ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Unique Bio-identification for Home-Security on IoT

Vaibhav Kale[1], Rohit Kashid[2], Meghan Nagvekar[3], Baswaraj Walke[4], Prof.G.M.Gaikwad[5]

Department of Information Technology, SIT Lonavala, Maharashtra, India

ABSTRACT: -The document explains the importance of access to modern smart homes over the Internet, and highlights several security issues associated with it. In this work, we propose a two-step verification process for smart homes using a fingerprint i.e bio-identification and device fingerprinting, which verifies the person and after owner accessing the home over the Internet. In this system, when an owner wants to access the home via the Internet, which requires the server access page, the server returns the login page with the Java fingerprint script. There are two fingerprints in our database whose elements accumulate over time. Whitelist is a list of authorized or unauthorized fingerprints. The blacklist is a list of unauthorized or malicious fingerprints from potential attackers who have tried to gain access to the home. In the Emergency Time System also generated the One Time Password (OTP) and sends it to the legally registered mobile phone number through the Short Message Service (SMS), the user enters the site and therefore the legitimacy of the user is verified.

KEYWORDS: Fingerprint Sensor, Raspberry Pi, Motor, Device Fingerprinting.

I.INTRODUCTION

The emergence of smart devices has boosted the concept of connecting everyday objects via the existing networks. The drastic increase of connected devices has outreached the boundaries of the conventional networks, resulting the renaissance of the web as the third wave “Internet of Things (IoT)”. IoT is rapidly growing network of heterogeneous devices and objects, which are uniquely addressable within the network and capable of identifying and sharing information with or without human interaction. The concept of Home Automation was a topic of interest in the Academic arena since the late 1970s, with time and advancement of technology people‘s expectations about Home Automation and how they should access their home has dramatically changed. The affordability and popularity of electronic devices and internet were contributing factors to this change.

The modern Home Automation System is a delicate balance of Ubiquitous Computing Devices and Wireless Sensor/Actor Networks. The added expectations and Convenience of Access‘has brought new security challenges to the Home Automation front. Various researchers showed that, there are vulnerabilities in many commonly used devices and technologies in Home Automation. In this sense, learning and recognizing human behavior has emerged as a relevant issue, and, concurrently, the analysis of the human–machine interaction and the definition of the appropriate ways to communicate with a smart home as intuitively and naturally as possible has become crucial. With respect to this, gesture interpretation represents an appealing, as well as valid, alternative to other more conventional contact-based or video-based modalities.

In particular, the specialized literature reports on studies that refers to context-aware multimodal interfaces based on video and audio inputs, static hand pose and dynamic hand gesture visual recognition glove-based sensing, or marker-based motion capture systems. These technologies have pioneered the research in the field but show some limitations for a seamless employment in a smart home: They require a dedicated and often expensive environment; they frequently need a complex setup that involves calibration procedures and may be strongly affected by environmental nuisances (e.g. light changes); finally, they impose constrains n on their usage, for example, in the relative pose between.

Home Automation System uses the technology of Internet of Things for monitoring and controlling of the electrical and electronic appliances at home from any remote location. Implementation of a low cost, flexible home

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

automation system is presented. It enhances the use of wireless communication which provides the user with remote control of various electronic and electrical appliances. A smart home automation based on device fingerprinting improves the security. Device fingerprinting is used for fighting fraud on websites. The device fingerprint along with username based security enables the verification of user as well as the device used to access the home. This significantly improves home security when they are accessed over the internet

II.LITERATURE SURVEY

The paper explains the importance of accessing modern smart homes over the internet, and highlights various security issues associated with it. The work explains the evolution of Device Fingerprinting concept over time, and discusses various pitfalls in existing device fingerprinting approaches. In this paper, they propose a two stage verification process for smart homes, using Device Fingerprints and Login Credentials, which verifies the user device as well as the user accessing the home over the internet [1]. They propose a smart home control system using a coordinator based ZigBee networking. The working of the proposed system is three fold, 1) smart interference control system controls the interference caused due to the co-existence of IEEE 802.11x based wireless local area networks (WLAN) and Wireless Sensor Networks (WSN), 2) smart energy control system is developed to integrate sunlight with light source and optimizes the energy consumption of the household and 3) smart management control system to efficiently control the operating time of the electronic appliances [2].

Home automation involves automatic control of household features, activity and appliances. A home with an automatic control system is known as smart home. Automation system helps one's home to promote security, comfort and convenience.. This paper explains the importance of accessing modern smart home over the internet and highlights various security issues with it [3]. The proposed methodology aims at providing high accuracy classification for home automation systems, which are generally user independent, device independent, and device orientation independent. The approach illustrated in this paper is composed of three main steps: event identification; feature extraction; and ML-based classification [4].

