A REVIEW ON USING VOICE BIOMETRIC OF SECURING A SMART HOME NETWORK AND IMPLEMENTATION

T. BHARGAVA RAMU
Research Scholar
Shri JJT University
Rajasthan
bhargava.ramu@yahoo.com

ABSTRACT:

The biometric frameworks are progressively utilized in our general public. In this paper, we will address on one of these framework: the biometric confirmation utilizing voice. Beginning from the general foundation of the current biometric frameworks we will continue to investigate each progression of a voice confirmation framework. We will depict the standards of utilization and simultaneously the principle issues identified with this framework, similar to security and unwavering quality of this sort of framework. Like each other verification framework, this one can be focus of dangers and assaults to its security and we will attempt to clarify the fundamental ones. Hence we will give a review about how the framework is utilized practically speaking. The developing age of Wireless Sensor Networks, is the Internet of Things. This framework is connecting physical articles, legitimately to the Internet utilizing microcontrollers or chip. Envisioning, the cutting edge web, the Internet of Things (IoT) gives the foundation of inescapable remote detecting and ID frameworks with billions of extraordinarily recognizable savvy gadgets to shape an omnipresent situation. The World Wide Web gives incredible chances to information assortment and examination, just as, for interoperability of items, that can't be associated with a similar neighborhood. This system of gadgets otherwise called universal figuring, in any case, suggests a genuine conversation starter of security in such an enormous number of gadgets. This paper centers around the security viewpoint and a suitable technique for giving tied down access and activity to the clients, in such sort of a system as characterized. A biometric approach dependent on Voice Recognition and Speech Recognition is proposed which frames a double layer of security and validation for every client, the first for the recognizable proof of the client to have a place with the system and the other for getting to the different gadgets.

Keywords: *Internet of Things, Biometric, Voice Recognition.*

1.0 INTRODUCTION:

Imagining, the cutting edge web, the Internet of Things (IoT) gives the idea of unavoidable remote detecting and recognizable proof frameworks with billions of interestingly recognizable savvy gadgets to shape a universal situation, which can remain associated through various mediums consistently. The dynamic idea of inescapable system get to must be coordinated with a design including the system, availability, security and preservance. The unavoidable system get to engineering needs to have a comprehensive rundown of design choices, arrange/endpoint gadget backing, and mix decisions so as to achieve a variety of different clients, gadgets and their interoperability. Unavoidable system get to dynamicity, requires a broad sending, design and strategy alternatives that can be effectively controlled and halfway overseen. These necessities, demand an incredibly secure condition for an inescapable system to be followed. While growing such sort of a situation, the attention has been on usage, and not on different elements, for example, security of the changed clients in a specially appointed system. The interconnections inside a system stay inclined to an unapproved access because of absence of

an appropriate and legitimate safety effort. The customary key based strategy has not been discovered quite a bit of utilization in preferences of, such sort of a domain. In this paper biometric based security engineering has been proposed which considers voice as a decision of the biometric among various different biometrics.

2.0 LITERATURE REVIEW:

Norman Desmarais, (2000) This paper inspects the procedures utilized in the two classifications of biometric strategies (physiological and conduct) and considers a portion of the applications for biometric advances. Basic physiological biometrics incorporate finger attributes (fingertip [fingerprint], thumb, finger length or example), palm (print or geology), hand geometry, wrist vein, face, and eye (retina or iris). Social biometrics incorporate voiceprints, keystroke elements, and manually written marks.

Christian Zeitz, (2008) Adjacent to the enhancement of biometric mistake rates the general security framework execution in regard to purposeful security assaults assumes a significant job for biometric empowered validation plans. As customarily most client confirmation plans are information or potentially ownership based, right off the bat in this paper we present a technique for a security examination of Internet-based biometric verification frameworks by improving referred to approachs, for example, the CERT assault scientific categorization with a progressively definite view on the OSI-Model. Besides as evidence of idea, the rules separated from this approach are carefully applied to an open source Internet-based biometric validation framework (BioWebAuth). As contextual investigations, two model assaults, in view of the discovered security spills, are explored and the assault execution is introduced to show that during the biometric validation plans adjacent to biometric blunder execution tuning likewise security issues should be tended to. At long last, some structure proposals are given so as to guarantee a base security level.

