International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Nov -2016 www.irjet.net p-ISSN: 2395-0072

Home Security Using Wireless Technology

Akshaykumar Patil[1], Pankaj Jadhav[2],Vinod Magar[3],Omkar Dahyalkar[4]

[1234]*UG Student, Dept. of Computer Engineering, SITS. Narhe, Pune, India.*

Abstract -*Near Field Communication(NFC) technology system is one of the most useful and promising technologies in the field of mobile application services recently. We propose an integration design of both a near field communication (NFC) and a smartphone to develop a door lock control system. This design consists of a built-in NFC capabilities of a Smartphone. This design also offers the Human sensing using Human Sensor Detection. This system allows only for authorized people. When authorized people verified the specific door which is secured by this door lock control system immediately opens. Hacker are does not hack this system easily. The door lock control system is fixed on the door, and also provides both the sleep state and the standby state is for power consumption and longtime operation.*

Key Words: NFC, Smartphone, Door lock, Human Sensor Detection.

1.INTRODUCTION

IoT security is the area of effort concerned with protecting connected devices and networks in the Internet of things (IoT).

The Internet of Things contain the increasing ascendancy of objects and entities – known, in this context as things -- provided with unique identification module and the ability to automatically transfer data over a network. Much of the increase in IoT communication and networking comes from computing devices and embedded sensor systems used in industries for machine-to-machine (M2M) communication smart electrical grids, home automation, vehicle to vehicle communication and wearable technology devices.

The main problem is that because the conception of networking appliances and other objects is comparatively new, security has not always been considered in design of product. IoT products are often sold with old and vulnerable embedded operating systems and software. Furthermore, owners often fail to modify the default passwords on smart devices -- or if they do change them, fail to select sufficiently passwords which is enough for security. To increase security, an IoT device that needs to be directly accessible over the Internet, should be dividedinto its own network and have network access is highly restricted. The network segment should then be monitored to identification of the potential anomalous traffic, and action should be taken if there is an any problem.

Security specialist have warned of the potential risk of large numbers of vulnerable devices connecting to the Internet since the IoT concept was first advance in the late 1990s. In December of 2013, a scientist at Proof point, an enterprise security firm, discovered the first IoT devices infected with malicious software(botnet). According to Proof point, more than 25 percent of the botnet was made up of devices other than computers devices, including smart TVs, baby observers and other household devices or appliances.

1.1. Problem Statement

To implement system for door lock using wireless technology. In the home automation means door lock, windows lock, Doors of cupboard we use this system. Also in the office doors and in a car we use this lock and open door easily without any key.

2.LITERATURE SURVEY

According to Il-Kyu Hwang e.t. all [1], Digital door lock is one of the most popular digital consumer devices because of the user vantage and reasonable price. In reality, it is replacing a lot of standard types of lock. As mobile technologies become more sufficient and credible, wireless technologies will be more highlight in a real home networking market. Specially, the ZigBee, one of the important wireless protocol, has become fair in both of trading and research areas, because of open standard, affordable, and low-power consumption. In this study, we proposed a novel wireless access observation and control system based on the digital door lock system, which is epispastic to used as a digital consumer device. It was basically related to IEEE 802.15.4, specifically ZigBee wireless network protocol used for wireless communication. ZigBee module and digital door lock with HDS(human detection sensor) were implemented. ZigBee module was proposed to support wireless sensor network and also used for the ZigBee tag to identify or verify the access objects. Digital door lock module was implemented as a digital consumer device to monitor and control the access system as well as digital locking system. Merit is, Its profitable and low power consumption characteristics.

Open standard, low-cost. And demerit of ZigBee is, ZigBee only allows one-way wireless communication.

According to Seung-Hyun Seo e.t. all [2], with the rapid development of smartphone devices and home networks, smartphones can remotely control Home Security System via the home network. Sometimes, during the homeowner's absence, they may want to delegate the authority to another person such as a housekeeper. For example, a homeowner may want to delegate the authority to monitor or control the security devices. In this paper, we proposed a new security mechanism that provides authentication and authorization of the delegated user. It is secure against offline password guessing attack and replay attack. Moreover, it efficiently provides the immediate revocation of the delegated user s access rights. Using our mechanism, delegated users can remotely control the Home Security System in the stead of the homeowner. Next, we implemented a Android smartphone application that allows people to remotely regulate their Home Security System. Advantage is, control methods in the access of home security system which monitors and controls security devices, installed around houses by using smartphones. And disadvantage is, Easily Hack because any one use smart phone.

