IOT Based Smart Door Locks

Dr.N.Krishnamoorthy,
Assistant Professor,
Department of CSE,
Kongu Engineering College,
Perundurai, Erode – 638060
nmoorthy@kongu.ac.in

Kalaimagal.R,Gowri Shankar.S, Abdhul Asif.N.S,
Department of CSE, Kongu Engineering College,
Perundurai,Erode–638060

Abstract— The planned technique is based on the IoT technology and also the application of mobile communication technology to standard device like door lock to send the status of the door whether it's opened or closed. The aim is to forestall the protection issues in mistreatment manual physical key and conjointly to send automatic SMS to the house owner regarding the standing of the door. Above all, this study proposes the Secure Door Lock System based on security improvement set up for the protection issue caused by the physical key utilized in remote-controlled automation machines, like ATMs, KIOSKs, and marketing machines.

Keywords-Authentication,Security,Door locks,Communication.

*****

I.INTRODUCTION

The IoT technology is that the interaction between individuals to individuals, machine to machine communication network. Application services supported data and communication technology has been actively investigated within the knowledge data society. Above all, the foremost ascent will be determined in convergence services which mixes over 2 parts for a similar purpose. Convergence services influence represent Internet of Things (IoT) technology,because it permits all objects to produce intelligent service and interactive communication through wired or wireless networks. Moreover, the IoT trade is deemed the core industrial field of the long run. IoT provides convenient and effective services in anywhere at any time, on the far side the technical and economical restrictions, still because the temporal and spatial limits by providing services needed in numerous varieties of fields. It also aids the distribution of intelligent terminals which incorporates good phones, in conjunction with the advancement of knowledge and communication technology.Meanwhile, the demand on convenience and speed has augmented within the economic sectors of contemporary society. The monetary sector, amongst alternative fields, need IoT technology as mentioned above. monetary institutes have augmented the distribution of unmanned and automatic machines to strengthen aggressiveness by advancing monetary services, streamlining the business processes, automating the system, and ultimately reducing prices. [5]

Iot Functional Blocks

An IoT system is comprised of a number of functional blocks to facilitate various utilities to the system such as, sensing, identification, actuation, communication, and management. [1]

Maintaining the Integrity of the Specifications

Communication: The communication block performs the communication between devices and remote servers. IoT communication protocols generally work in data link layer, network layer, transport layer, and application layer.

Services: An IoT system serves various types of functions such as services for device modeling, device control, data publishing, data analytics, and device discovery.

Management: Management block provides different functions to govern an IoT system to seek the underlying governance of IoT system.

Security: Security functional block secures the IoT system by providing functions such as, authentication, authorization, privacy, message integrity, content integrity, and data security.

Application: Application layer is the most important in terms of users as it acts as an interface that provides necessary modules to control, and monitor various aspects of the IoT system. Applications allow users to visualize, and analyze the system status at present stage of action, sometimes prediction of futuristic prospects.

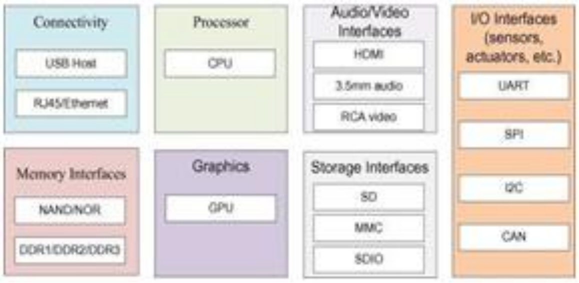

Figure 1. IoT device components.

Utilities Of Iot

IoT may be characterized as the holder of key utility factors as given below [1]

Dynamic and self adapting: IoT devices and systems should have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user's context, or sensed environment. For example, consider a surveillance system comprising of a number of surveillance cameras. The surveillance cameras can adapt their modes (to normal or infra-red night modes) based on whether it is day or night. Cameras could switch from lower resolution to higher resolution modes when any motion is detected and alert nearby cameras to do the same. In this example, the surveillance system is adapting itself based on the context and changing (e.g., dynamic) conditions.

Self-configuring: IoT devices may have self-configuring capability, allowing a large number of devices to work together to provide certain functionality (such as weather monitoring). These devices have the ability to configure themselves (in association with IoT infrastructure), setup the networking, and fetch latest software upgrades with minimal manual or user intervention.

Interoperable communication protocol: IoT devices may support a number of interoperable communication protocols and can communicate with other devices and also with the infrastructure.

Unique identity: Each of IoT device has a unique identity and unique identifier (such as IP address or URI). IoT systems may have intelligent interfaces which adapt based on the context, allow communicating with users and environmental contexts. IoT device interfaces allow users to query the devices, monitor their status, and control them remotely, in association with the control, configuration and management infrastructure.

