IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

IOT Based Smart Anti-Theft System

Rutuja Patil, Sarthak Lolge, Samruddhi Patil, Pranav More
Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik

Abstract: *The fundamental idea is to design a cost-effective and efficient system for an individual to be able to detect any kind of theft in real-time and provide instant notification of the theft to the house owner or shop owner. Current system is designed for safety, protection of people, places and properties which should be kept locked when not in use to have a secured home, but there has been high level of concern with issues of security and safety with doors and its structure. This project is concentrates primarily on the security aspects by listing the typical security challenges in IOT systems in general and summing these challenges up to develop a functional and secure product from scratch. Current system is designed for safety, protection of people, places and properties which should be kept locked when not in use to have a secured home, but there has been high level of concern with issues of security and safety with doors and its structure. At present, most doors are under mechanical lock and key which are not adequately secured from authorized individual.*

Keywords: Sensors, IoT Technology, Alarm, Equipment Control.

I. INTRODUCTION

IOT is generally considered as “Infrastructure of information Society”, it enables us to obtain the data by each and every type of mediums like animals, kitchen appliances, humans, vehicles. Without human intervention IOT connects the physical objects that can exchange and communicate information between them. In the modern era, security and surveillance are important issues. Recent acts of theft/terrorism have highlighted the urgent need for efficient video surveillance and on-the-spot notification of ongoing thefts to house owners and other household members. This project is concentrates primarily on the security aspects by listing the typical security challenges in IOT systems in general and summing these challenges up to develop a functional and secure product from scratch. A microcontroller is chosen for this project and a test environment is built to experiment and develop the security breaches. Architectural designs are chosen for the API being developed and even for the Android Application. A detailed description is made of the multi-master database represented by Azure active directory and its importance to achieving the security of an essential security breach.

II. PROBLEM DEFINATION

Conceptual Security has consistently been a significant worry to the general public either in the family units or the workplace condition. There are different methodologies set up to address these issues. This venture is proposed to build up a savvy locking framework utilizing the Internet of Things. Utilizing conventional keyed locks is basic since the start of humankind, anyway there is a high risk of keys being lost or getting into inappropriate hands.

III. OBJECTIVE OF SYSTEM

1. **Reduced Installation Costs:** First and foremost, installation costs are significantly reduced since no cabling is necessary. Wired solutions require cabling, where material as well as the professional laying of cables (e.g. into walls) is expensive.
2. **System Scalability and Easy Extension:** Deploying a wireless network is especially advantageous when, due to new or changed requirements, extension of the network is necessary. In contrast to wired installations, in which cabling extension is tedious. This makes wireless installations a seminal investment.
3. **Aesthetical Benefits:** Apart from covering a larger area, this attribute helps to full aesthetical requirements as well. Examples include representative buildings with all-glass architecture and historical buildings where design or conservatory reasons do not allow laying of cables.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

IV. LITERATURE SURVEY

1. A smart door system which can be controlled by the android application installed on smart phone is proposed in this paper. Earlier, smart locks were used which enhanced the security features of the house. The proposed model can eliminate the concept of lock system as here the security is provided to the door itself. This would result in a safe and secure door with no locks! Controlling the movement of the door is enabled by Raspberry pi and its related embedded software. Also merging IOT with android is has many advantages in terms of security. The motion sensors are used to detect any movement in front of the door.
   If any person comes in front of the door, a motion is triggered; the image is captured and notified to the owner. Thus, in overall proposed system, two technologies are concentrated on, one is motion sensing in the front of the door in real time even if there is no one at home and the second is to control the movement of the door by the smart phone. Thus, by connecting a mobile phone to a door, the owner gets notified whenever any visitor visits his home and looking up to the images, the owner of the home can send the open-door signal for only the trusted visitors.
2. In recent trends, smart buildings have become the base for the Internet of Things (IoT). The usage of the internet is increased by connecting the devices in the homes to make the places more comfortable, provident, delightful, and secure. The proposed approach addresses a security aspect in smart home technologies, namely the door lock system. The door lock system determines the security by allowing the owner to monitor the buildings with a Smartphone-controlled, Bluetooth-connected system using Arduino UNO.
   Users can open or close the door lock by installing the developed android application in devices like tablets, smartphones, laptops, etc. by providing the login credentials like username and password which is verified in the database over the internet. If the credentials are invalid, the buzzer rings and an SMS alert is sent to the owner of the building which enhances the security. This approach can further be scaled to commercial sectors like ATMs, vending machines, etc. by using other wireless communication.
3. The trend towards smart cities that use devices based on IOT has been rapidly adopted across the globe. The devices in the smart cities are connected to database and key features include convenience, economical, and most importantly secure. In this paper a biometric authentication based automated secure and smart IOT door lock is developed. The access to authorized user is accomplished by face recognition. Further a provision for passcode-based authentication and access has also been incorporated. The proposed door lock takes care of the user comfort by eliminating the need of carrying keys or RFID cards. An email and app-based notification system is also incorporated that collects the data and also informs and alerts the end user.
4. IoT (Internet of Things) has a large portion of our life. This is manifested by the large number of connected devices. With the exponential growth of IoT devices, IoT security is becoming important. In particular, Smart Door Lock system is extremely important because it is closely related to the safety of the user. However, the data sent and received of existing Smart Door Lock system is vulnerable to forgery and hacking.
   To improve these security issues, we propose a Smart Door Lock system based on blockchain. Also, this provides data integrity and non-repudiation. Lastly, we propose an algorithm that the Smart Door Lock system judge some situations around itself and operates based on data sent from sensors