According to Pavithra.D e.t. all [3], In this paper, we have introduced the event of a home management and security system exploitation using Raspberry pi and Internet of Things technology. The system is suitable for real-time home safety monitoring and for remotely controlling the home appliances and protection from fire accidents with immediate solutions. The system may be employed in many places like banks, hospitals, labs etc. that dramatically cut back the hazard of unauthorized entry. Proof may be given to the safety department if any theft issue happens. Advantage is, it enhances the facet of protection from fireplace accidents is its capability of sleuthing the smoke in order that within the event of any fireplace, associates an alerting message and an image is sent to Smartphone. And disadvantage is, this is real-time home safety monitoring. Easily Hack because any one use smart phone.

According to Freddy K Santoso e.t. all [4], Security and convenience are two major requirements for successful deployment of IoT in a smart home environment. This paper proposes and implements a smart home system based on Wi-Fi network. Using the AllJoyn framework as the base, the proposed system uses a gateway to provide a better authentication process and a convenient interface for the user via an Android device. However, the current method of entering device ID, pre-shared secret key and AP name by hand during the addition of a new device is inconvenient to the user, even though this process is only to be performed once for each device. A possible improvement to perform this procedure is to embed the relevant information of each device in a QR code on the device, which can then be scanned and read by the Android application initiated by the user. Advantage is, IoT include privacy, authentication and secure end-to-end connection. And disadvantage is, With the WIFI the hacker can hack the system and unlock it.

According to Jonghyun BAEK e.t. all [1], Today, NFC technology may have many benefits to our daily life, i.e. financial service, transportation service, leisure and royalty service. Especially, the use of NFC in NFC enabled device and onsite 'Smart Posters', which readable NFC tags have been placed, enables fast and easy ticketing, speedy access control, the downloading of pertinent travel- and entertainment-related information, and much more. The common factor is an NFC tag that has an NDEF message stored in it and is attached or embedded in the desired medium. However, if an attacker can overwrite an NDEF message in the legitimate tag or replace an NFC tag with hacked tag, they can deliver a mobile malware to user devices without user recognition. In this paper, we propose the authentication protocols for the NFC tag and NFC-enabled device which are uses XOR operation, hash function and random value generator that are suitable to a low-cost tag, while also providing a countermeasure to prevent a mobile malware attacks as we mentioned above. In addition, we shown that the proposed protocol provides a number of identified security features and requires the least memory storage and computational power in a tag. Advantages is, Enables fast and easy ticketing, speedy access control, the downloading of pertinent travel and entertainment-related information, and much more. Disadvantages is, Spoofing/Phishing. Data modification DoS.

3.RELATED WORK

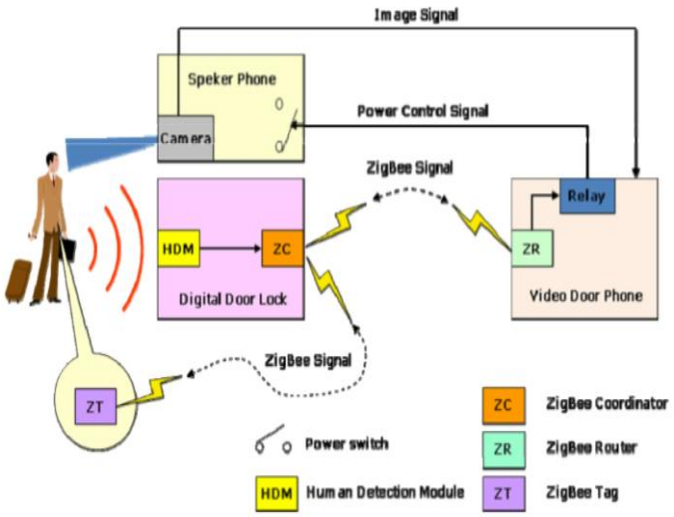

Fig.-1. System Configuration Diagram

Home network is a residential local network, and is used to connect multiple devices within the apartment or

