

# Enhanced Network Security in Personal Area Network with Reconfigurable Password

Bhuvaneshwari A J  
JRF/ECE Department  
SSN College of Engineering

Dr. P. Kaythry  
Associate Professor/ECE Department of ECE  
SSN College of Engineering

**Abstract:- Network security is an important technology for many applications. For network applications, security is a critical requirement. To defend systems from external attacks, network security is critical. Network security is essential to protect the systems from external threats. When it comes to a business, special precautions should be taken to protect shared data. Network security is one of the best ways to do so. Network security can be applied with different restrictions on different computers depending on the types of files they handle. Client and customer confidence is boosted, and your company is protected from the reputational and legal consequences of a security breach. Although several security tools have been developed to protect access to illegal Unauthorized users, problems still exist in society. With duplicate keys and unnamed tools, even traditional locks are vulnerable to steal. We should safeguard our network to avoid such a situation. Our indispensable objective is to design a tool to provide a greater secured multilevel protection and password reconfigure options in Personal Area Network. To triumph over the illegal authorization problem, we are going to develop a tool with a 2-way verification method. This provides a higher answer with multilevel security. Our proposed system offers extra security measures for transferring data in the network. It will act as a gatekeeper to the information and prevents illegal authorizers. It will protect a computer network and its resources from abuse, modification, or manipulation.**

**Keywords:-** Two-way Verification, Authentication, and Authorization, Network Security, Embedded Networks.

## I. INTRODUCTION

Nowadays everything is connected through networks. As we keep increasing the connectivity of physical devices, they often become susceptible to breaches in security. Network security is nothing but a set of rules and configurations that provides security to the integrity and susceptibility of devices. We see many issues that lock getting theft, so it becomes a fundamental requirement to provide locks with additional security. To overcome these issues, this Android-based totally safety locks with a Microcontroller provides a better solution with layered security and a more accessible GUI for the buyer to address in all paths of elements. Automobile ignition starters, schools, hospitals, residential areas, banks, and other major industries may all benefit from this type of technology. Because

