International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 5, Issue 2, February 2016 **ISSN 2319 - 4847**

Securing a Smart Home Network using Voice Biometric

Oinam Joymala[1] , Neha Khare[2]

[1] MTech. Final Year, Computer Science - Software Engineering, BBD University, Lucknow(U.P.), India

[2] Assistant Professor, Computer Science - Software Engineering, BBD University, Lucknow(U.P.), India

ABSTRACT

The emerging generation of Wireless Sensor Networks, is the Internet of Things. This system is linking physical objects, directly to the Internet using microcontrollers or microprocessors. Visualizing, the next generation internet, the Internet of Things (IoT) provides the infrastructure of pervasive wireless sensing and identification systems with billions of uniquely identifiable intelligent devices to form a ubiquitous environment. The World Wide Web provides great opportunities for data collection and analysis, as well as, for interoperability of objects, that cannot be connected to the same local area network. This network of devices also known as ubiquitous computing, however, poses a serious question of security in such a large number of devices. This paper focuses on the security aspect and a viable method of providing secured access and operation to the users, in such kind of a network as defined. A biometric approach based on Voice Recognition and Speech Recognition is suggested which forms a dual layer of security and authentication for each user, the first for the identification of the user to belong to the network and the other for accessing the various devices.

Keywords: Internet of Things, Sensor Networks, Pervasive Computing, Biometric, Voice Recognition.

1. INTRODUCTION

Visualizing, the next generation internet, the Internet of Things (IoT) provides the concept of pervasive wireless sensing and identification systems with billions of uniquely identifiable intelligent devices to form a ubiquitous environment, which can stay connected through different mediums seamlessly. The dynamic nature of pervasive network access must be orchestrated with an architecture including the network, accessibility, security and preservance. The pervasive network access architecture needs to have an exhaustive list of configuration options, network/endpoint device support, and integration choices in order to accomplish an array of dissimilar users, devices and their interoperability. Pervasive network access dynamicity, calls for an extensive deployment, configuration and policy options that can be easily administered and centrally managed. These needs, request an extremely secure environment for a pervasive network to be ensued. While developing such kind of an environment, the focus has been on implementation, and not on other factors, such as security of the varied users in an ad hoc network. The interconnections within a network remain prone to an unauthorized access due to lack of a proper and authentic security measure. The traditional key based method has not been found much of use in likes of, such kind of an environment. In this paper biometric based security architecture has been proposed which considers voice as a choice of the biometric among a number of other biometrics.

2. RELATED WORK

Relatively very little work has been done in the area of security for pervasive computing environment. The developers have been keener on developing on pervasive computing architecture but the security has been largely overlooked, resulting in key based methods being used largely. If we have to imagine a world where everything is connected to the user who uses it, it is required to provide a secure access method so as to isolate the users from each other as well as to provide a secured access of the devices. The current discussion brings out some methods and research which has been carried out earlier seeking the security aspects of the pervasive networks, body area network or internet of things in general. In M. Manaet. al [1], a trust key management scheme for wireless body area network is proposed, a solution to achieve link layer encryption. In the TinySec approach, packets are encrypted by a group key shared among biosensors. The group key is programmed into every sensor before the sensor network is deployed. If one biosensor discloses the key or it acts as an attacker, all the information in the BAN will be disclosed. The authors have also suggested a Hardware Encryption method, as an alternative approach of TinySec. In this approach, the base station shares the encryption key with every biosensor and only the base station can decrypt the traffic. The base station thus, collects data from the whole network and acts as a gateway to other networks. Therefore, it can be considered as a single point of failure of the network. If an adversary mounts several DoS attacks, the whole WSN will collapse. Another drawback of this method is that hardware encryption is highly dependent on the specific platform, being used. Q. Huang et. al [5], D. J. Malan et. al [6], and S. Zhu[8], have predominantly discussed about a new approach in their research works, the

Elliptic curve cryptography, which is a public-key cryptography approach based on the algebraic structure of elliptic curves over finite fields. D.J.Malan [6] has discussed the use of this technique in wireless sensor networks. Although it was, feasible for sensor nodes, its energy requirements are still in the orders of higher magnitude as compared to those of the symmetric cryptosystems. For example, some works are considered as costly due to high processing requirements. Some symmetric key distribution techniques require pre-deployment and adjust the topology when the network changes, which causes high computation cost because the topology of the network changes frequently. S. Cherukuriet. al [9], have suggested a Biometric system. The mechanism adopts the error-correcting codes and multiple biometrics to secure the key. Compared with the traditional asymmetric key algorithms, this technique can reduce the cost of computation and communication.
In this paper, no implementation details are given. The authors proposed a biometric based distributed key management approach, but only system architecture is given without detail experiments on physiological signals.

