International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 9, ISSN No. 2455-2143, Pages 156-160
Published Online January 2023 in IJEAST (http://www.ijeast.com)

A REVIEW ON BLUETOOTH LOW ENERGY ENABLED DOOR LOCKING SYSTEMS

Ujwal Kumar N L
Department of Electronics and Communication
Vidyavardhaka College of Engineering
Mysuru, Karnataka, India

Vaishak S
Department of Electronics and Communication
Vidyavardhaka College of Engineering
Mysuru, Karnataka, India

Vinay N
Department of Electronics and Communication
Vidyavardhaka College of Engineering
Mysuru, Karnataka, India

Kavyashree B
Department of Electronics and Communication
Vidyavardhaka College of Engineering
Mysuru, Karnataka, India

Vinutha A S
Department of Electronics and Communication
Vidyavardhaka College of Engineering
Mysuru, Karnataka, India

Abstract— **The Business market for smart phone applications using Bluetooth Low Energy (BLE) is constantly amplifying nowadays. The Bluetooth Special Interest Groups (SIG) expected that in future they will encounter more than 90 percent of all Bluetooth enabled devices which supports BLE systems. Bluetooth Low Energy is becoming progressively popular in smart phone applications due to the circumstance of using it for the proximity data. This project gauges the Bluetooth Low Energy in the context of using mobile applications to unlock a door automatically when an intruder approaches the door. Computations were performed to determine the reliability, signal strength, connection latency and energy consumption for the same. The hardware designed for this door lock system is the union of components like a Bluetooth module to act as a command agent, an android mobile phone which functions as the task master, an Arduino microcontroller to process the data or to operate as a control center and a solenoid as a output for the door lock system. All of the tests stipulated above will go according to the initial design of this research.This paper provides a insight on various available security system.**

Keywords—**Smart Lock, Android application, BLE, Wi-Fi, UUID, ESP32.**

I. INTRODUCTION

Technology is a never-ending aspect which gets updated frequently. Lately, there has been a lot of home breaching, which is a problem of the hour that needs to be solved. As there are new devices for personal use, such as smart home appliances, wearable devices and smart cars the users feel the urge to make their home safe and secure. The current popular security systems are biometric-based. It involves registering and maintaining biometric details that are affected by physical factors, thus making them less reliable. These systems are costly, and not everyone can afford them. Let us consider a scenario where the user has to use a fingerprint lock on a rainy day. As the rain can hinder the efficiency of the scanner, which makes the device less reliable.

Every currently available lock system has a unique key which needs to be remembered by the currently available security systems do not provide the option of having multiple keys, thus making them less accessible. A user can have 3–5 keys to unlock certain security systems, and it is difficult to add new keys to the system, which makes the system less smart. If any currently used device can be made into a key, it can improve the user experience.

BLE is a short-range, wireless personal area technology designed and marketed by Bluetooth. BLE can detect signals up to a range of less than 100m, which makes it ideal for short-range communication. It has data transmission rates of up to 250 K bits/s, 500 K bits/s, 1 Mbps and 2 Mbps. The technology was marketed as Smart Bluetooth, and integration into version 4.0 of the Core Specification was completed in early 2010. The first smartphone element with the 4.0 specification was the iPhone 4S, released in October 2011. Several other manufacturers released Bluetooth Low Energy Ready devices in 2012.Other communication technologies include Near-field communication (NFC), Wi-Fi, GSM, and Bluetooth. BLE technology is similar to this technology but has its advantages for the application of door locks. GSM and Bluetooth utilize less power compared to Wi-Fi, which makes them more reliable for a security system. The NFC technology range is less compared to BLE. If one uses NFC technology to unlock the door, the user needs to completely close to the door, which is inconvenient. Above all, NFC technology has a lower data transmission rate compared to BLE, which in turn makes it slower to work with Wi-Fi hence we need a router, but that is not the case with the BLE technology. BLE just needs a transmitter and receiver for the operation.

II. PROPOSED ALGORITHM

The BLE locking system consists of components like the receiver (ESP32), keypad, relay, solenoid lock, I2C LCD, IR proximity sensor, and a buzzer. A BLE device or beacon acts as a transmitter and is also a key to unlock the door. The main principle is that the transmitter sends a signal (i.e., UUID address) and the receiver receives it and checks if it matches the registered address. If so, then it unlocks the door. The ESP32 micro-controller acts as a receiver which reads all the available UUID addresses nearby. The relay acts as a switch to drive the solenoid lock. The IR proximity sensor monitors whether the door is closed or opened. The mobile application is used as a backup mode of unlocking the door in case the user forgets to bring the BLE device. The buzzer is used as an indicator in case the user enters the wrong password while using the keypad. The LCD is the main user interface component that shows the user the current status of the system. Figure 1 shows the operating flow chart of BLE Enabled Door Locking System.

