape is circle. The below equation is Daugman method [1], inner and outer boundary of iris are placed by using the operative integro differential operator.

$$\max_{(r,x_p,y_o)} \left| G_\sigma(r) * \frac{\delta}{\delta r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right| \quad (1)$$

Where,
I(x, y) is the eye image
Gσ(r) is a smoothing function of Gaussian
r is the radius
s is the circle of contour given by x0, y0, r.

The center point of the iris are acquired by using row or column profile method, it using information which the inner boundary (pupil) areas are gloomy than the other iris areas. Iris segmentation result shows the below figure 2.

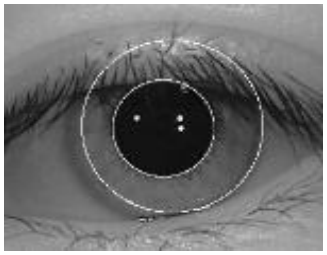

Fig-2: Iris Segmentation

Iris image Normalization processing segmented the iris and enhancement processing to enhance the normalized Iris [2].

2.2 Sectoring

Before normalizing the iris the sectoring is taken place at that particular region. In this paper, sector the iris regions at the angles 20, 40 and 60. After the Normalization stage is based on the sectored iris regions. The left and right side of the A and B regions follows the below figure 3 is best bits of iris regions.

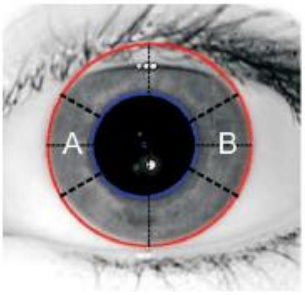

Fig-3: Sectoring

The sectoring is analyzed for different angles 20, 40, and 60 based on the Iris as shown in figure 4.

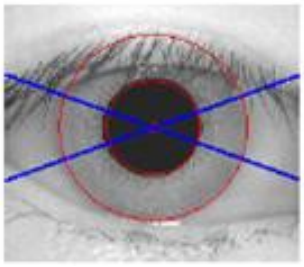

Fig-4: Sectored image at 20 degree

2.3 Normalization

The Daugman's rubber sheet model can applying the sectoring concept.

$$I(x(r, \varphi), y(r \varphi), y(r, \varphi)) \rightarrow I(r, \varphi) \quad (2)$$
$$x(r, \varphi) = (1-r)\, xp(\varphi) + rxi(\varphi) \quad (3)$$
$$y(r, \varphi) = (1-r)\, xp(\varphi) + ryi(\varphi) \quad (4)$$

(x, y) is the eye image
r is the radius
Gσ(r) is a smoothing function of Gaussian
s is the circle of the contour given by y0, x0, r.

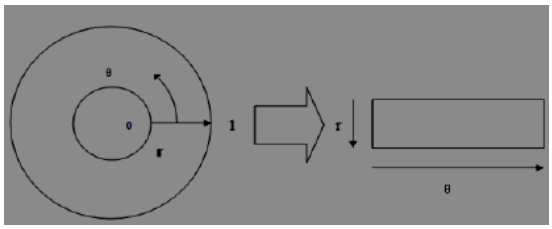

Fig-5: Daugman's rubber sheet model

Where,
φ is ( ),
m denotes the 3n, Here n align from 3, 4, 5…
r denotes the Inner and Outer boundary of iris range.

This denotes the angle of variations respectively. The Normalized Iris image can applying the Daugman's rubber sheet model for sectored regions as shown in below figure 5(a & b). Then the sectored part of the Iris is generating the iris code.

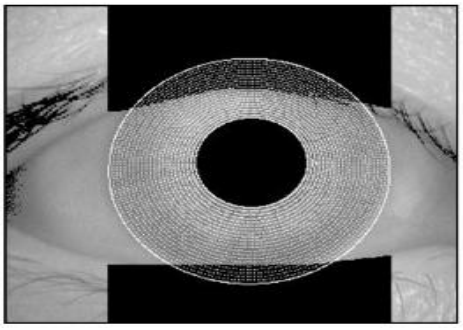

Fig-5(a): Iris region

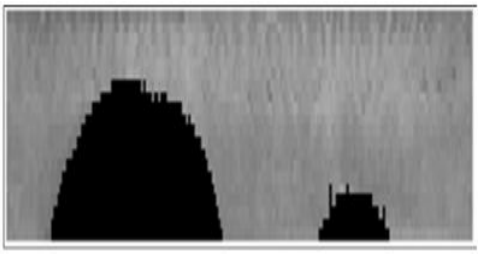

Fig-5(b): Normalization Iris region

2.4 IRIS Code

The given Iris code value is encoded into 256 byte. Each pixel value will be created the unique code. The uniqueness rely of the code rely on the randomness of the Iris pattern & uniqueness of the Iris. The below figure 6 shows Iris Code image.

