SECURED SMART SYSTEM DESING IN PERVASIVE COMPUTING ENVIRONMENT USING VCS

M Varaprasad Rao[1] and Prof N Ch Bharta Chryulu[2]

[1]Dept of CSE, Anurag Group of Institutions, Hyderabad,India - 88
[2]Dept of Statistics, Collegeof Science, Osmania University-7

ABSTRACT

Ubiquitous Computing uses mobile phones or tiny devices for application development with sensors embedded in mobile phones. The information generated by these devices is a big task in collection and storage. For further, the data transmission to the intended destination is delay tolerant. In this paper, we made an attempt to propose a new security algorithm for providing security to Pervasive Computing Environment (PCE) system using Public-key Encryption (PKE) algorithm, Biometric Security (BS) algorithm and Visual Cryptography Scheme (VCS) algorithm. In the proposed PCE monitoring system it automates various home appliances using VCS and also provides security against intrusion using Zigbee IEEE 802.15.4 based Sensor Network, GSM and Wi-Fi networks are embedded through a standard Home gateway.

KEYWORDS

GSM, WI-Fi, Zigbee, Context-aware, Smart Sensor, and Pervasive Computing Environment, Public-Key Encryption, Visual Cryptography Scheme and MMS.

1. INTRODUCTION

Many approaches to design the user interfaces such as Interaction Design, User Experience Design (UX), Interactive Systems Design, Cognitive Ergonomics, Man-Machine Interface (MMI), User Interface Design (UI), Human Factors, Cognitive Task Design, Information Architecture (IA), Software Product Design, Usability Engineering, User-Centered Design (UCD) and Computer Supported Collaborative Work (CSCW). The PCE are getting saturated with computing and communication capability, and integrated with human users. The researchers proposed number of security systems based on new technologies such as GSM (Global System for Mobile Communication)[1], GPRS (General Packet Radio Service), Internet, Ubiquitous sensor networks and Microcontroller unit and ZigBee sensor network[5]. The PCE created by the smart Sensors [3], wireless networks and context-aware routing protocol for wireless sensor networks. Each smart Sensor node should have multipath routing protocol to automatically establish the wireless networks between Smart Nodes. This paper introduces the pervasive computing based smart home monitoring system's using VCS design; that provides secure smart services to users and demonstrates its implementation using a real time environment.

The general Biometric system [3-5] is described in figure 1. As its foresights are Authentication has to be transparent, Trusted third party may not be available, Traditional key based systems will not scale well, Trust based models work well with devices and agents, and Trust is not well defined for human user. The advantages of biometrics are Uniqueness, No need to remember passwords or carry tokens, Biometrics cannot be lost, stolen or forgotten, More secure than a long

password, Solves repudiation problem, and Not susceptible to traditional attacks. The issues are Biometrics is secure but not secret, permanently associated with user, used across multiple applications, and can be covertly captured. Examples for Biometrics are 1. Physical Biometrics – Fingerprint, Hand Geometry Iris patterns. 2. Behavioral Biometrics – Handwriting, Signature, Speech, Gait. 3. Chemical/Biological Biometrics – Perspiration, Skin composition (spectroscopy). The Hashing technique is implemented using Biometric as shown in figure2.