A prototype to control and monitor home appliances using Face book in a smart home environment is proposed in this project. Ethernet device with microcontroller (atmega1284p) analyses and processes the information and also provides virtualization services to users. In the proposed method, the Face book authenticated and preloaded Ethernet device collects and stores home appliance information and sends the information to the Face book user page. The user can control the appliances of smart home by sending commands from their Face book account [5].

III.BACKGROUND

This study has analyzed current lock systems that are usedin houses and offices at present. It has been found that althoughthese methods are helpful in the initial days, eventually theybecome outdated and pose much threat to security issues.They have also been identified as quiet expensive. Below is adiscussion on the pros and cons of the existing systems.

A. Password-Authentication

This system stores the password of authenticated users forthe purpose of validation which provides considerable securityto the users. Power consumption is efficient and usage isuser-friendly. However, unauthorized users can easily acquirepasswords through different methods (hacking, guessing and so on.).

B. Face detector locks

\

These systems have difficulty in recognizing a face fromimages captured from two drastically different views and underdifferent illumination conditions. It is questionable whether theface itself, without any contextual

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

information, is a sufficientbasis for recognizing a person from a large number of identities with an extremely high level of confidence.

C. Retinal scanner

The retinal vasculature is rich in structure and is supposedto be a characteristic of each individual and each eye. The image acquisition requires a person to peep into an eyepiece and focus on a specific spot in the visual field sothat a predetermined part of the retinal vasculature could beimaged. This device is frequently used for security purpose.The false acceptance and rejection rates are lower in thisdevice. But the problem of this device is, it is not user-friendlyand the equipment cost is very high.

D. Iris scanner

Iris recognition is a method of biometric authentication, based on extraction features of the iris of an individual's eyes.Each individual has a unique iris; the variation even existsbetween identical twins and between the left and right eye ofthe same person. The advantage of using iris scanner is, it has very high accuracy and the accuracy of iris scanners canbe affected by changes in lighting. As iris is a small target anda scanner cannot be performed properly for multiple people ofdifferent heights. The main shortcomings with iris recognitiontechnology, is that the iris scanners are very expensive andrequires a lot of memory to store data.

E. Voice recognition

Voice recognition or speaker recognition is the problem ofidentifying a speaker from a short utterance. This biometrictechnology uses the acoustic features of speech that have beenfound to differ between individuals. These acoustic patternsreflect both anatomy (e.g., size and shape of the throat andmouth) and learned behavioral patterns (e.g., voice pitch, speaking style). A disadvantage of voice-based recognitionis that speech features are sensitive to a number of factors suchas background noise.

IV.PROPOSED METHODOLOGY

3.1 Block Diagram:

The block diagram as shown in Fig 1. It consist of Raspberry Pi, Fingerprint Module. This project provides a secure, authentic and user-friendly mechanisum for automatic home security. Our work utilizes user fingerprinting and legitimate login credentials as a part of double verification process for authorized user. The user provides the login credentials, if login credentials verification is passed then system request to give an fingerprint of user. Then the gathered fingerprint is analyzed and matched with original one.There are two lists in our database; the 'whitelist' is the list of approved or authorized fingerprints belonging to legitimate users and the 'blacklist' is a list of unauthorized or malicious fingerprints belonging to potential attackers who tried to gain the access to the locker. Client with fingerprints in whitelist are allowed to enter in home after login credential verification. The client with fingerprints in the blacklist are not allowed to access the locker even if their login credentials are correct. The user must contain the Android App which generate an One Time Password(OTP) and sent it the legitimate usre's registered mobile number via message, which is user enters into the website and thus legitimacy of the user is verified. If the user is not verified any of this stages then that user is added in blacklist and he is not able to enter in home at all. Then that blacklisted users information is given to that of authorized person. The authorized user can add the users in blacklist if he wants and trusted third party device can enter in home after verification by legitimate user.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

