IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

IoT Device Authentication and Authorization

Raj Patil, Aman Tickoo, Kunal Golhait, Akanksha Nandre
Students, Department of Information Technology
Smt. Kashibai Navale College of Engineering, Pune, Maharastra, India

Abstract: *With the rapid development of the Internet of Things in the market, companies have a tendency to focus on and what time to go to the market and introduced a product to the market as quickly as possible, instead of creating a safe and essential to the product. This allows for a lot of Things, for products with insufficient protection against different types of attacks. For the safety and security of the Internet of Things is an ever-growing problem, and even with a large amount of research on this topic, and there's not a lot of significant work in the area of approximation or standardization, which could solve the problem. For the safety and security of the Internet of Things, which is of great importance, as are the consequences of a breach of the security, the Internet of Things, it can be catastrophic. The breaking up of a smart car, and a lock of it to the lock, it can lead to a product, or theft of, or even the victims, and in some extreme cases. Even if one is not detected, a breach, will not work, but it is still there, it shows that the product in question is a false sense of security, and that it is ethically unacceptable.*

Keywords: Internet of Things, Smart doors, Testing, Security and Authorization

I. INTRODUCTION

For the safety and security of the Internet of Things, which is of great importance, as are the consequences of a breach of the security, the Internet of Things, it can be catastrophic. The breaking up of a smart car, and a lock of it to the lock, it can lead to a product, or theft of, or even the victims, and in some extreme cases. Even if one is not detected, a breach, will not work, but it is still there, it shows that the product in question is a false sense of security in a way that is ethically unacceptable. Due to inconsistencies between the IoT product, its architecture, and as the technology used, it is not possible to do in order to be able to develop security measures, offering a wide range of different appliances. Therefore, IoT products are designed around the safety, not the other way around. The smart door lock will give us an example of the use of this project, and it will represent the typical Internet-of-Things device in today's world.

1.1 Objective

To offer high security and easy access control. The development phase will rather focus on delivering a prototype that is well-protected against malicious attacks than extensive user functionality. This can lead to a product that has high security. To provide safety and efficiency by making it easier for people to get around

1.2 Motivation

The obvious reason for doing this kind of remote access to a door on the lock was at the house, organizations, education institutions, faculties, it is much safer and will be able to remotely unlock or lock the doors in front of the guests, etc., etc. This operation ensures that the user does not need to worry about is whether or not the door has been left open or not, and it is, therefore, a guarantee for added peace of mind for you.

1.3 Purpose of System

The main challenge for this project was the privacy and the security of the IoT-based systems. Therefore, the project is a comprehensive study of the security and privacy of the IoT-based systems, focusing on the improvement of the lock mechanism to connect to the Internet, so it's a safe, productive, and reproductive health.

1.4 Scope

The goal of the project is to construct and IOT system. The system should be secure and user-friendly. The main goal has been allocated to the following subgoals

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

1. The Construction of a network architecture, in terms of safety, security, and functionality.
2. The Creation of a safe and secure method for determining that the user is in the physical proximity of the lock of the door.
3. To Achieve the correct authentication policy for users trying to gain access to the front door.
4. Create a server in python that can be used as a user terminal.

II. Problem Statement

In the aspect of security is the greatest concern is associated with the IoT or entity of such changes. The data that may be personal, business or personal. To achieve an acceptable implementation of a smart door lock (SDL), a security is considered to be a serious problem. Let's summarize the problems in the various questions

1. How do we make the high and safe authentication of the user of the point object in the API, and the house has a strict privacy safeguards?
2. What can we do to generate an access token for a user that has the privilege to be in order to unlock all of the doors, and how do we do this holder is, in many ways.
3. What is the connection protocols that can be used in the product, and give you the ability to verify and access management? The local Wi-Fi network to meet the security obligations?
4. Which IOT platform, will comply with the product for the purpose of providing a safe and secure IoT system.

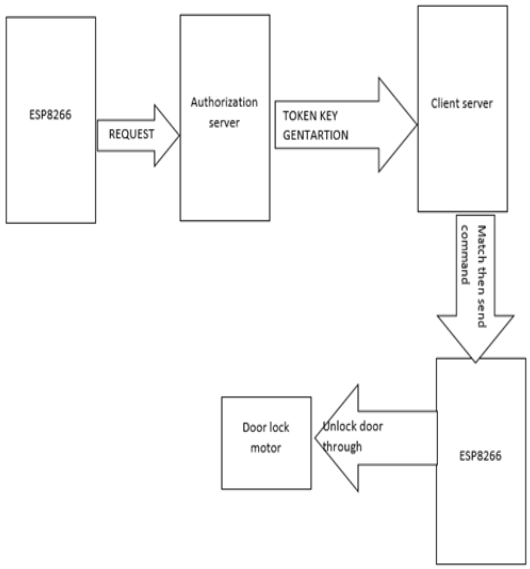


Figure 1: Architecture of System

The flow that system follow is:

1. ESP8266 send request to Authentication server.
2. Authentication server generate token to the client server.
3. Client server key match then the client server and command.
4. The ESP8206 received command and door lock will be open.