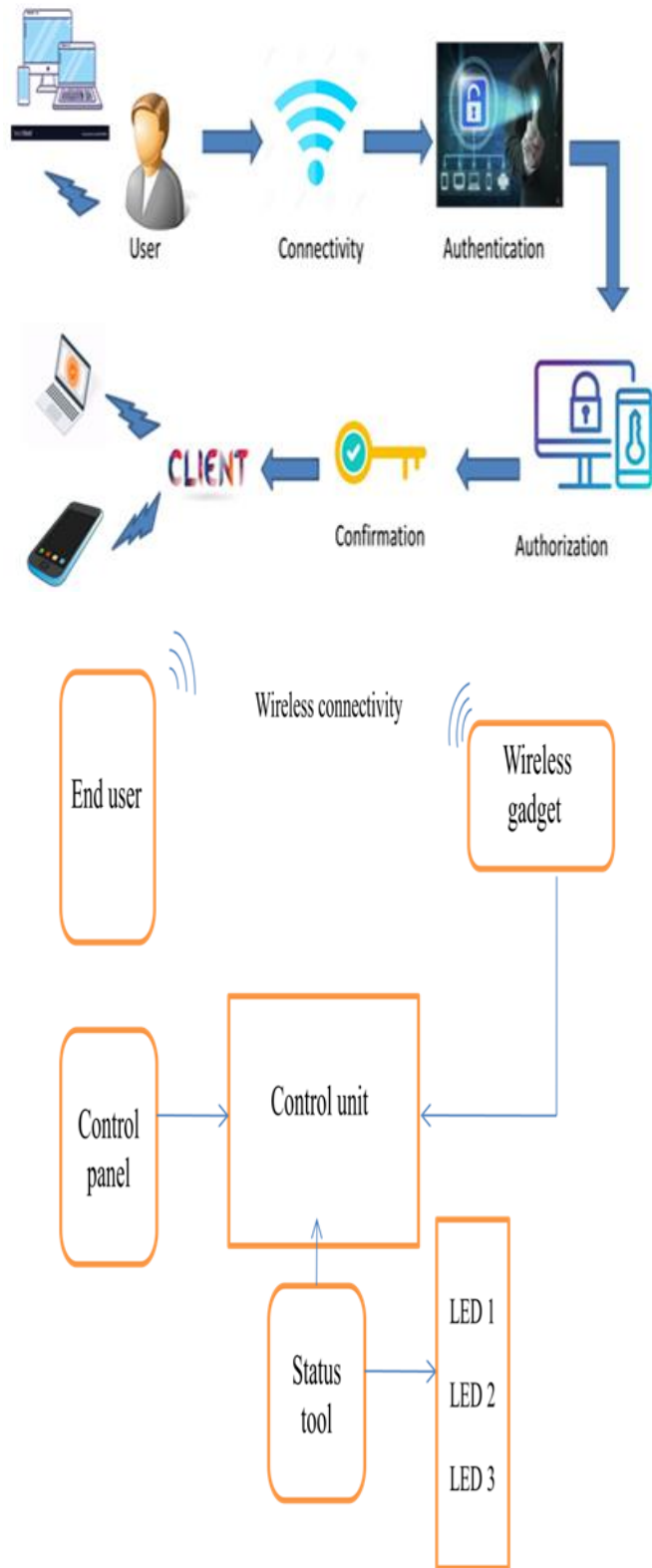
this lock is built into Android programmes, it is simple and secure for us. The system helps to reduce crime and unauthorized entry to our facilities. There is no option to utilizing traditional keys while using PAN devices such as Bluetooth. Unauthorized users will be unable to guess the location of the lock if hardware circuits related to our safety locks are installed inside the premises room. It will be difficult to expect the assistance of unknown women and men coming to bypass the protection because the password may have the maximum length with unusual characters. The phone of the legal person is also accessible, although passwords are converted using login templates.