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

V. SYSTEM ARCHITECTURE

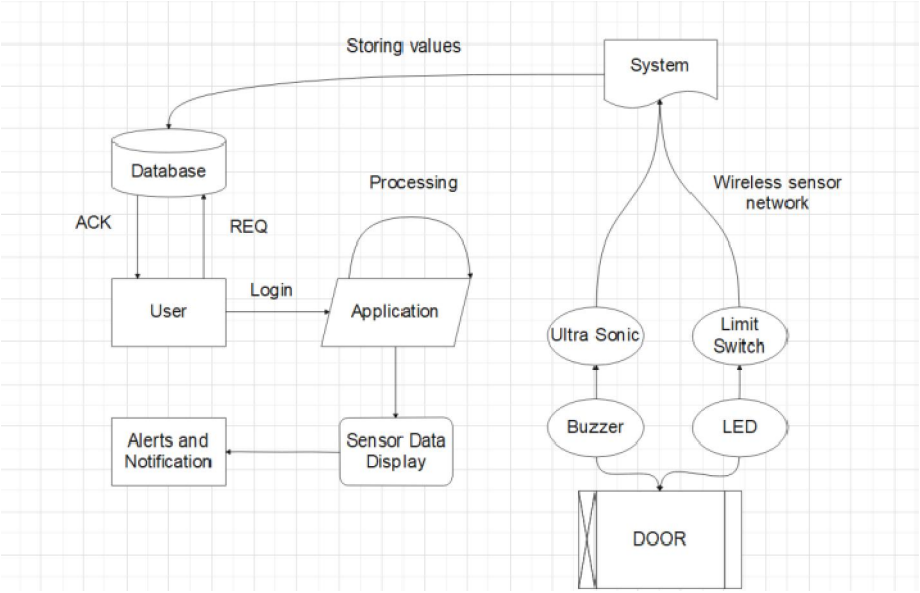

Fig -1: System Architecture Diagram

VI.ADVANTAGES

- Easy to used system
- Control system from anywhere
- Centralized system

VII. SYSTEM REQUIREMENTS

- **Software Used:**
  1. Operating System: Windows XP and later versions Front End: HTML,CSS.
  2. Programming Language: Python
  3. Tool: Arduino IDE
  4. Domain: IOT
  5. Algorithm: Hashing.

- **Hardware Used:**
  1. Processor – i3 or above
  2. Hard Disk – 150 GB
  3. Memory – 4GB RAM
  4. Ultra Sonic Sensor
  5. Relay
  6. Limit Switch
  7. Cables
  8. Buzzer

VIII. ALGORITHMS

Hashing & Mapping:

A cryptographic hash function (CHF)is a mathematical algorithm that maps data of an arbitrary size (often called the "message") to a bit array of a fixed size (the "hash value", "hash", or "message digest").It is a one-way function, that is, a function for which it is practically infeasible to invert or reverse the computation. Ideally, the only way to find a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

message that produces a given hash is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes. Cryptographic hash functions are a basic tool of modern cryptography.

IX. CONCLUSION

Hence, In the proposed framework, IT Lab automation system Hence we can conclude that This project presents an innovative method to prevent smart home or shop [theft by providing spontaneous notification of ongoing intrusion. The research has provided a novel wireless sensing system for the surveillance and detection of a human intruder as well as instant notification of the intrusion to prevent theft, we are also providing the system which will allow user to control the home equipment's from anywhere using internet.

REFERENCES

[1] M. Mendez, J. Carrillo, O. Martin, C. Tchata, P. Sundaravadivel and J. Vasil, "Easy Yard: An IoT-Based Smart Controller for a Connected Backyard", IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), pp. 257-261, 2019.

[2] P. Wilmoth and P. Sundaravadivel, "An Interactive IoT-based framework for Resource Management in Assisted living during pandemic", 22nd International Symposium on Quality Electronic Design (ISQED), pp. 571-575, 2021.

[3] A. Sallah and P. Sundaravadivel, "Totmon: A real-time internet of things based affective framework for monitoring infants", 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 600-601, 2020.

[4] Jing Sun and Xiaofen Zhang, "Study of ZigBee Wireless Mesh Networks", Proc. 9th IEEE International Conference on Hybrid Intelligent Systems, pp. 264-267, 2009.

[5] Kwang Koog Lee, Seong Hoon Kim, Yong Soon Choi and Hong Seong Park, "A Mesh Routing Protocol using Cluster Label in the ZigBee Network", Proc. 2006 IEEE International Conference on Mobile Ad hocand Sensor Systems (MASS'06), pp. 801-806, 2006.