3. THE PROBLEM STATEMENT

This section formally states the problem statement and highlights some key issues related to security in a pervasive network environment.
Traditionally, while developing such kind of an environment, the focus has been on implementation and not on other factors such as security of the different users in an ad hoc network. The interconnections within a network as such be prone to an unauthorized access due to lack of a proper and authentic security measure. The traditional key based method has not been found much of use in such kind of an environment. The key issues in a pervasive network environment can be summarized below:

1. The network architecture: The network architecture should be the one feasible to construct and cost-effective. Traditionally RFID, GPRS, GSM based modules have been used. It can be extended to latest technologies like ZigBee etc.
2. The security aspect: The security of a pervasive network is the key to its successful implementation. Strict measures need to be developed to save ones` home network from intruders.
3. Interoperability: Another key issue is the interoperability of the devices connected and the priority of their operations when a series of commands are in the queue.

4. PROPOSED MODEL

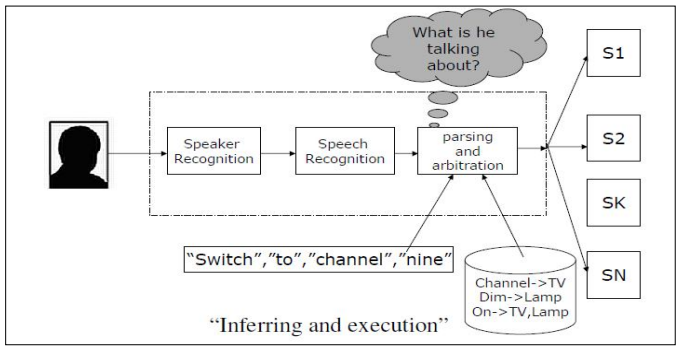

Figure 1 The System Architecture

The above diagram shows the proposed system architecture which uses Voice as the Biometric to secure the pervasive network in a household scenario. The Architecture can be divided into two phases:

1. The training Phase
2. The recognition and operation Phase.

The training phase is used to train the pervasive network and its various components i.e. the devices, which can be connected through RFID, Zigbee or other kinds of sensors. The network components can be trained with the voice of the users of the home and the database is created. In the recognition phase the matching with the existing database is performed and the devices are operated. The following section throws more light on both the phases and the methods used.

The Training Phase:
The training phase comprises of recording a word snippet of all the users using a microphone and creating a database. For our proposed model we require two kinds of databases:

The user database

The command database

a) The user Database: Let us consider a smart home where all the devices e.g refrigerator, TV, Door etc are all automatic and have sensors embedded in them. Sensors can be of any type like the most commonly used RFID based, GSM based, GPRS based etc. These devices are connected in a networked architecture and only the family members can have access on these devices. The first step of our proposed architecture is to train the network with the voices of all the persons who have to be authenticated for access. For example only the male family head and the female family head are to access the system thus the system has to train with their voices. A catch phrase or a group of words can be given to the users to be authenticated to be spoken in standard test environments using the microphone and recorder. A test environment has been created for this purpose with the use of MATLAB tool, in this research.
The users are made to speak those words and the features are detected and stored in the database. This forms our user database. The cepstral coefficients of the voice are used as the characteristics feature to record and to differentiate between users. The below diagram shows a step by step description:

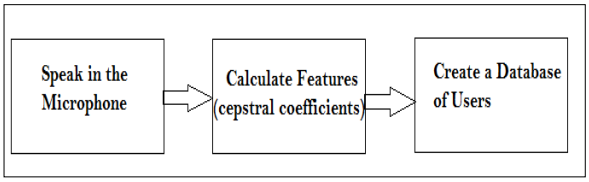

Figure 2 User Registration

b) The command Database: The second step is to create a command database depending on the number of devices to be operated. Each user will be required to train the network with his/her own voice. Let us consider three devices, the Door, the refrigerator and the TV to be connected in a home network. Thus we will require to train each user with commands to operate these devices. Each user will be required to speak in the microphone all the commands and the features of his/her voice corresponding to that command will be calculated and stored in the command database. A step by step procedure for this step is shown in the below figure:

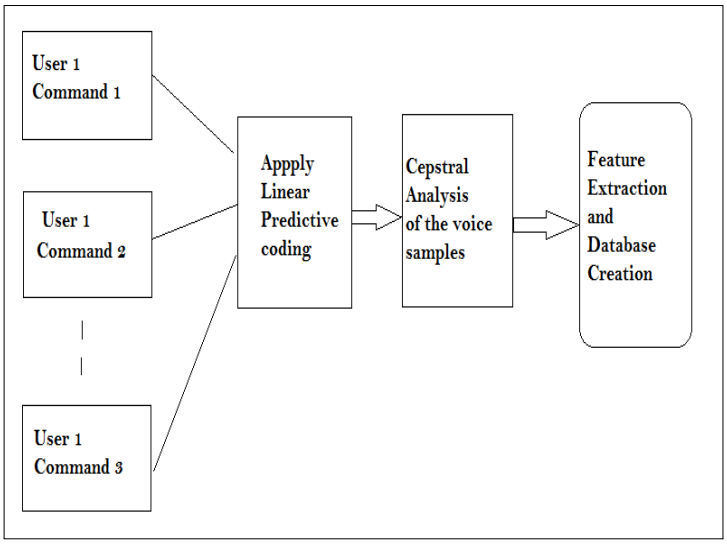

Figure 3 Database for Command

The Operation Phase:

The operation phase comprises of recognition and day to day operation of the network. The recognition phase is similar to the training phase in finding out the feature with the difference that no database is required to be created and the facility is only provided to calculate the instantaneous values of features from real time voices of the user and then a comparison to the database is made to check for the authenticity of the user and also to identify which command to be followed. On matching with one of the database values, the corresponding command is followed.
The step by step description of the operation phase is defined below:

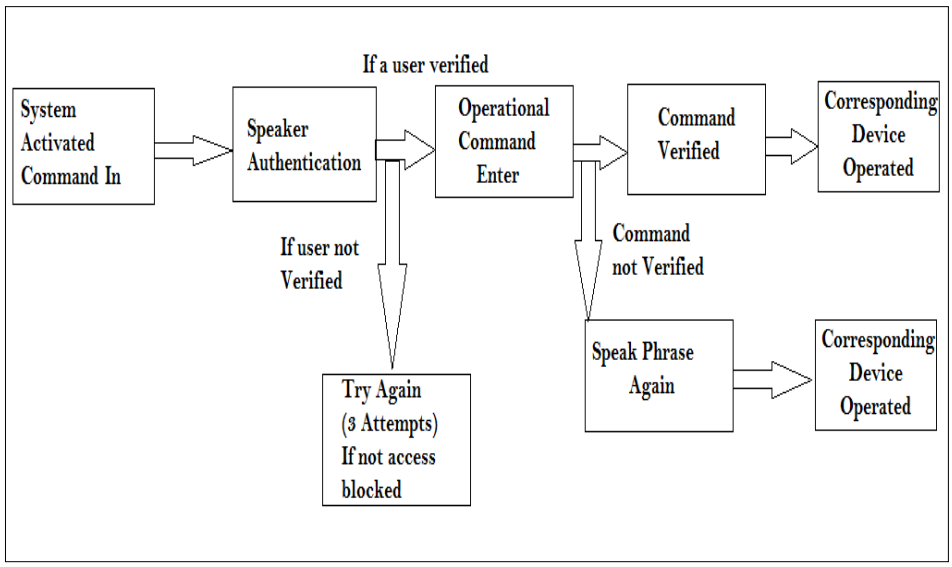

Figure 4 Operational Phase

5. RESULTS AND DISCUSSION

A simulation to study and analyze the proposed research is done using MATLAB 2010. The system architectures are enacted virtually using programming. The first phase i.e. training phase is used to train the system with all the users who will have access to the network. Figure 5, shows the GUI (Graphical User Interface) which was made for implementing and testing the model. For testing the system was made to work for a 2 users. The main interface contains two options of either going to the user database or to the command database. Both of the two database have two options to either train or to operate. The user database is trained to recognize the two users' voice and then only the access to operate the network is granted. The words used to train the system are:

Good Work Jones- 1st User

Blessing in Disguise- 2nd User

In a manner it acts as public key for the two users to access the system. Not only they would be tested for the correct words but also for the correct cepstral coefficients, when they speak those particular set of words thus giving a better security and kind of a hybrid cryptography.