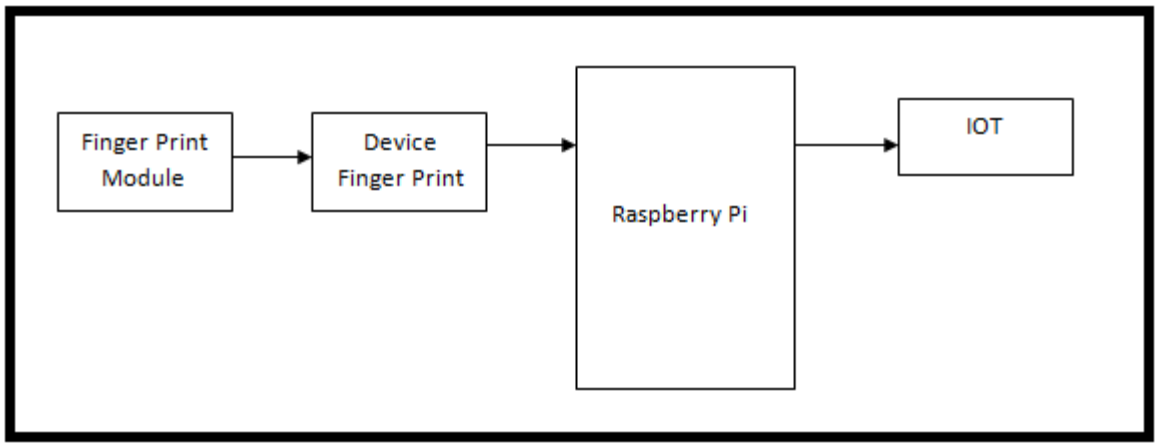

Fig 3.1.1 Block Diagram of System

3.2Elements of Block Diagram:
1. Raspberry Pi:-

Raspberry Pi is a credit-card-sized single board computer developed in the UK by Raspberry Pi foundation with the intention of stimulating the teaching of basic computer science in schools. It has two models; Model A has 25 6Mb RAM, one USB port and no network connection. Model B has 5 12Mb RAM, 2 USB ports and an Ethernet port. It has a Broadcom BCM2835 system on a chip which includes an ARMl176JZF -S 700 MHz processor, Video Core IV GPU, and an SD card. The GPU is capable of Blu-ray quality playback, using H.264 at 40MBits/s. It has a fast 3D core accessed using the supplied OpenGL ES2.0 and Open VG libraries. The chip specifically provides HDMI and there is no VGA support.

2. Fingerprint Module:

Finger print sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person.

3. Device Fingerprint:

When a user wishes to access the home over the internet, he requests the login page from the server, the server then returns the login page along with the fingerprint java script. The user provides the login credentials along with the fingerprint of the device he is using. The login credentials are verified, if the verification is passed, then the gathered device fingerprint is analyzed to see if there are enough device fingerprinting parameters available to provide a comprehensive fingerprint of the user device.

V. FUTURE SCOPE

Smart door lock system based on device fingerprinting with user finger print improves the security. Device fingerprint gives us an identity related to device and sensor module box for biometric fingerprint. A two stage verification process for smart home is implemented. All we need to addis the number of parameter's for much better door locks system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

VI.CONCLUSION

In this paper, a novel architecture for low cost and flexible home control and monitoring system using Android based Smart phone is proposed and implemented. The proposed architecture utilizes restful based Web services as an interoperable application layer for communicating between the remote user and the home devices. Any Android based Smart phone with built in support for Wi-Fi can be used to access and control the devices at home. When a Wi-Fi connection is not available, mobile cellular networks such as 3G or 4G can be used to access the system. Also high security will be provided. Future works will focus on creating a wireless network between the home server and the home devices using Zigbee and implementation of voice commands for controlling the application via voice.

REFERENCES

[1] Arun Cyril Jose, Reza Malekian, "Improving Home Automation Security; Integrating Device Fingerprinting into Smart Home", DOI 10.1109/ACCESS.2016.2606478, IEEE Access.
[2] Murad Khan, BhagyaNathali Silva, Kijun Han"Internet of Things based Energy Aware Smart Home Control System", DOI 10.1109/ACCESS.2016.2621752, IEEE Access.
[3] AthiraSankar, Lakshmi S, "A Survey On Improving Home Automation Security by Integrating Device Fingerprinting Into Smart Home", International Research Journal of Engineering and Technology (IRJET) ,Volume: 04 Issue: 04 | Apr -2017.
[4] Angelo Cenedese, Gian Antonio Susto, "Home Automation Oriented Gesture Classification from Inertial Measurements", IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, 2015.
[5] P.Kabilan, H.NafilAskar, P.NareshAnand, S.Manimaran, G.Venkatesh, "FACEBOOK BASED HOME APPLIANCES SECURITY CONTROL AND MONITORING USING MICROCONTROLLER", Asia Pacific Journal of Research, Vol: I. Issue XXV, March 2015.
[6] R. Malekian, D. C. Bogatinoska, A. Karadimce, J. Trengoska, W. A. Nyako, "A Novel Smart ECO model for Energy Consumption Optimization", Elektronika ir Elektrotechnika, Vol. 21, No.6, pp.75-80, 2015.
[7] J. Shao, L. Wang, W. Zhao, Y. Zhong, R. Malekian, "An improved Synchronous Control Strategy based on Fuzzy controller for PMSM", Elektronika ir Elektrotechnika, Vol. 20, No. 6, pp. 7-23, 2014.
[8] C. Karlof, D. Wagner, ―Secure routing in wireless sensor networks: attacks and countermeasures‖, Ad Hoc Networks, vol. 1, pp. 293–315, 2003.
[9] Y. Hu, A. Perrig, D. Johnson, ―Wormhole attacks in wireless networks‖, IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370–380, Feb. 2006.
[10] J. Wright, ―Practical ZigBee Exploitation Framework‖, Toorcon, Oct. 2011.