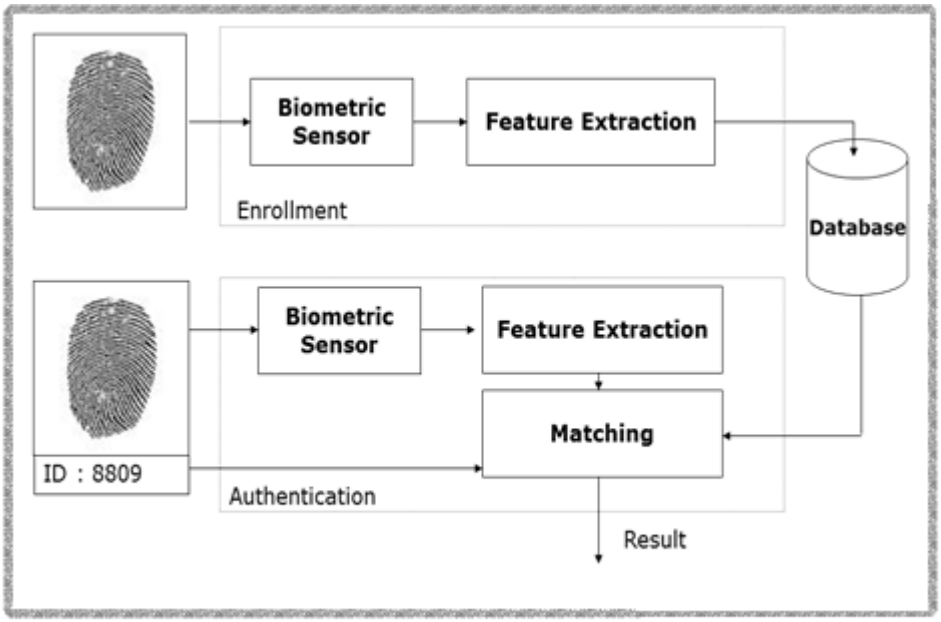

Figure 1: General Biometric System

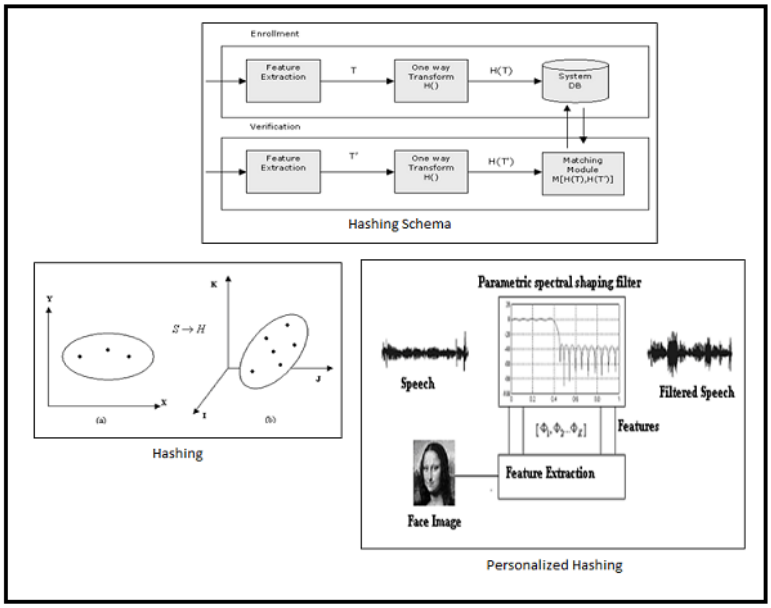

Figure 2: Biometric Hashing

Now a days mobile computing with tiny devices has been explored very much rapidly [10–15]. The pollution monitoring application using Cell-Phone-based Sensor Network (CPSN) developed

in [16] uses short-range communication outlets such as Wi-Fi or Bluetooth. In this paper, we consider the same CPSN architecture as of [16] shown in following Figure 3.

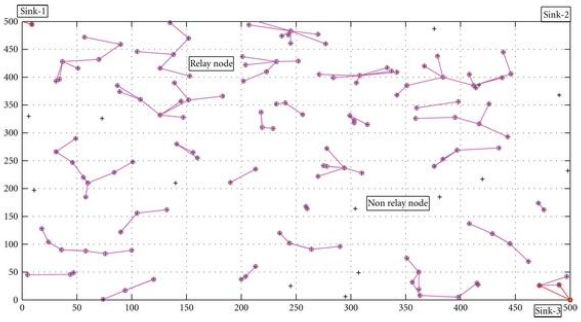

Figure 3: Cell-phone-based sensor network.

VCS is a method for distributing a secret among a group of participants. Each Participant is given a share of the secret. The secret can only be reconstructed when the shares are combined together. Any individual participant cannot recover the secret on his/her own. In secret sharing scheme, let there are 'n' participants. Each participant gets a share in such a way that any group of 't' or more participants can together reconstruct the secret but no group of less than 't' participants can recover the secret. Such a system is called a (t, n) – threshold scheme, where 't' is the threshold. In (t, n) visual cryptographic schemes, a secret image (text or picture) is encrypted into 'n' shares, which are distributed among 'n' participants. The image cannot be decoded from any (t–1) or fewer shares but any't' or more participants can together decode it visually, without using any complex decoding mechanism shown in following figure 4. Naor and Shamir [22] first proposed the concept of visual cryptography in the open literature in 1994.

In this proposal, an image consisting of text, drawings etc. are encrypted and the resultant into two images. These images are given to two different parties as shares. Decryption is possible only when having both of them together. These shares are stored on transparencies and the process of decryption begins with stacking these two transparencies together on the overhead projector. In 1995, Blakely introduced the concept of Visual Cryptography Schemes (VCS) by considering each share is a plane and the secret is the point at which three shares intersect. Two shares out of three are insufficient to determine the secret. This scheme is less efficient than Shamir's scheme because the shares are 't' times larger where 't' is threshold.