## II. RELATED WORK

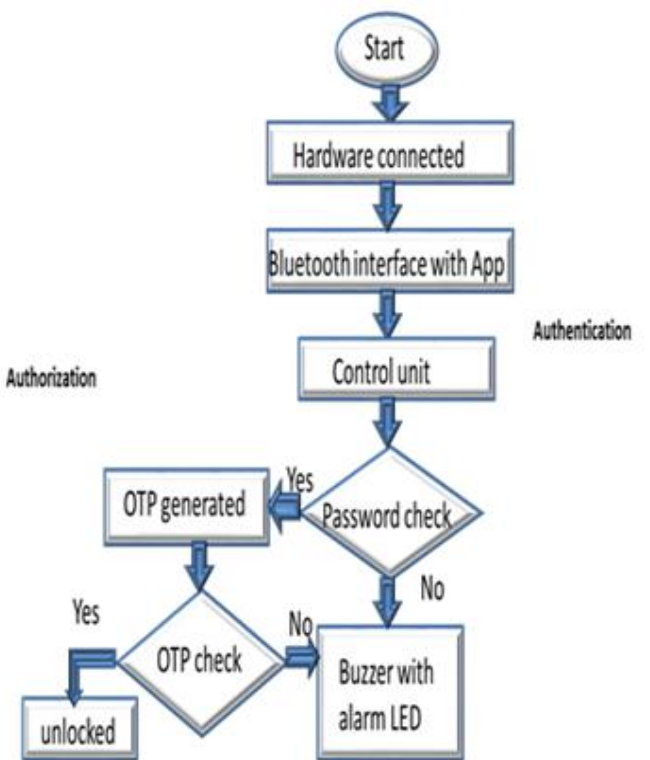
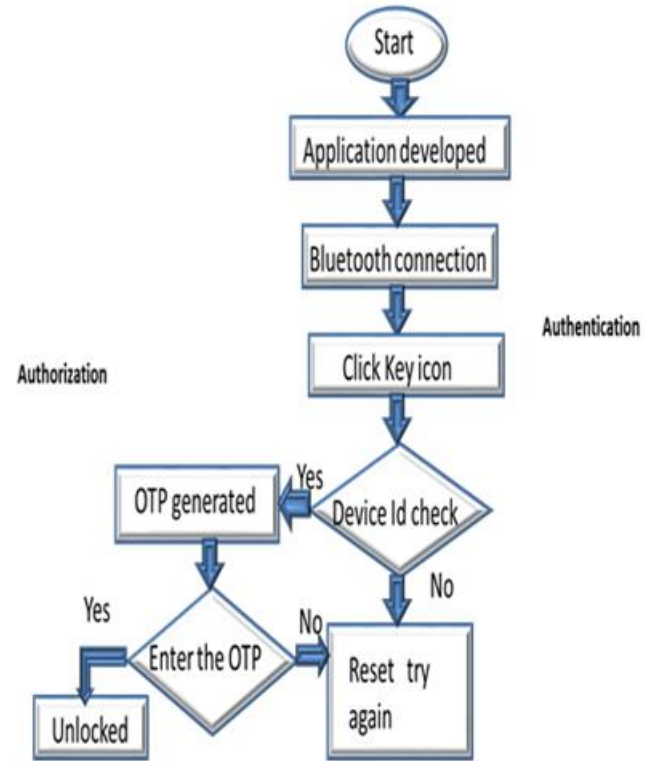
To access the device, the existing well-known solutions use a [1] default password and a changeable password configuration. The device password can be changed at any moment by a valid user. The password configuration option will be protected by a password, thus unauthorized users will not be able to access or change the password. [2] The lock cannot be opened even if the physical key is replicated. For device access, they employ a hex keypad, which is a wired network. [3] use face recognition as a locking and unlocking mechanism. It is user-friendly and specially developed for impaired individuals so that authorized people can easily utilize the device. [4] They use a key to open the lock here. A password is set by the user to safeguard the lock system. When the proper password is entered, the lock opens.

## III. PROPOSED SYSTEM

In networks, our suggested solution provides effective authentication and authorization. It focuses on end-user confirmation and authorization. It is executed using hardware and software modules. The hardware used is Arduino UNO which has an ATmega328P processor as a control unit. The programming for two way verification process is written in Arduino UNO.



**Fig 1a & b:** General & Functional Block Diagram of Proposed System



**Fig 2 &3:** Flow Chart for Application and Hardware Execution respectively.

*A. Procedure for two way verification*

**Step 1:** At first the user must install the security lock app on their Android smartphone.

**Step 2:** The user must enter the valid password which has been saved in the EEPROM previously.

**Step 3:** Only the privileged user can change the already existing password that shall be protected by one another password.

**Step 4:** When an erroneous password is entered, our device will sound an alarm and display the Lock's status.

**Step 5:** With the help of status LEDs, we can determine the condition of the lock during incorrect password entry, closing/opening, and password setup.

**Step 6:** A random generated OTP is delivered to the user's device through PAN device if the user enters the proper password for two-way verification.

*B. Procedure for Proposed System:*

**Step 1:** The device is connected through the wireless access points like connecting devices or the cloud network.

**Step 2:** The authorized client alone can be allowed by using the 2-way verification method:

1. Default password verification
2. OTP generation and verification

**Step 3:** The status of Connected/disconnected are displayed using LED and the facility of reset/change password are also included.

*C. Procedure for Functional Block Diagram:*

The functional block diagram describes the hardware units and the functions of the proposed system.

