INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 5)
Available online at: www.ijariit.com

Algo locking system

Sripriya Annepu
sripriyaannepu@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Sahaya Sakila. V
shyla1992lipna@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

N. Saiteja
sai.tejaomkar@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

N. Vishnu Kiran
nvishnukiran222@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

ABSTRACT

Wireless accessing and monitoring the control system time to time. This is mainly based on sensors and security authentication to the conventional device. There are a unit security issues just in case of lost keys. An innovative lock system epitome mistreatment today's technologies square measure given. The novelty of this epitome depends on the very fact that victimisation new technologies at the side of recent ones can lead to a wise and a lot of economical.

Keywords— *Double authentication, Sensors, Module, Central control*

1. INTRODUCTION

The main aspect of the project is that to open the lock and a double authentication procedure has to be done before. Consider if a user tries to login with his credentials in a given system present in that particular room/place. Because the login page will be connected to only that particular server and it will be restricted to that particular place.

The login page cannot be opened if the user is not connected to that particular server. And after the user successfully logins into the page a verification number will be sent to user mail. This verification number has to be entered in the second page i.e., the confirmation page and then after successful authentication, the locker will be opened.
Many safety measures like password encryption server security are enhanced.

2. EASE OF USE

2.1 Advanced encryption standard

The Advanced Encryption commonplace or AES could be a regular block cipher chosen by the US Government to guard classified info and is enforced in package and hardware throughout the planet to cipher information.

2.2 Authentication server

The Central Authentication Service (CAS) could be a single sign-on protocol for the online. It conjointly permits internet applications to certify users while not gaining access to a user's security credentials, like a countersign.

3. EXISTING SYSTEM

In the traditional architecture, the server was only meant to store data. The security then was very weak and all the automation had to be done only on the client side which was an expensive maintenance. In this, every client has to be trained on how to use the application.

Security in the existing system is the motivation factor for a new system with a higher level security standards for the information exchange. Previously the servers had a very weak security system which provided good vulnerabilities to the hackers. And the server was also not that effective (i.e speed, amount of storage etc).

Passwords and confidential data were always exposed in the database as it is. These were never in an encrypted form. Thus this also became a vulnerability to the hackers. They steal the information from the database and re-modify everything according to their needs.

Databases were not that advanced to note down everything when an activity takes place. As mentioned earlier there is was no automation in the server side.

4. DOUBLE AUTHENTICATION SYSTEM

Nowadays the technologies have emerged so much that anything can be done with a touch. As the security was the main flaw in many systems which existed before, we have come up with a security system which has minimal flaws. Automation is taken care in the server side itself. Database management is all automated.

For security development, we have implemented a double authentication in the system which reduces the flaws in the security. When the user logins from the portal page, the user gets a validation code into his mail for the authentication

purpose. All these details of login (i.e., user_id, the name of the user, date, time, etc) will be noted in the database automatically. And the validation code sent to the mail will be valid only for some certain amount of time. If the user fails to provide the validation code within time then the page automatically logs out.

The user can never enter into the server if he/she is not connected to the WiFi network provided, which is only restricted to the place where the locker is present. This restricts the third party access onto the server.