house. It may consist of a broadband modem PCs, a router,a wireless access point, other electronics and entertainment peripherals. It allows users to remotely monitor, control consumer electronics through the external network such as Internet. Until home network has greatly getting a lot of attention in both research sectors and commercial. The home network has become the network of consumer related electronics for various useful applications such as telecommunications, entertainments, remote control and automation systems and monitoring systems. Owing to the rapid growth of the Internet and personal computers, high advance telecommunication technologies, the importance of the home network has increases emphasized in the both domains.

I. System Overview

In the system, a digital door lock, a video phone, phone, ZigBee tags and a speaker are connected on the network, as shown in Fig. 1. All users who are at the door can be identify by the tag of ZigBee. ZigBee tag is kind of ID with module of ZigBee including batteries. The digital door lock includes a human detection module and ZigBee module. The video door phone, which is a wireless connected to door lock, includes an LCD display, a relay, a ZigBee module, and a power switch with ZigBee relay module. In the camera module speaker phone is includes. Using ZigBee module, the digital door lock is control the video door phone wirelessly. A person at the gate is detected by the human detection, the ZigBee module of door lock sends a message to the video door phone and check whether the person has a ZigBee tag wirelessly. Then the video door phone sends a command to camera to turn it on. If a valid authorization code is taken from the ZigBee tag at the gate, digital door lock controls a motor connected to the locking system for open door. Otherwise the user can interact with the person using the speakerphone.

II. ZigBee Module

ZigBee module is used in video door phones, ZigBee tag and digital door lock. In this study we defined 2 terminologies, ZigBee tag and ZigBee module. ZigBee Tag is a kind of ID with ZigBee module. i.e., ZigBee module is used as a wireless communication device, whereas ZigBee tag is used as a communication device as well as a key of the digital door lock.

III. Digital Door Lock

The structure of the door lock and connection of the modules are shown in Fig. 2. The digital door lock is composed of a control board, a ZigBee module, a motion detection sensor board, a door sensor, a buzzer, a keypad, a motor, open/close limit sensors,a key-on switch, and batteries. The power voltage of digital door lock is 6V that is supplied by 4 serial batteries of 1.5V. The function of the control board is to control the functions of the door lock, and it includea tag registration button, a 3.3V regulator, a MCU, a password registration button, an open/close button, and a motor driver.

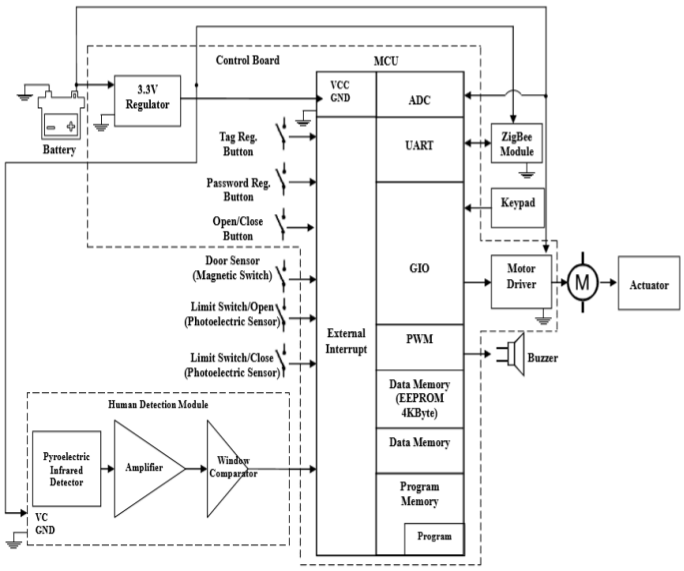

Fig.- 2. The structure diagram of the digital door lock

3.1.System Implementation

In this system implemented a prototype system for the access monitoring and control based on door lock with ZigBee protocol. As describe in the previous, four types of hardware module are developed, digital door lock module, ZigBee module and tag, ZigBee relay moduleand human detection module. Although there are many wireless solutions but, ZigBee protocol used in that system because of its low power consumption properties and economic. As shown in Fig. 3, implemented ZigBee module and tag are composed of battery, microcontroller unit, ZigBee chip and RF antenna of