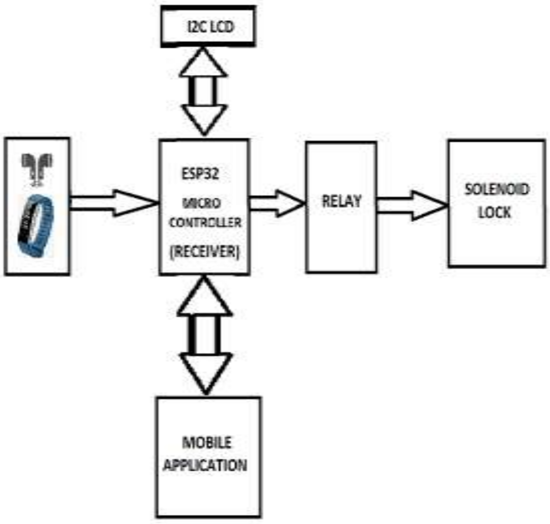

Figure 1: General operating flow chart of BLE Enabled Door Locking System

III. LITERATURE REVIEW

Grant Ho, Derek et.al [1] altogether have discussed the advantages of smart locks over traditional locks for home security and the operation and architectures used in those smart locks. The three essential parts of the smart lock system are the web server, the mobile application which controls the lock, and the deadbolt affixed on the door. The smart locks may use either of the two architectures. In the first architecture, the smart locks themselves are not directly connected to the Internet. Instead, these locks use users' mobile phones as a "gateway" to the Internet. The second architecture has a direct Internet connection between the smart lock and the server. Depending on the application either of the architectures are used. The digital keys have made the smart locks automated and more user-friendly. The major drawback is that there are many classes of attacks or threats which the lock has to fight against, even though the security is high.

Jia Liu et.al [2] discussed how the Bluetooth Low Energy (BLE) can be a primary protocol in building low power computing devices and consumer products in the upcoming generations and also analyzed the neighbor discovering energy of BLE. It has excellent energy performance because of which it is popularly used in wireless consumer products. It has been a low-power solution for many controlling and monitoring applications. In order to analyze the neighbor discovering energy of BLE, they have considered two modes of working. The first one is the scanning mode and the second one is the advertiser mode. In scanning mode, it scans for the devices and in advertising mode, it transmits the advertising information via channels. There are two types of Advertising Event for BLE they are Directed Advertising Event and Undirected

Advertising Event. The directed is used to establish connections with the prior known devices and the undirected is used for unknown device detection, it is also the exact type required for the device discovery. To determine the neighbor detecting ability of BLE, a model was built and was also utilized to determine the latency of the device discovery and derived the performance under various conditions.

Diamond Celestine Aluri [3] proposed a smart door locking system which uses a cryptographic key to open the door via Bluetooth Low Energy (BLE) enabled devices. These smart locks have to be associated with smartphone applications to authenticate. The process uses a wireless protocol and a cryptographic key to alert user’s Bluetooth device when an unauthorized person tries to unlock the door. At first, the user transmits signals to door locking system through any BLE device to lock or unlock the door. Devices will be paired in the range of BLE and the user can then control the lock. Besides an easy installation process, it is also easier to access and activate the lock as it does not restrict the control system only to smartphone applications but also to other available BLE devices that can access the locks simultaneously. Along with smartphone application access to lock or unlock the door, now there are locks which provide a keypad to create a pin or password combination. The major drawback of this smart locking system is when the owner tries to access the lock through smartphone with a low battery condition and also during a blackout of the control unit or any faulty condition.

Siddhi Kavde et.al [4] all together proposed a digital door lock system using Bluetooth technology. They have used an actuator as a door lock, an AVR atmega-32 microcontroller for authentication and a Bluetooth application which provides live scanning with a web camera. It is constructed using components like a client application, a server and an Android user. The door lock system uses a web camera to detect the person in front of the door. At first, by using a Bluetooth application and then via server the owner receives a message notification about the person found in front of the door. The user has two options i.e., he can either grant the permission to that unknown person to enter the home if he is authorized or else, he may deny the access for him through the android application. For a person who wants to access the door regularly, a database is created to permanently store his or her identity details for ease of access. In this project they have used a hashing algorithm which uses MySQL database to generate a database for the unknown person identified in front of the door by the Bluetooth application web camera. In this system the owner can access digital door locks by gaining hassle-free access from anywhere.

N.H, Ismail et.al [5] discussed a current initiative that meets the at-home needs of those with physical limitations where Bluetooth is used to establish a connection between the user's smartphone and the controller card. The home door can be locked and opened using the prototype's manual or micro-controller controls. Where a relay board is used to complete the circuit and a Bluetooth connection is made to the Arduino controller board, remote access from a tablet or smartphone is also made possible. The functionality and development of the Android-based application to aid disabled individuals in taking control of their living space are the subjects of this work. This study's goal is to provide a method for helping people with disabilities to access a magnetic door wirelessly using an Android smartphone via Bluetooth technology built into the mobile device, scope and security issues were taken into account. By pushing a button on a smartphone, the technology might function as a pin to lock or unlock the door from a close distance.