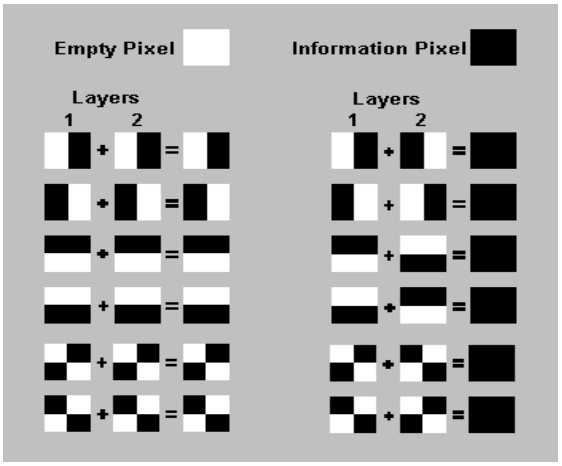

Figure 4: VCS image

The Existing System

There are many definitions available in the literature.

1. Describes a system using Internet, GSM and Speech Recognition. In this system the home gateway is connected via Internet and it needs a Personal Computer (PC). To work with PC for longer time is very hard and it consumes power.

2. Describes a Java enabled mobile system. The research proposes an embedded home server but it is required an Internet connectivity for GPRS. The mobile systems are directly connected to processors via cables; this causes increasing the cost and also required typical installation process. Once this system is installed successfully then it becomes permanent network, and it is not easy to change the geographical location from one to other place.

3. Describes a Bluetooth system, it consists of a primary controller and sub-controllers, these sub-controller are enabled by Bluetooth. Every home applicance is directly connected to a local sub-controller. The home devices communicate with their corresponding sub-controller using wired communications. The communication is done sub-controller to primary controller via wireless communications. It is mandatory that evry home appliance is directly connected to a Bluetooth module.

4. The Biometric describes as; it is secure but not secret, permanently associated with user, used across multiple applications, and can be covertly captured. The types of circumventions may be Denial of service attacks, Fake biometrics attack, Replay and Spoof attacks, Trojan horse attacks, Back end attacks and Collusion & Coercion**.**

Features of the Proposed System

The proposed system is a combination of Internet, GSM, BAN and Zigbee. The connection and communication of sensors is done by Zigbee and to cover these sensors of a large space is done through GSM. The proposed system provides reliable, secure, and anywhere access. To transmitting the information to control panel the sensors uses wireless Zigbee. The control panel controls the operation of this system and it acts like a gateway of home. This model uses the wireless controlling methods such as, GSM Networks, Internet, Zigbee Sensor Network. It also provides confidential and authentication credentials through VCS to maintain secure and secrecy by a three step procedure explained in the proposed algorithm.

2. SYSTEM ARCHITECTURE

The following figure 5 explains about conceptual design of pervasive computing high secured home system. The network has low speed data and high speed data rate; ZigBee is used for low speed data and Wi-Fi is used for high speed data rate. A home gateway is used to provide interoperability between the heterogeneous Zigbee and Wi-Fi networks. It also provides local and remote control, and monitoring over the home's devices. Remote users can access the system using the Internet. The remote user's can do communicates the data in the form of cryptographic secret sharing scheme via MMS over an Internet until they reach the home network. Then the PCE uses wireless transmission using the homes Wi-Fi network to the Home Gateway.