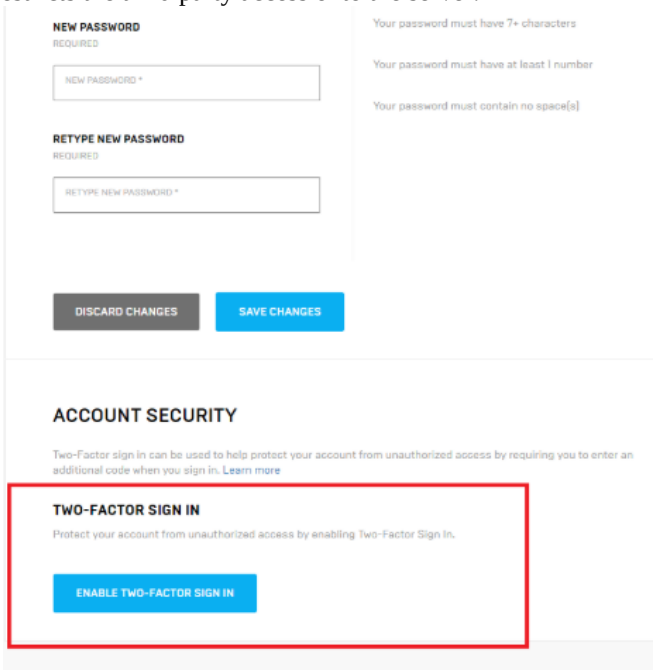

Fig. 1: Double authentication system

5. PROBLEM STATEMENT

The security towards the server side connections and the authentication part. Previously many systems were built on this domain but have failed in some of the other parts. We have come up with a system which guarantees minimal failure in the system.

Previously the server could be accessed from anywhere which led to a security threat. This became a vulnerability to the hackers who then hack into the server and try to steal the credentials from the database. But we ensure that the server will only be connected if the user is particularly connected to that wifi/module network. This happens only when the user is in that particular place where the locker is situated.

Passwords and many of the data formats were not encrypted in the previous models. And also when the user logins into the portal page the information was never stored (i.e at what particular time and day did the user login).

But this doesn't become a flaw in our model , we have ensured that all the credentials given will be encrypted and time to time, whenever a user tries to login into the portal page the details of the user, will be entered into the database (like users name, user_id, time, date, etc.) for security purposes.

Existing system: In the traditional architecture, the server was only meant to store data. The security then was very weak and all the automation had to be done only on the client side which was an expensive maintenance. In this, every client has to be trained on how to use the application.

Security in the existing system is the motivation factor for a new system with a higher level security standards for the information exchange. Previously the servers had a very weak security system which provided good vulnerabilities to the hackers. And the server was also not that effective (i.e., speed, amount of storage etc).

Passwords and confidential data were always exposed in the database as it is. These were never in an encrypted form. Thus this also became a vulnerability to the hackers. They steal the information from the database and re-modify everything according to their needs.

Databases were not that advanced to note down everything when an activity takes place. As mentioned earlier there is was no automation in the server side.

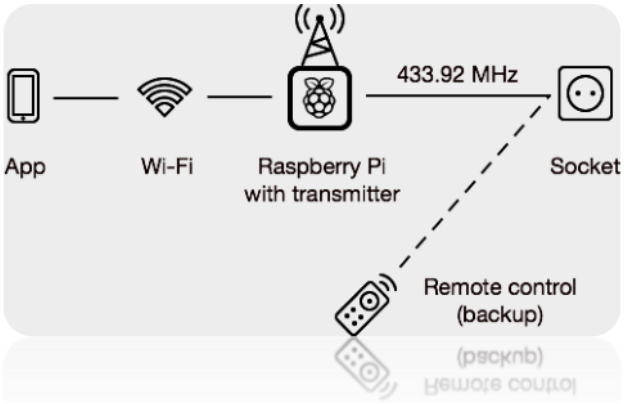

Fig. 2: Algo Flow

6. LITERATURE SURVEY

Smart lock systems are classified based on technology used as
1) Zig-bee module based,
2) z-wave wireless based,
3) RFID technology based,
4) Bluetooth connections based

6.1 Zig-bee module based systems

This can be split into 2 halves: the hardware half and also the code part.

The primary half deals concerning incorporating MCU with sensors, Zig-Bee design, and transportable to create an operating circuit that supports movability while not compromising responsibleness, and also the second half is to create a C-code for programming the MCU to watch and management secured atmosphere.

Fig. 3: Zig-bee module based systems

6.2 RFID Technology-based systems

RFID, frequency Identification is a cheap technology, are often enforced for many applications like security, plus trailing, individuals trailing, inventory detection, access management applications. The most objective of this paper is

to style and implement a digital security system which may deploy in a secured zone wherever a solely authentic person is often entered.