Kirat Pal Singh, (2016) The strengthening in organize on chip (NOC) and System on chip (SOC) in Microelectronics and Sensors have built up the different remote correspondence Network advancements. In the previous hardly any years, numerous scientists have been concentrating on building framework engineering of system observing to improve the specialized prerequisite uniquely intended for organize security. Less research was found in giving the solid biometric based system security framework to give impenetrable security. The famous MIPS based cryptography processor is utilized for equipment and programming items and principles require enormous cryptography keys length for higher security level. The significant shortcoming of Normal cryptography framework dependent on deviated calculations need the capacity of mystery keys. Put away keys are regularly ensured by ineffectively chosen client passwords that can either be speculated or acquired through beast power assaults. Joining biometric with MIPS cryptography processor is as a potential arrangement. In this paper I propose another way to deal with organize security utilizing MIPS put together crypto processor based with respect to contactless palm vein biometric framework. This methodology considers NOC requirements and its topology. It gives greater security less key length and

there is no compelling reason to store any private key anyplace.

3.0 PROPOSED MODEL

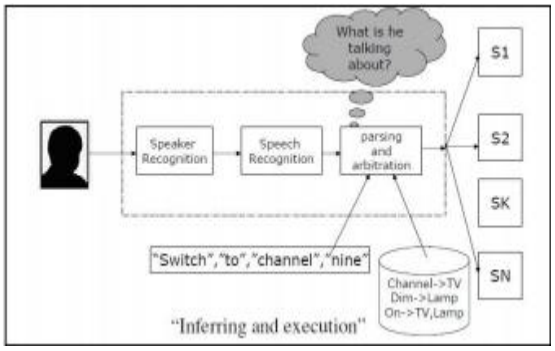

Figure 1 The System Architecture

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 client Database: Let us consider a shrewd home where every one of the gadgets e.g fridge, TV, Door and so on are for the most part programmed and have sensors inserted in them. Sensors can be of any kind like the most usually utilized RFID based, GSM based, GPRS based and so forth. These gadgets are associated in an arranged design and just the relatives can approach on these gadgets. The initial step of our proposed engineering is to prepare the system with the voices of the considerable number of people who must be validated for get to. For instance just the male family head and the female family head are to get to the framework hence the framework needs to prepare with their voices. A catchphrase or a gathering of words can be given to the clients to be confirmed to be spoken in standard test situations utilizing the amplifier and recorder. A test domain has been made for this reason with the utilization of MATLAB apparatus, in this examination. The clients are made to express those words and the highlights are identified and put away in the database. This structures our client database. The cepstral coefficients of the voice are utilized as the qualities highlight to record and to separate between clients. The beneath outline shows a bit by bit depiction:

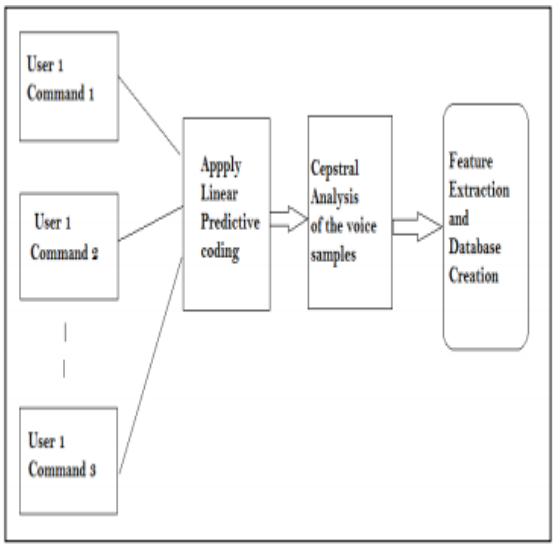

Figure 2 Database for Command

The Operation Phase:

The activity stage involves acknowledgment and everyday activity of the system. The acknowledgment stage is like the preparation eliminate in finding the component with the distinction that no database is required to be made and the office is just given to ascertain the quick estimations of highlights from ongoing voices of the client and afterward a correlation with the database is made to check for the legitimacy of the client and furthermore to recognize which direction to be followed. On coordinating with one of the database esteems, the comparing order is followed.

The step by step description of the operation phase is defined below:

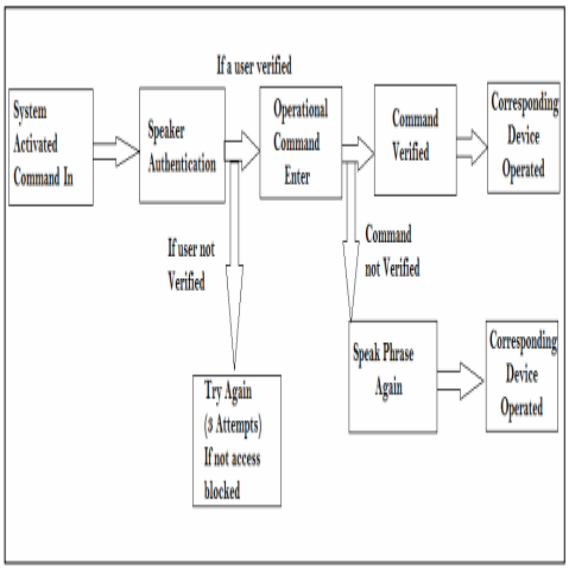

Figure 3 Operational Phase

4.0 RESULTS AND DISCUSSION

A reproduction to contemplate and investigate the proposed research is finished utilizing MATLAB 2010. The framework designs are instituted for all intents and purposes utilizing programming. The principal stage for example preparing stage is utilized to prepare the framework with every one of the clients who will approach the system. Figure 5, shows the GUI (Graphical User Interface) which was made for actualizing and testing the model. For testing the framework was made to work for a 2 clients. The fundamental interface contains two alternatives of either setting off to the client database or to the order database. Both of the two database have two choices to either prepare or to work. The client database is prepared to perceive the two clients' voice and afterward just the entrance to work the system is allowed. The words used to prepare the framework are:

Great Work Jones-first User

Surprisingly beneficial turn of events second User

In a way it goes about as open key for the two clients to get to the framework. Not just they would be tried for the right words yet in addition for the right cepstral coefficients, when they talk those specific arrangement of words along these lines giving a superior security and sort of a half breed cryptography.

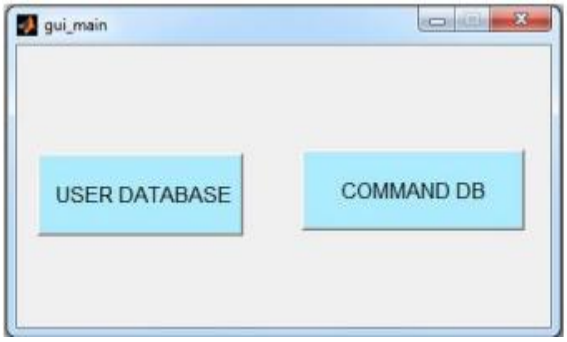

Figure 4 Main GUI

A reproduction to contemplate and investigate the proposed research is finished utilizing MATLAB 2010. The framework designs are instituted for all intents and purposes utilizing programming. The principal stage for example preparing stage is utilized to prepare the framework with every one of the clients who will approach the system. Figure 5, shows the GUI (Graphical User Interface) which was made for actualizing and testing the model. For testing the

framework was made to work for a 2 clients. The fundamental interface contains two alternatives of either setting off to the client database or to the order database. Both of the two database have two choices to either prepare or to work. The client database is prepared to perceive the two clients' voice and afterward just the entrance to work the system is allowed. The words used to prepare the framework are:

Great Work Jones-first User

Surprisingly beneficial turn of events second User

In a way it goes about as open key for the two clients to get to the framework. Not just they would be tried for the right words yet in addition for the right cepstral coefficients, when they talk those specific arrangement of words along these lines giving a superior security and sort of a half breed cryptography

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 KH_z

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 prepared again as and when required to more directions just as progressively number of clients. The activity stage is genuinely straightforward, the client needs to press the catch to and talk after it inside one seconds, a typical structure as utilized in telephones or Google Voice direction application accessible in our telephones, tablets and so on. The correlation between the runtime voice and database is finished utilizing the Euclidean separation strategy. The Euclidean separation is determined between the cepstral coefficients of highlight network and contrasted and the component framework in database and in like manner the order is deciphered as the base element separation. The framework was tried for 100 examples utilizing various directions in both the modules. The framework appeared around 58.60 percent of right acknowledgment. The most right perceived words were "Open the Door", with very nearly 78 percent right acknowledgment while the least right perceived word was "Entryway Close" with under 45 percent acknowledgment.

5.0 CONCLUSION:

As of now the biometric is by all accounts the normal development of the conventional frameworks coming about because of advancements improvement. Surely the voice is one of the more contemplated advances. The customary access strategies have a progression of issues, they can be lost, taken or loaned in an unapproved way. In addition they don't control the successful personality of the client and need that the client recalls codes or secret phrase. The biometric key is produced from the individual attributes of the individual, in this manner isn't dependent upon the issues recorded previously. Anyway there are others issues. For instance the choice is probabilistic, it doesn't shows an outright

sureness, it communicates just resemblance: a breaking down receiver or a virus could contort the outcome. The security part of unavoidable systems, into thought and proposed a potential way to deal with secure Body Network Networks, sensor systems or some other sort of inescapable systems. The voice Biometric was taken as the identifier for people just as directions. The thought is to make an all around verified Internet of Things, with various gadgets. The tests were performed essentially on programming and different directions were tried to show a decent measure of exactness. Further research can be engaged to improve the precision of the framework. In spite of the fact that, it is generally comprehended that greater part of biometric frameworks particularly the voice put together framework are colossally reliant with respect to different conditions like the earth, voice conditions in various climate and wellbeing states of the client and so on., in this way 100 percent or near 100 percent precision is exceptionally extreme objective to acquire.

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 selforganizing 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.