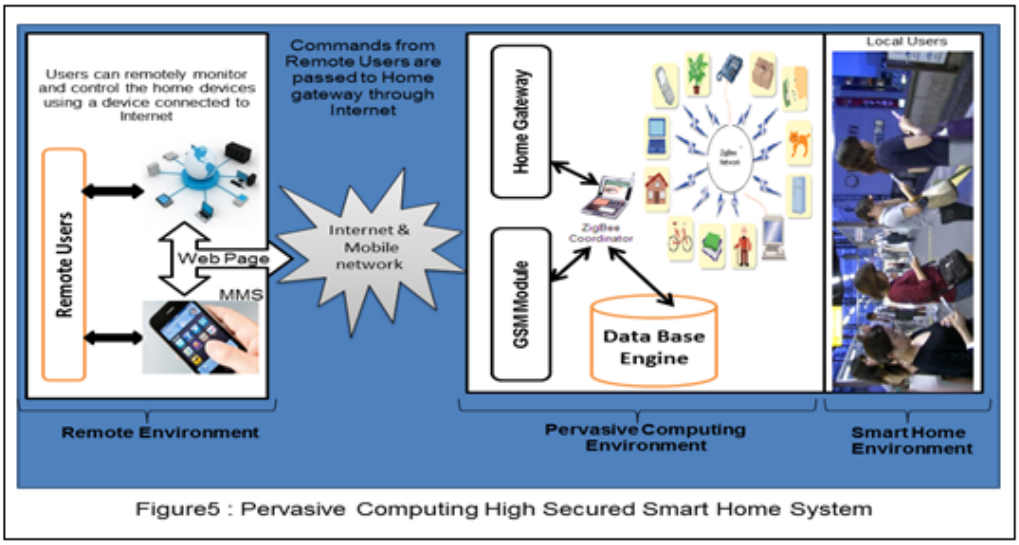

Figure5 : Pervasive Computing High Secured Smart Home System

3. SYSTEM IMPLEMENTATION

As depicted above the PCE based smart home system is implemented for the perceiving and control of household devices. To facilitate high data rate a Wi-Fi network is implemented in connect with PCE devices. The interoperability is provided via home gateway. The gateway provides an interface to user to access local and remote networks. The existing system PCE provided security and safety of the smart home environment. To demonstrate the feasibility and effectiveness of the proposed system for smart devices, a light switch, smart fan, smart sensors, GSM networks and ZigBee remote control system have been developed and integrated with the smart home automation system.

Security

The privacy is very less in the existing home automation system. So we proposed an algorithm Smart Secure Hash Algorithm (SSHA) for Smart Home System using by pervasive computing technologies.

Smart Secure Hash Algorithm

Security is considered as a major issue when it comes to a smart home system with the pervasive computing environment. The proposed algorithm Smart Secure Hash Algorithm (SSHA) used in smart home system and it works as follows:

1. Start the Digital Door Lock System.
2. Use the physical biometric measurement (Fingerprint or Iris pattern or Hand Geometry) to read the data/image of a secured person through Smart Sensor.
3. The captured Biometric image will now check and match the image which is already stored in the database engine.
4. If the image matches with the database image then

    a. Obtain SMS based one time password/random number to mobile phone from an authorized person. (Confidentiality)

b. The database engine now will combine that captured biometric image and the one time password and construct a (2, n) VCS data by using SHA, Biometrics security algorithm and Visual Cryptography Secret Sharing Scheme. (Authentication)
c. The constructed (2, n) VCS code is now sent to the database and compared with the image of database. (Authentication)
d. If it matches then
   The door will be opened
   else
   The error message will be displayed.

Else
The error message will be displayed.

5. If the Digital Door opens then all Smart Sensors and GSM module will be activated; and will be allowed to control the home appliances of Pervasive Computing Environment. Otherwise the defect sensor determines that who is not an authorized person.
6. Once GSM system is activated a customized message will be sent to all the connected users of the database. For example, "Mark Weiser is opened the door at 6.30 pm"
7. If the person entered inside home is not secured then a hidden camera is activated by human defect sensors, it captures a MMS image and sent the same to the connected database users. Immediately the secured user will have to lock the door remotely by availing the SMS service.

4. CONCLUSION

In this paper, we made an attempt to propose a new security algorithm for providing confidentiality and authentication credentials in Pervasive Computing Environment (PCE) system using Public-key Encryption (PKE) algorithm, Biometric Security (BS) algorithm and Visual Cryptography Scheme (VCS) algorithm. In the proposed PCE monitoring system it automates various home appliances using VCS and also provides security against intrusion using Zigbee IEEE 802.15.4 based Sensor Network, GSM and Wi-Fi networks are embedded through a standard Home gateway.

5. REFERENCES

1. Bares Yuksekkaya, M. Bilgehan Tosun, M. Kaan Ozcan and Ali Ziya Alkar. "A GSM, Internet and Speech Controlled Wireless Interactive Home Automation System" IEEE Transactions on Consumer Electronics, Vol.52 No. 3, pp: 837-843, 2006.
2. M. Van Der Werff, X. GUI and W.L. Xu. "A Mobile-Based Home Automation System" 2nd International conference on mobile technology, Applications and systems. Pp 1-5,2005.
3. N. Sriskanthan, F. Tan and A. Karande, "Bluetooth based home automation system", Microprocessors and Microsystems, Vol. 26, no. 6, pp. 281-289, 2002.
4. H. Ardam and I. Coskun, "A remote control for home and office appliances by telephone", IEEE Transactions on Consumer Electronics, Vol. 44, no. 4, pp. 1291-1297, 1998.
5. Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu,"A ZigBee Based Home Automation System", IEEE Transactions on Consumer Electronics, Vol. 55, No. 2, MAY 2009
6. Minal S.Khandare,Anjali Mahajan " Mobile Monitoring System For Smart Home",3rd International conference on Emerging Trends in Engineering and Technology.IEEE 2010