A Smart-Lock is an electromechanical lock which is designed to perform locking and unlocking services on a door when it gets such instructions from an authorized device using a wireless protocol, Bluetooth, and a cryptographic key to perform the authorization process. It also manages access and sends signals for the different roles it controls and some other important functions connected with the status of the device.

III. Proposed System

With the smart door system allows you to direct the automation of the owners. Of course, you may have seen automatic door openers, in malls, theaters, and office buildings. These systems can be used to open the door, when a person is

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

approaching the end of the handle of the door and plug it in after you enter the door.

In this project, is to provide a system for the automatic opening and closing of the door, sensing the movement of the body, near the front door. This is achieved by using a PIR (passive infrared) sensor is used.

IV. IMPLEMENTATION

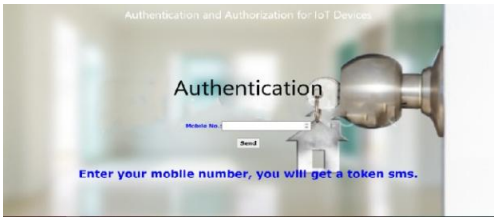
We used double Authentication and authorization technique so that we achieved strong security design system This system is implemented in hardware +software.

1. In this project switch is connected to node MCU (ESP8266) first switch gets pressed so that REQUEST is first comes into PHYTON then in python page it will show ENTER YOUR MOBILE NO
2. After that mobile no is entered so that TOKEN is generated .for TOKON generation PN sequences algorithm is used which will generate random tokens for different mobile no.
3. Then generated TOKEN is Authentication in system if TOKON is Authenticated ,then again REQUEST is goes to second node where motor are connected .again it will verify that received TOKEN then it will open the door.
4. If in case mobile no is not verified in that case it will generate information of that person like it will send photo to telegram account of owner and based on telegram account owner will decide to give access to that unknown person based on command of second NODE MCU.
5. The message will be the “unauthorized person trying to access your door lock” is sent to owner of door bell

V. RESULT

Switch is pressed to open the door

Mobile is entered for generation of token

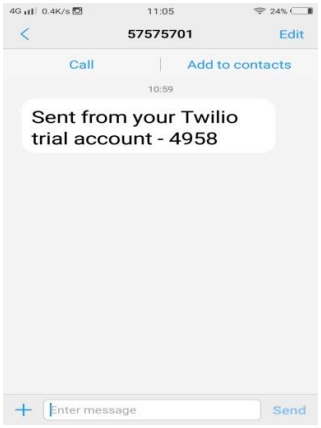


Token is generated for authentication.

Token is verified for opening door

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

If unknown is try to access the doorbell then SMS is send on telegram



Based on token it will decide to give access or not

VI. ADVANTAGES

1. To provides automated security to our home.
2. It is Reliable.
3. Easy to use.
4. System have been secured by sensor authentication.

VII. DISADVANTAGES

1. If you use a different locking mechanism, you won't be able to use them. And if the door isn't firmly closed, the smart lock may not secure the deadbolt.
2. Smart locks can also control the locks of one door, and technological issues can set you back. If the battery fails, you may find yourself locked out.

VIII. CONCLUSION

In this project we used double Authentication and authorization technique so that we achieved strong security design system .and no one can easily hack this system. Also in this system the algorithm used for token generation is PN sequence which will generate random TOKEN so no one can access this system and hack the system

IX. FUTURE SCOPE

In future, the android application should offer assistance in controlling more doors, windows and basic home electronic appliances. Battery backup system should also be considered to ensure the completeness of the system. An auto trigger report of the attempt to theft can be sent to nearest police station along with residential address. This idea can be considered to make the proposed system better.

ACKNOWLEDGMENT

The authors would like to thank Prof. A. D. Londhe for his/her help. This work was supported in part by the National Science Foundation under grant no. XXXXX, etc.

REFERENCES

[1]. S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia, and G. Bianchi, OAuth-IoT: an Access Control Framework for the Internet of Things Based on Open Standards, in Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC). IEEE, July 2017.

[2]. S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios, IEEE Sensors J., vol. 15, no. 2, pp. 1224?1234, Feb. 2015.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

[3]. Sebasti an Echeverr a, Grace A. Lewis,Dan Klinedinst,Ludwig Seitz, Authentication and Authorization for IoT Devices in Disadvantaged Environments 2019 IEEE 5thWorld Forum on Internet of Things (WF-IoT)

[4]. Smart Door Locking System using IoT, Karthik A Patil, Niteen Vittalkar, Pavan Hiremath, Manoj A Murthy ,Student, School of Computing and Information Technology, REVA University, Bengaluru, India

[5]. IoT Based Smart Security and Home Automation System, Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana Department of Electronics and Communications Engineering National Institute of Technology, Warangal.