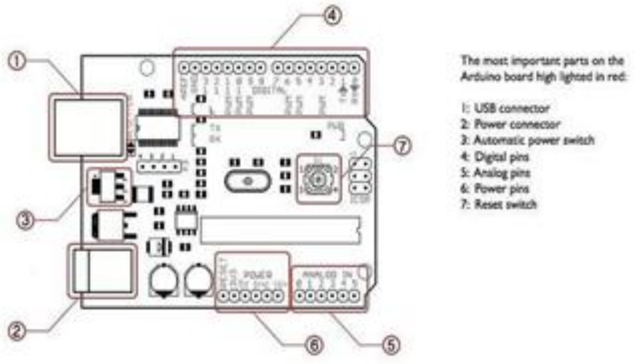

Fig 2:Arduino –UNO board Description

Context-awareness: Based on the sensed information about the physical and environmental parameters, the sensor nodes gain knowledge about the surrounding context. The decisions that the sensor nodes take thereafter are context-aware.[2]

COMPONENTS USED

A.Arduino-Uno:

Arduino is an open source computer hardware and software company, project, and user community that designs and manufactures single-board microcontrollers and microcontroller kits for building digital devices and interactive objects that can sense and control objects in the physical world. The project's products are distributed as open-source hardware and software, which are licensed under the GNU Lesser General Public License (LGPL) or the GNU General Public License (GPL)[3],permitting the manufacture of Arduino boards and software distribution by anyone. Arduino boards are available commercially in preassembled form, or as do-it-yourself (DIY) kits.

Arduino board (Fig.2) designs use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits. The boards feature serial communications interfaces, including Universal Serial Bus (USB) on some models, which are also used for loading programs from personal computers. The microcontrollers are typically programmed using a dialect of features from the programming languages C and C++.

A radio frequency identification reader (RFID reader) is a device used to gather information from an RFID tag, which is used to track individual objects (Fig-3). Radio waves are used to transfer data from the tag to a reader. RFID is a technology similar in theory to bar codes. However, the RFID tag does not have to be scanned directly, nor does it require line-of-sight to a reader. The RFID tag it must be within the range of an RFID reader, which ranges from 3 to 300 feet, in order to be read. RFID technology allows several items to be quickly scanned and enables fast identification of a particular product, even when it is surrounded by several other items. RFID tags have not replaced bar codes because of their cost and the need to individually identify every item.

Researchers have developed an RFID-SN i.e., RFID enabled Sensor Network, Buettner et al. (2008) comprising of RFID tag, reader, and computer system for understanding system behavior. Fosstrak one has developed a novel RFID related application based on SoA management (Foss track). Scientists have proposed an EPC network[4] configured RFID reader based system by catering multiple data related services on its application layer e.g., aggregation, filtering, lookup and directory service, tag identifier management, and privacy, utilizing the SoA paradigm.

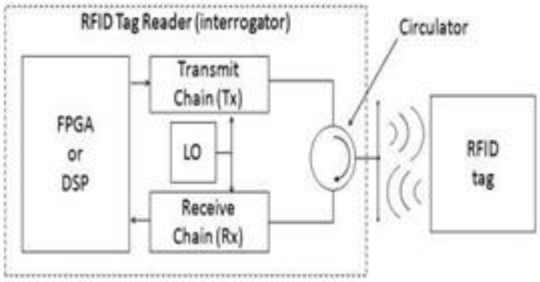

Fig-3:RFID reader operation.

C.Servo Motor:

Servo implies an error sensing feedback control which is utilized to correct the performance of a system. It also requires a generally sophisticated controller, often a dedicated module designed particularly for use with servomotors. Servo motors are DC motors that allows for precise control of angular position. They are actually DC motors whose speed is slowly lowered by the gears. The servo motors usually have a revolution cutoff from 90° to 180°. A few servo motors also have revolution cutoff of 360° or more. But servo motors do not rotate constantly. Their rotation is limited in between the fixed angles.

A servo motor consists of three wires- a black wire connected to ground, a white/yellow wire connected to control unit and a red wire connected to power supply. The function of the servo motor is to receive a control signal that represents a desired output position (Fig.4) of the servo shaft and apply power to its DC motor until its shaft turns to that position.

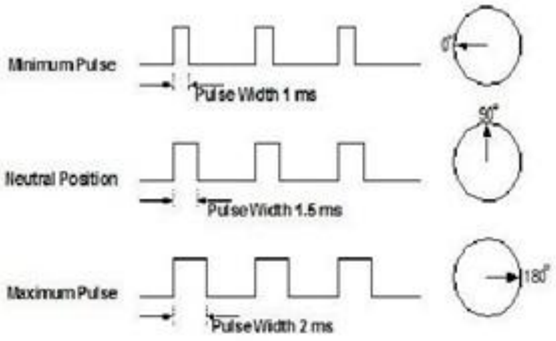

Fig.4:Servo motor working

D.Gsm Module:

GSM (Global System for Mobile Communications, originally Groupe Spécial Mobile) is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation digital cellular networks used by mobile devices such as tablets, first deployed in Finland in December 1991.