**Step 1:** The user is wirelessly connected to a gadget using IEEE 802.15 module with the control unit.

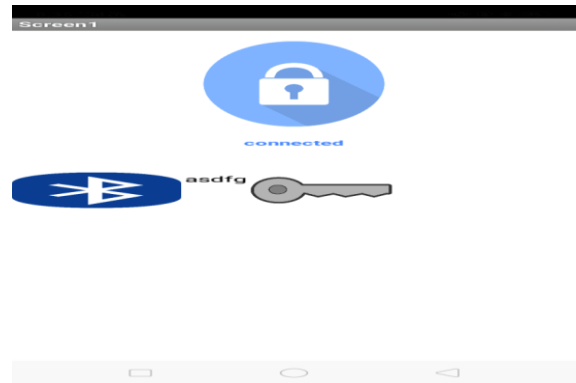
**Step 2:** The control unit we use is ATmega328P which connects the control panel and the status bar (LED1, LED2, and LED3).

**Step 3:** The status bar is used to display the status of the process like:

1. LED1: used to display light when the user entered the wrong password.
2. LED2: used to display light when the user is connected.
3. LED3: used to display light when the user is disconnected.

*D. Features*

- Achieve sensitive and secure data transfer
- Android-based safety lock.
- The microcontroller is completely secured.
- Convenient for users.
- Use of 2-way verification.
- No alternative use.

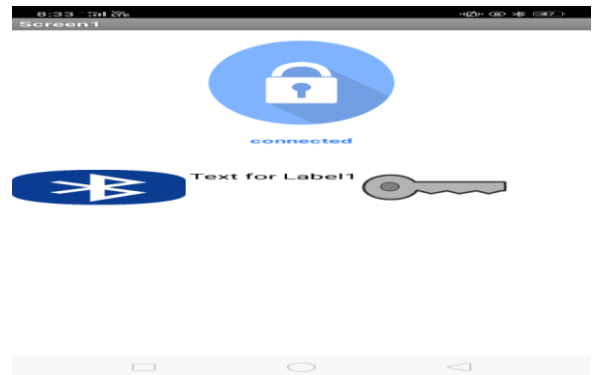


**Fig. 4:** Default Password Check

**Fig 4:** shows the user must enter the default password. When the key icon is touched, the user needs to enter the password.

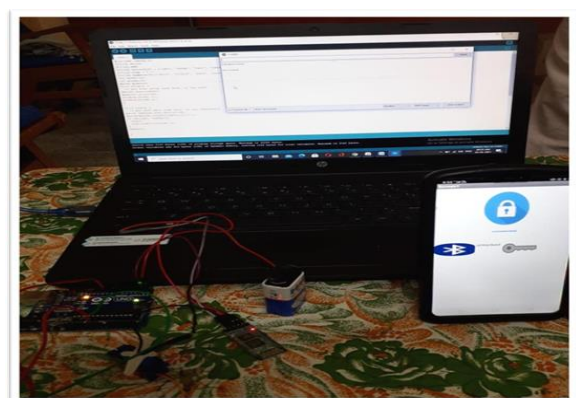
**IV. STIMULATION RESULTS**

The Programming for the two-way verification process is written and dumped in the Arduino module.

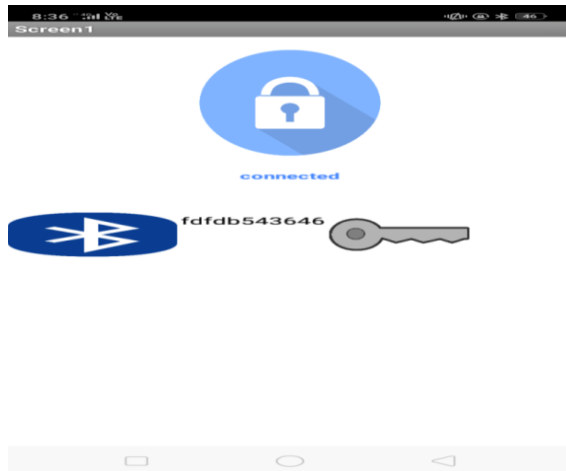


**Fig.5:** Application Overview

**Fig.5:** Android application interface with Bluetooth module.



**Fig.6:** Hardware Setup



**Fig.7:** OTP Generation

**Fig.7:** The device will check whether the default password is correct. If it matches, the One Time Password will be generated.