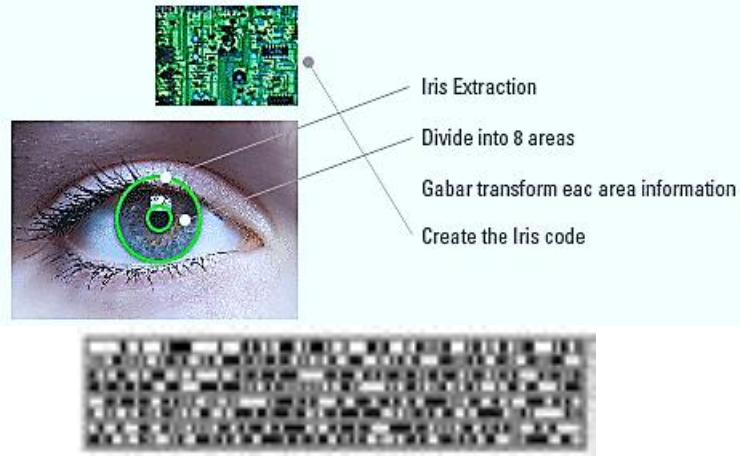

Fig-6: Iris Code

2.5 Matching:

Hamming Distance

In order to calculate the similarity of two iris codes, hamming distance method is used as equation (5) and lower hamming distance means the higher similarity.

$$HD = \frac{1}{2N}\left[\left(\sum_{i=1}^{N} A_h(i) \oplus B_h(i)\right) + \left(\sum_{i=1}^{N} A_v(i) \oplus B_v(i)\right)\right] \quad (5)$$

Where Ah(i) and A,(i) mean enrolled iris codes over the 40 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 and $\oplus$ means the XOR operator defined as equation (6).

$$x \oplus y = \begin{cases} 0 & x = y \\ 1 & x \neq y \end{cases} \quad (6)$$

During Matching the input image is undergone all the above processing steps and the final iris code is generated for 3 sector regions.

$$FAR(\%) = \frac{\#\text{ of false acceptances}}{\#\text{ of total imposter attempts}} \quad (7)$$

$$FRR(\%) = \frac{\#\text{ of false rejections}}{\#\text{ of total authentic attempts}} \quad (8)$$

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 (7) and the false rejection rate was computed as equation (8).

3. PERSISTENCE ENVIRONMENT:

Cloud persistence system was designed in a manner that the message *d* (or) data to be stored was divided into *n* blocks in *m* distributed storage server. In cloud persistence system a threshold proxy re-encryption scheme was introduced to provide a secure data storage [3][4]. Codes over an encrypted message were supported by this scheme. This persistence server independently encodes the given data and performs partial decryption. The general parameter settings are $m=an^c$ where $c \geq 1.5$ and $a > \sqrt{2}$, $m=an^c$ permits the number of storage servers that must be more than the number of chunk of messages. To increase the entire replicas message symbol

directed to storage server the number of storage server allocation was determined. The combination of encrypted message symbols with encoded results is stored in each storage servers because of that increase in size was not possible in the storage server. The replication process improves the robustness of the data and the server allocation helps in replacement of new storage server in the case of faults (or) failure.

3.1 Data Storage

In this phase, user performs data encryption that has to be stock in the cloud persistence system with the Identifier ID and posts it into the arbitrarily elected storage server [6][7]. The storage server that obtains message involves in the corrosion of the message d into n blocks $d_1, d_2 \ldots d_n$. Linear combination of received cipher texts was performed by each storage server and data storage was done with the code word generated. Fewer numbers of n blocks might be received by the storage server so undertake that the value of n is known by the storage servers.

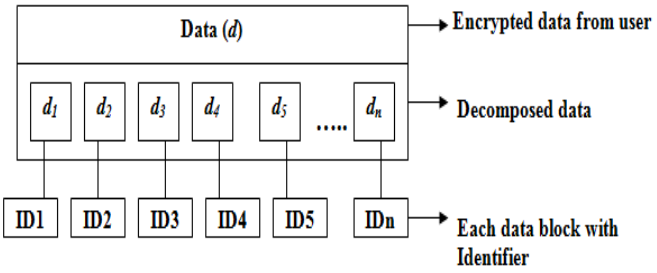

Fig7- : Data decomposition

3.2 Proxy Re-Encryption

The cipher text with the identifier ID by a user was re-encrypted using the secret key provided by the user[4]. Each data blocks decomposed by a server were re-encrypted with the help of provided secret key SK^{ID} of a user. The secret key was distributed to other storage servers to perform code word symbol re-encryption and for lateral recovery appeal by user.