2G networks developed as a replacement for first generation (1G) analog cellular networks, and the GSM standard originally described as a digital, circuit-switched network (Fig.5) optimized for full duplex voice telephony. This expanded over time to include data communications, first by circuit-switched transport, then by packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution, or EGPRS).

Subsequently, the 3GPP developed third-generation (3G) UMTS standards, followed by fourth-generation (4G) LTE Advanced standards, which do not form part of the ETSI GSM standard.

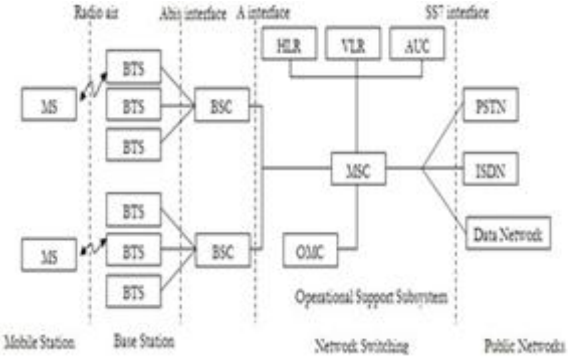

Fig.5:GSM Architecture

EXPERIMENTATION

A.Installation:

Download Arduino.lnk file from the server. Install Arduino.exe file. Run the software.

B.Reading Data from the Rfid tags:

Download MFRC522 library file created by miguelbalboa. Install the RFID library in Arduino UNO. Upload and view it in the serial monitor. Read data from RFID. For reading data from a RFID tag, we are taking electromagnetic RFID cards and RFID keychain. The working principle is shown in the (fig.6)

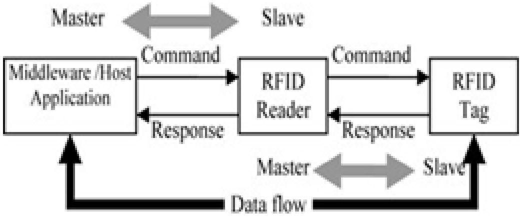

Fig.6:Working principle of RFID

C.Accesing Correct Data:

Add the UID of the card we need to give access. Upload the code and view it in serial monitor. Let the reader and the tag closer. It will show the status of the authentication.

D.Experiment with Door Locks:

Connect the servo motor with the Arduino-UNO board as given in the connection diagram. Write down coding for operating with servo motor. Now let the RFID tags closer to the Reader. Follow the status of the device.

E.Working with Gsm Module:

Connect Arduino UNO to the GSM Module(Fig.7). Access the module for sending automatic SMS when the RFID reader is ready to be sensed at anytime. The SMS will be the status of the device sensed.

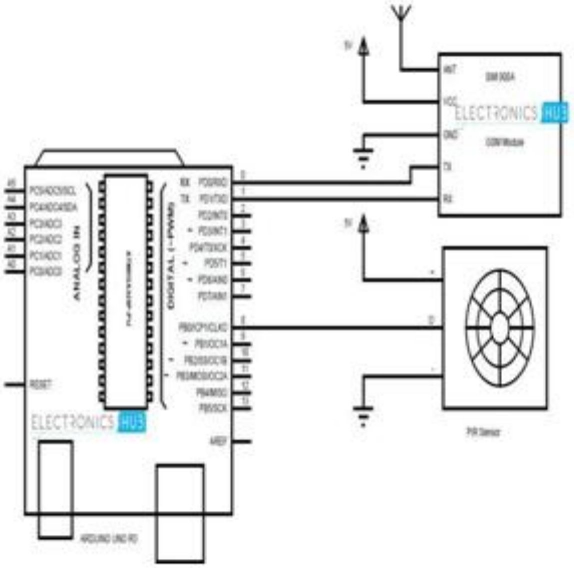

Fig.7:Circuit diagram of Arduino via GSM

CONCLUSION

The proposed work approaches with the recent IoT technologies along with the mobile communication techniques to authenticate the status of the conventional device. Thus, this study has been approved for security and safety issues. The future work may include the accessing permission which is to be given by the property owner for more security measures.

REFERENCES

[1] Sebastian, S., Ray, P.P., 2015. Development of IoT invasive architecture for complying with health of home. In: Proceedings of I3CS, Shillong, pp.

[2] G. Yang, X. Li, M. Mäntysalo, X. Zhou, Z. Pang, L.D. Xu , S.K. Walter, Q. Chen, L. ZhengA,2014 health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor and intelligent medicine box.

[3] Justin Lahart (27 November 2009). "Taking an Open-Source Approach to Hardware". The Wall Street Journal.

[4] C. Floerkemeier, C. Roduner, M. LampeRFID application development with the Accada middleware platform

[5] J.-i. Jeong,Department of Law, Kyonggi University, Iui-Dong, Yeongtong-Gu, Suwon-Si,
Gyeonggi, South Korea