7. Ventylees Raj.S / International Journal of Engineering Science and Technology (IJEST) ISSN : 0975-5462 Vol. 4 No.11 November 2012 4668
8. Joseph. B. Kruskal,"On the Shortest Spanning Subtree of a Graph and the Traveling Salesman Problem," In Proceeding of the American Mathematical Society, Vol. 7, no. 1, pp. 48–50, Feb.1956.
9. Naeem Jan, Chankil Lee, Saeed Iqbal, "Implementation of Zigbee-GSM based Home Security Monitoring and Remote Control", 2011 IEEE.
10. T. Abdelzaher, Y. Anokwa, P. Boda et al., "Mobiscopes for human spaces," IEEE Pervasive Computing, vol. 6, no. 2, pp. 20–29, 2007. View at Publisher · View at Google Scholar · View at Scopus
11. S. Eisenman, N. Lane, E. Miluzzo, R. Peterson, G. Ahn, and A. Campbell, "Metrosense project: people-centric sensing at scale," in Proceedings of the 1st Workshop on World-Sensor-Web (WSW'06), Citeseer, Boulder, Colo, USA, 2006.
12. S. C. Hu, Y. C. Wang, C. Y. Huang, and Y. C. Tseng, "A vehicular wireless sensor network for CO2 monitoring," in Proceedings of the IEEE Sensors Conference (SENSORS'09), pp. 1498–1501, Christchurch, New Zealand, October 2009. View at Publisher · View at Google Scholar · View at Scopus
13. B. Hull, V. Bychkovsky, Y. Zhang et al., "CarTel: a distributed mobile sensor computing system," in Proceedings of the 4th International Conference on Embedded Networked Sensor Systems (SenSys'06:), pp. 125–138, November 2006. View at Publisher · View at Google Scholar · View at Scopus
14. U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi, "Mobeyes: smart mobs for urban monitoring with a vehicular sensor network," IEEE Wireless Communications, vol. 13, no. 5, pp. 52–57, 2006. View at Publisher · View at Google Scholar · View at Scopus
15. P. Mohan, V. Padmanabhan, and R. Ramjee, "Nericell: rich monitoring of road and traffic conditions using mobile smartphones," in Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems, pp. 323–336, 2008.
16. D. Chander, B. Jagyasi, U. B. Desai, and S. N. Merchant, "Spatio-temporally adaptive waiting time for cell phone sensor networks," International Journal of Distributed Sensor Networks, vol. 2011, Article ID 962476, 21 pages, 2011. View at Publisher · View at Google Scholar · View at Scopus
17. M. B. Shah, S. N. Merchant, and U. B. Desai "Human-Mobility-Based Sensor Context-Aware Routing Protocol for Delay-Tolerant Data Gathering in Multi-Sink Cell-Phone-Based Sensor", International Journal of Distributed Sensor Networks, Volume 2012 (2012), Article ID 785984, 19 pages, doi:10.1155/2012/785984
18. Adhikari A, Bose M, 2004, "A new visual cryptographic scheme using Latin squares", IEICE Trans Fund E, Vol.87, pp.1998-2002.
19. Adhikari A, Bose M, Kumar D, Roy B, 2005, "Applications of PBIBD's in developing visual cryptographic schemes", ISI Technical report No: ASD/2005/11.
20. Atenson G, Blundo C, de Santis, Stinson D, 1996, "Visual cryptography for general access structures", Information and Computation, Vol.129 (2), pp.86-106
21. Atenson G, Blundo C, de Santis, Stinson D, 1999, "Construction and bounds for Visual cryptography", Theoretical Computer science, Vol.250, pp.143-161
22. Noar M, Shamir A, 1994, "Visual cryptography", Eurocrypt'94, Springer-Verlog, Berlin, pp.1-12.
23. M Varaprasd Rao, A Damodaram, N Ch Bhrta Chryulu "Algorithm for clustering with Intrusion Detection using Modified & Hashed K-means algorithms"; CSIA12.
24. INKA research group. INKA research group "Information and Communication Systems". [Online]. http://inka.htw-berlin.de/
25. http://oracle.com/Java APIs (2012).
26. MIT Project Oxygen. http://oxygen.lcs.mit.edu/videometaglue.html
27. CMU Project Aura. http://www-2.cs.cmu.edu/ aura/.
28. IBM Planet Blue, http://researchweb.watson.ibm.com/compsci/planetblue.html
29. http://www.google.co.in/search?q=pervasive+computing+devices&hl=en&tbo=u&tbm=isch&source=univ&sa=X&ei=LwUUbrJLYK0rAeV5oHIBw&sqi=2&ved=0CCwQsAQ&biw=1024&bih=629