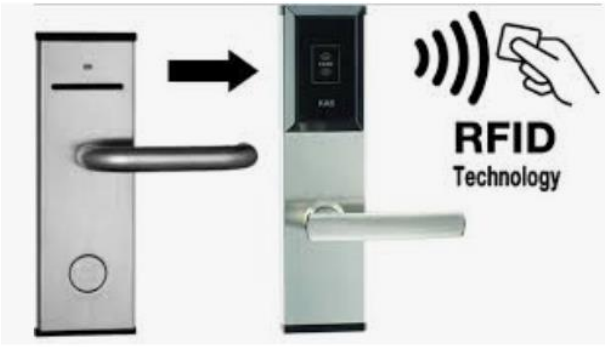

Fig. 4: RFID Technology-based systems

6.3 Z-wave technology-based systems

With our Z-Wave Door Locks, you may be ready to open any door remotely mistreatment your portable computer, telephone or pill. So now, you'll open the door for housecleaning, landscaping or the other service while not the necessity to be physically there. In addition, mistreatment any information science Camera you'll watch what and the way they're doing in your property. Door locks are often additionally related to any Z-Wave sensing element in your house and triggering the sensing element will open or lock the door. This is often extremely wherever home automation comes handy, it's straightforward, helpful and safe.

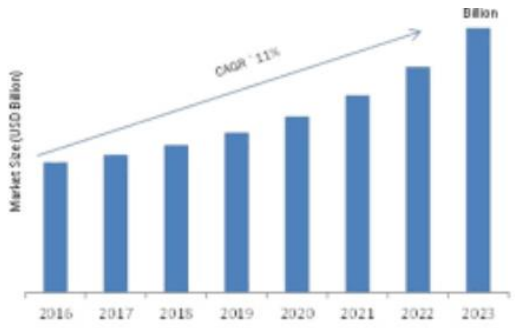

Fig. 5: Graph

6.4 Bluetooth Technology-based systems

The mobile device needs an arcanum to extend the security of the system. The hardware on the door uses a microcontroller to regulate a linear mechanism that acts because of the locking mechanism. The Bluetooth protocol was chosen as a communications technique as a result of it's already integrated into several golem devices and is secured through the protocol itself. It conjointly matches well into the look necessities of the project for a brief vary, wireless association method. Our good lock system can operate over a wireless network like Bluetooth.

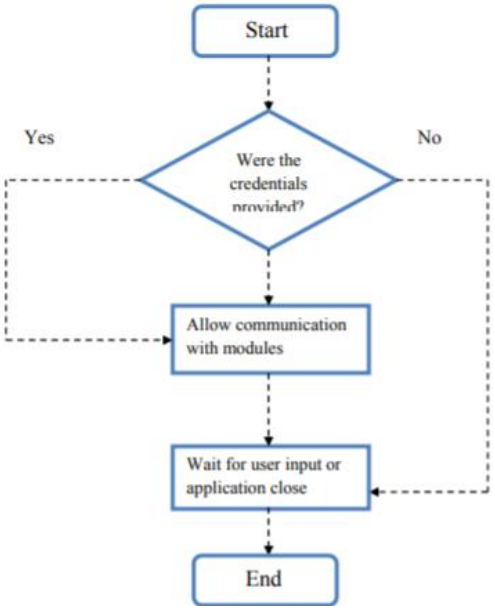

Fig. 6: The mobile application

7. ACKNOWLEDGMENT

We extremely indebted to Ms. Sahaya Sakila for her steerage and constant management furthermore as for providing necessary info relating to the project for her support in finishing the project.

8. REFERENCES

[1] T. V. A. Pham, 'Security of NFC applications', Master's thesis, Royal Institute of Technology, School of Information and Communication Technology, Stockholm, Sweden, June 2013, TRITA-ICT-EX;2013:125.
[2] Zig-bee module implementation, 2009-Smart Locking System.
[3] Blockchain technology, 2017-Blockchain used smart lock system.
[4] RFID technology and RABBIT microprocessor, 2018-Motion based smart lock system on Android platform.
[5] Intel Galileo Boards, 2018- Smart lock on Galileo board.
[6] Dual-tone multi-frequency module, 2014-Smart lock using DTMF polyphonic tone sensor
[7] Mobile App via Bluetooth, 2012-Intelligent Locking System.