3.3 Data Retrivel

Data stored by the user was retrieved by sending a request to the storage server. An authentication procedure was accomplished by a storage server after receiving the request from the user. Then the code word symbols from the randomly chosen servers are gathered by a storage server and partial decryption was performed using the secret key. Then the partly decrypted code word symbols are pooled to obtain the original message M.

3.4 System Recuperating

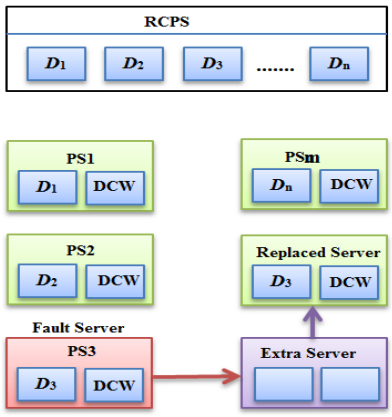

Fig8-: System Recovery

RCPS: Randomly Chosen Persistence Server.
D1, D2, D3, Dn: re-encrypted data.
PS: Persistence Server.
DCW: Double encrypted Code Word.

An inclusion of novel server was done when a storage server under goes failure situation. Here m available storage servers are queries by new storage server and received code word symbols are combined by the novel server and store in it.

4. Warm Detection

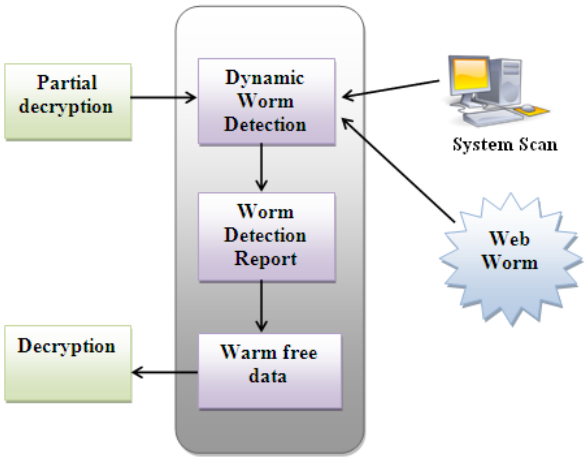

Fig9-: Dynamic worm detection

Fig:9 describes the worm detection is the third phase of the biometric device architecture which the dynamic worm can be detected in two basic forms are by scanning the system the detection of worm can be monitored and while accessing the web may detect some ananymous worm detection is made and named as web worm.

4.1 Dynamic Worm

The Dynamic worm performance is to be hidden and its action is absolutely kept secret. It is to influence the systems but won't diminish the traffic level. First, the current network in the Dynamic worm searches all the Internet Protocol then it classifies the number of worm affected systems, number of protected systems, number of worm affected systems & number of vulnerable systems. The Discrete Mathematical model is used to detect the worm and control the worm is based on special technique called spectrum and C-worm focuses only the vulnerable systems. In this paper uses the power spectral density (psd) allocation of the scan traffic volume and its equivalent spectral flatness measure (sfm) to differentiate the C-Worm traffic from surrounding traffic

4.2 Spectrum Based Analysis

The activities of the worms contrast in the time sequence is used to find out by Spectrum method and Its activities watchful also. To recognize the activities of the worms we apply Spectrum method. Once we find the behaviour is modified, the system will be aware to identify the worm and we could capable to find whether the worm is static or dynamic activities. Detecting based on spectrum that uses the reachable destination count which contains the targeted IP addresses of destination are launched and scans when the propagation of worm. There are two way which the worm can then be propagated they are dynamic worm propagation and static propagation either of this can propagate. These may be spread across the web hosts, routers, and firewalls and other gateways. Monitoring the guarded traffics and responsible to monitor and exposing to the admin. It is then the responsible for the admin to take over the ride on the received traffic logs and the detection is made on the worm attacks.

4.3 Power Spectral Density (PSD)

Use the allocation of PSD and its corresponding SFM of the scan traffic to identify the dynamic Worm spread in the Frequency domain. Convert data from the time domain into the frequency domain to find the PSD allocation for worm discovery data. The power of a time series is distributed in the frequency domain is described by PSD. The time series be in contact to alter in the number of worm occurrence that aggressively carry out scans over time.