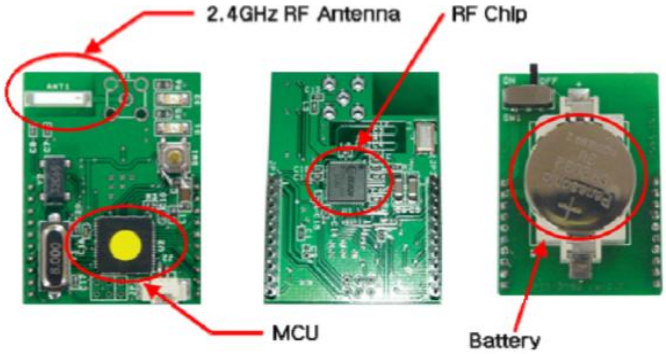

Fig.- 3. ZigBee Module

2.4 GHz. ZigBee could establish 2-way communication, and enabled a storing function of the access history in tags and

in the system. It also satisfied the wireless communication standard specifications, and adapted to home network systems due to powerful extension characteristics. Data rate of the ZigBee communication is 250 kbps. Data transfers range of ZigBee modules is up to 100 m. The maximum number of tags, which is used in the system is 254. ZigBee tags were modified to connect the system in distance range between 50 cm and 1 m. It is a practical range for the actual life. Long range might cause a problem because door is open so early before the person appear at the gate if the range is too long.

The developed system could be applied practically in the actual market for home networking system. Further, the system can be enlarged to another service such as a interconnection between home networking system and mobile phone.

3.PROPOSED ARCHITECTURE

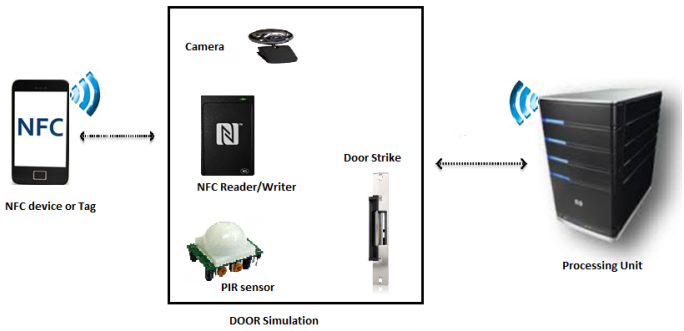

Fig -4. Proposed Architecture

In this proposed architecture of door lock system there is a Electronic Control Access System which is control by administrator. Lock system is place on the door. The NFC devices like NFC tag, NFC smartcard, NFC mobile are used to enter input to the system.

System checks the input and compare, if input is correct then door is open otherwise system captures the image of unauthorized person using camera which is placed with the door lock system.

4.CONCLUSION AND FUTURE SCOPE

NFC technology has number of advantages over other wireless technology because it provides bidirectional communication for interchange data i.e. both devices can receive and send data simultaneously unlike Bluetooth which promotes unidirectional communication.

This system is very easily handle by user. In the home automation means door lock, windows lock, Doors of cupboard we use this system. Also in the office doors and in a car we use this lock and open door easily without any key.

5.REFERENCES

[1] Il-Kyu Hwang, Member, IEEE and Jin-Wook Baek, "Wireless Access Monitoring and Control System based on Digital Door Lock", IEEE Transactions on Consumer Electronics, Vol. 53, No. 4.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Seung-Hyun Seo & Taenam Cho, "An Access Control Mechanism for Remote Control of Home Security System", 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.

[3] Pavithra.D and Ranjith Balakrishnan, "IoT based Monitoring and Control System for Home Automation.", Proceedings of 2015 Global Conference on Communication Technologies(GCCT 2015).

[4] Freddy K Santoso, and Nicholas C H Vun, "Securing IoT for Smart Home System", 2015 IEEE international Symposium on Consumer Electronics (ISCE).

[5] Jonghyun BAEK & Heung Youl YOUM, "Secure and Lightweight Authentication Protocol for NFC Tag Based Services ", 2015 10th Asia Joint Conference on Information Security.