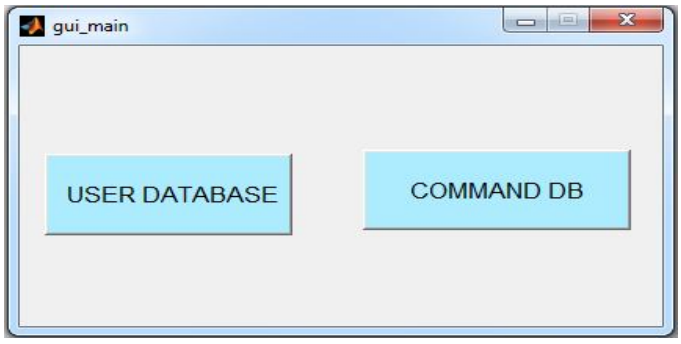

Figure 5 Main GUI

Every user is made to speak 20 times the particular word and corresponding cepstral coefficients are evaluated and stored in the directory. MFCC or Mel-frequency Cepstral Coefficients in short also known as cepstral coefficients are based on human hearing perceptions which cannot perceive frequencies over 1Khz.MFCC is thus, based on known variation of the human ear's critical bandwidth with frequency[13]. Linear Predictive Coding has been used to generate an approximate linear envelope of the spoken words. LPC is a source-filter analysis-synthesis methodology that approximates sound generation as an excitation (a pulse train or noise) passing through an all-pole resonant filter.
Both the training and operation phase uses almost the same set of procedures to generate the data set. The following table summarizes the parameters:

Table 1: Parameters during Training

Parameter	Description
No. of Users	2
No. of Samples per user	20
Characterization	MFCC
Time to train	1 seconds/sample
Devices	Microphone, Computer
Frequency	16000 KHz

The same process is undertaken to evaluate the coefficients for command database. The words used to train the system are:

a) Open the Door- To open the door
b) Door Close- To close the door
c) Switch on Light- To Switch on Light
d) Lights Off- To Switch off Light

The Database can be trained again as and when required to more commands as well as more number of users.
The operation phase is fairly simple, the user has to press the button to and speak after it within one seconds, a very common form as used in phones or Google Voice command app available in our phones, tablets etc.
The comparison between the runtime voice and database is done using the Euclidean distance method. The Euclidean distance is calculated between the cepstral coefficients of feature matrix and compared with the feature matrix in database and accordingly the command is interpreted as the minimum feature distance. The system was tested for 100 samples using different commands in both the modules. The system showed around 58.60 percent of correct recognition. The most correct recognized words were "*Open the Door*", with almost 78 percent correct recognition while the least correct recognized word was "Door Close" with less than 45 percent recognition.

6. CONCLUSION

This paper has taken the security aspect of pervasive networks, into consideration and suggested a possible approach to secure Body Network Networks, sensor networks or any other kind of pervasive networks. The voice Biometric was taken as the identifier for persons as well as commands. The idea is to create a well secured Internet of Things, with a number of devices. The tests were performed virtually on software and various commands were tested to show a good amount of accuracy. Further research can be focused to improve the accuracy of the system. Although, it is widely understood that majority of biometric systems especially the voice based system are hugely dependent on various conditions like the environment, voice conditions in different weather and health conditions of the user etc., thus 100 percent or close to 100 percent accuracy is highly tough goal to obtain.

REFERENCES

[1] M. Mana, M. Feham, and B. A. Bensaber, "Trust key management scheme for wireless body area networks," International Journal of Network Security, vol. 12, no. 2, pp. 61–69, 2011.
[2] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, (SenSys '04), pp. 162–175, Baltimore, Md, USA, November 2004.
[3] M. Guennoun, M. Zandi, and K. El-Khatib, "On the use of biometrics to secure wireless biosensor networks," in Proceedings of the 3rd International Conference on Information and Communication Technologies: From Theory to Applications, (ICTTA '08), pp. 1–5, Damascus, Syria, April 2008.
[4] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: testing the limits of elliptic curve cryptography in sensor networks," in Proceedings of the 5th European Conference on Wireless Sensor Networks, pp. 305–320, Bologna, Italy, February 2008.

[5] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in Proceedings of the International Workshop on Wireless Sensor Networks and Applications, (WSNA '03), pp. 141–150, San Diego, Calif, USA, September 2003.

[6] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," in Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, (SECON '04), Santa Clara, Calif USA, October 2004.

[7] F. Adelstein, S. K. S. Gupta, G. G. Richard, and L. Schwiebert, Fundamentals of Mobile and Pervasive Computing, McGraw-Hill, New York, NY, USA, 2005.

[8] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security, (CCS '03), vol. 2, pp. 500–528, Washington, DC, USA, October 2003.

[9] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," inProceedings of the International Conference on Parallel Processing Workshops, pp. 432–439, Kaohsiung, Taiwan, October 2003.

[10] S. M. K.-U.-R. Raazi, H. Lee, S. Lee, and Y.-K. Lee, "Bari+: a biometric based distributed key management approach for wireless body area networks," Sensors, vol. 10, no. 4, pp. 3911–3933, 2010.

[11] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," IEEE Communications Magazine, vol. 44, no. 4, pp. 73–81, 2006.

[12] S. D. Bao, C. C. Y. Poon, L. F. Shen, and Y. T. Zhang, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," IEEE Transactions on Information Technology in Biomedicine, vol. 12, no. 6, pp. 772–779, 2008.