4.4 Spectral Flatness Measure (SFM)

SFM used to categorize the scan traffic of the dynamic Worm from the ordinary worm scan traffic to compute the flatness of the PSD. ordinary worm scan traffic does not focus at any particular frequency and some frequent incidence are presents here that are not reason for its random dynamics .dynamic Worm monitor the port-scan traffic details, it will be tough for the dynamic Worm to create the SFM related to the background traffic. Closed-loop control nature of dynamic worm is the reason for the small value the SFM. It can describe abnormality performance of the worm in certain range of frequencies.

CONCLUSION

In the featured based computing environment the cloud plays the vital role to take over the evolutionary storage models that enhances the security based computation make the strengthen services. The biometric strategy that enriches the provable security enhancement in cloud storage with the iris recognition acts as the primary authentication medium to perceive the strong verification service. The analysis about the morphology identification server that checks with input iris by different levels and makes sure there is a match with the existing iris and provide authorized access. The persistent environment that works with the different location based stored servers that communicate with the persistent storage server to exchange information. While the travelling of data via cloud storage takes place the detection of dynamic worm and checks if any detected worm exists and reports the worm details. The partial decryption takes place and then generates the worm list. Finally the decryption is implemented by the user to get the novel message via globally connected cloud service.

REFERENCES

[1]. J. Daugman, ―How iris recognition works,‖ IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 21–30, Jan. 2004.
[2]. Jong-Gook ko, Yeon-Hee Gil and Jang-Hee Yoo. "Iris Recognition using Cumulative SUM based change Analysis", IPACS 2006.
[3]. A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Decen-tralized Erasure Codes for Distributed Networked Storage," IEEE Trans. Information Theory, vol. 52, no. 6 pp. 2809-2816, June 2006.
[4]. M. Mambo and E. Okamoto, "Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts," IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, vol. E80-A, no. 1, pp. 54-63, 1997.
[5]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.
[6]. P. Druschel and A. Rowstron, "PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility," Proc. Eighth

Workshop Hot Topics in Operating System (HotOS VIII), pp. 75-80, 2001.
[7]. H.-Y. Lin andW.-G. Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.
[8]. D. Moore, C. Shannon, and J. Brown, "Code-Red: A Case Study on the Spread and Victims of an InternetWorm," Proc. Second Internet Measurement Workshop (IMW), Nov. 2002.
[9]. D. Moore, V. Paxson, and S. Savage, "Inside the Slammer Worm," Proc. IEEE Magazine of Security and Privacy, July 2003.
[10]. CERT, CERT/CC Advisories, http://www.cert.org/advisories/,2010.
[11]. Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao, Fellow, IEEE "Modeling and Detection of Camouflaging Worm" MAY/JUNE 2011.
[12]. Yellamandaiah Gogula1, E.Jhansi Rani2 "Paradigmatic and Exploration of Blind Worm" Nalanda Institute of Engineering & Technology, to JNTUK, Kakinada, A.P., India 2012.

BIOGRAPHIES

Ms. R. Vijayalakshmi pursuing my Post Graduation Final Year M. Tech (CSE) in Christ college of Engineering and Technology, Pondicherry University, Pondicherry. Completed Under graduation (M.C.A) at Pondicherry Engineering College, Pondicherry. Pondicherry University, Pondicherry.

Mr. T. Prasath pursuing my Post Graduation Final Year M.Tech (CSE) in Christ college of Engineering and Technology, Pondicherry University, Pondicherry. Completed Under Graduation (B.E.) at I.F.E.T College of Engineering, Gangrampalayam, Villupuram. Anna University Affiliated.

Ms. S. Sathiyadevi pursuing my Post Graduation Final Year M. Tech (CSE) in Christ college of Engineering and Technology, Pondicherry University, Pondicherry. Completed Under graduation (M.C.A) at Rajivi Gandhi College of Engineering and Technology, Pondicherry, Pondicherry University, Pondicherry.

Mrs. S. Nagadivya pursuing my Post Graduation Final Year M. Tech (CSE) in Christ college of Engineering and Technology, Pondicherry University, Pondicherry. Completed Under graduation (B.E.) at Paavai Engineering College, Namakal, pachal. Anna University Affiliated.

Mrs. D. Rampriya pursuing my Post Graduation Final Year M. Tech (CSE) in Christ college of Engineering and Technology, Pondicherry University, Pondicherry. Completed Under Graduation (B.E.) at A.V.C Engineering College, Mannampandal, Mayiladuthurai. Anna University Affiliated.