## V. CONCLUSION

In this paper, we proposed a new approach to secure a device based on a reconfigurable password setting application. This paper presents a basic concept for managing device protection in the home. It also ensures that users of Android smartphones are safe. Our project is extremely beneficial to users who have had to deal with the issue of unauthorized permission. The implementation rate is low-cost and affordable. The Android and Arduino platforms are used in this venture. Because the microcontroller has achieved Bluetooth connectivity, the device may be set up even more quickly. The design has been well-thought-out and prototyped. In this paper, we use a two-way verification mechanism to provide a simple prototype. In destiny, however, it can be extended in many areas. As a result, the reconfigurable password mechanism for the Personal Area Network has been designed. The suggested system focuses on the notions of authentication and authorization. As a result, the suggested security solution is ideal for data transfer and access applications.

## FUTURE ENHANCEMENT

The project model is effective. We intend to expand and implement this project in IoT (internet of things) in the future so that we may analyze and store data in the cloud and use it more effectively. It will be fully automated and suitable for smart city applications.

## REFERENCES

- [1]. N.H. Ismail, Zarina Tukiran, N.N. Shamsuddin, E.I.S Saadon, "Androidbased Home Door Locks Application via Bluetooth for Disabled People," 2014 IEEE International Conference on Control System, Computing and Engineering, 28 - 30 November 2014, Penang, Malaysia
- [2]. Ketan Rathod, Prof.Rambabu vatti, Mandar Nandre, Sanket Yenare, "Smart Door Security Using Arduino and Bluetooth Application," Indian technical Research organization, vol. 4, no. 11, 2017.
- [3]. Md. Maksudur Rahman, Mohammed Sowket Ali and Md. Shoaib Akther, "Password Protected Electronic Lock System for Smart Home Security," vol. 7, no. 4, April 2018.
- [4]. G. Kiruthikamani, B. Abinayaa, B. Saranya, P. Devi and R. Gayathri, "Smart Vehicle Safety System Using Arduino," International Journal of Trend in Research and Development, vol. 3, no. 6, pp. 804-807, December 2017.
- [5]. Bhaktishwar Rajiwade, Shital Thakar, Payal Pokharkar, Shankar Malbhare, "Design and Implementation of Smart Door Lock Control System using Bluetooth Controller of Smart Phone International Research Journal of Engineering and Technology (IRJET), vol. 3, no. 11, Nov. 2016.
- [6]. Jeffrey Schiller, Franklyn Turbak, Mark Friedman "Live Programming of Mobile Apps in App Inventor," October 2014
- [7]. Shweta Chanda, Deepak Rasaily, Prerna Khulal, "Design and Implementation of a Digital Code Lock using Arduino," International Journal of Engineering Trends and Technology (IJETT) – Volume 32 Number5-February 2016.
- [8]. Sutariya Hardik Jayantilal, "Interfacing of AT Command based HC-05 Serial Bluetooth Module with Minicom in Linux", IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 03, 2014.
- [9]. Anisha Cotta, Naik Trupti Devidas, Varda Kalidas Naik Ekoskar, "wireless communication using hc-05 bluetooth module interfaced with arduino", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 4, April 2016.
- [10]. Harshit Singhal, Abhishek Umrao and Ameer Faisal, "Android & Bluetooth Module Based Door Automation System" Advances in Computer Science and Information Technology (ACSIT), vol. 2, no. 12, July-September, 2015.
- [11]. Leo Louis, "working principle of arduino and using it as a tool for study and research", International Journal of Control, Automation, Communication and Systems (IJCACs), vol.1, no.2, April 2016