Jayant Dabhade et.al [6] proposed a smart home control systems which are essential for daily life in the modern world. Given how quickly technology is developing, it is now necessary to make easy and technical advancements in home security for client access. This method mostly deals with keyless door locks that are operated by smartphones and utilize SMS, email, images, anti-theft, and the generation of B-IDs for visitors. As a result, only the guest user's password will be able to open the door for a set period of time. Additionally, the device has motion detectors that will aid in identifying the user. The camera will take pictures of the user at the gate if an unauthorized person tries to open the door. These photos will be delivered to the owner. Additionally, this strategy is one of the most used digital products in the digital door lock devices because of their affordability and user-friendliness. In actuality, it is displacing a variety of traditional locks. This article attempts to provide a revolutionary wireless access and monitoring control system made up of various phases and User recognition. Home automation is made safer and more costeffectively efficient using a low-cost authentication solution based on Bluetooth technology. However, the cost of implementation and the availability of supplies for the necessary hardware needs to be considered.

Wafa Elmannai et.al [7] proposed a system with conventional door locks with a deadbolt that can be operated by available electronic devices like cell phones through Bluetooth or WI-FI which has grown in recent years. Although there are many different types of smart locking systems available in the market, the majority of those are expensive and are prone to security threats like network attacks and malware. These current Smart locks also have a limited feature set. They suggested a secure, trustworthy and an affordable platform that supports smart locks based on point-to-point communication. This application will offer improved secure communication. A secure virtual element was also created using host card emulation (HCE). The created system is tested by using three key parts they are by using an emulation circuit, an NFC module, a Beagle bone Blue and a lock. With the use of peer-to-peer connectivity, they were able to build a system that is safe, reasonably priced and dependable. The suggested method is based on SE Hybrid and HCE which is a novel strategy that demonstrated improved security and safety. In order to continue this work in the future, they would prefer to develop unique hardware drivers rather than using generic ones for both server connection devices and NFC capabilities.

Dr. Aziz Makandar et.al [8] discussed about how security is becoming increasingly important in all fields as technology develops and grows every day. We must protect our private spaces because everyone wants a location where no one may enter without their consent where they keep our priceless accessories, papers, data, and jewelry in their rooms, offices, lockers, etc., and for this, a "Password Based Door Lock System utilizing Arduino" has been created in the proposed work. This gadget is a password- or PIN-protected digital door lock. It disables door opening unless the user enters the proper password or PIN number. Due to the availability of numerous additional security technologies, including fingerprint, retinal scanner, RFID card, pattern, etc. This system is quite affordable, though the result of using reasonably priced components is cost-effective. Additionally, the library makes it very easy to create code, and anyone can utilize this model for security purposes. An Arduino-based door lock system can be used to fix the issue with the current door lock system’s irreplaceable components because it is simple to install and take apart. A programmable module will help us deliver better security and save time in the password lock system using Arduino.

Andrea Lacava et.al [9] proposed measures to detect threats against BLE such as jamming, Btlejack attack and man in the middle attack (MitM). The current BLE devices vary from version 4.0 to 5.2, each version has different security modes and features. The developed BLE architecture follows one of the following secure modes - No security, Authenticated and Encrypted. Depending on the Malicious attack, the BLE devices can be made secure using different BLE secure modes. The system also proposes counter measures against these attacks.

Muhammad Sabirin Hadis et.al [10] designed a method for utilizing IoT Technology with Bluetooth as a mode of communication which helps people with disability to access doors using their phones and websites. The system uses a Smart lock Bluetooth architecture which is more secure and user-friendly compared to Wi-Fi. The developed design uses Bluetooth as the main mode of communication between the control system and the smartphone. The data from the control system is communicated using a Wi-Fi module to the server, which is accessed by the user. The design uses a physical cable to connect with a door lock. The special feature of the system is that the users can access the system if the device is lost. The design also uses multiple Bluetooth security authentication which makes it more secure.

Andersson Tim [11] proposed a system that may be used for proximity data as Bluetooth Low Energy is growing popularity in mobile applications. By estimating the Bluetooth signal's strength one can determine a user's proximity to a specific area and take appropriate action. This document assesses BLE in the context of smartphone use for automatically unlocking a door when a user approaches the door, which is one of the most fascinating proximity applications. Measurements were taken to ascertain the signal's strength, reliability, energy use and latency of connections. Despite the wide range in signal strength the results demonstrate that BLE is an appropriate technology for proximity-based door locks. A BLE evaluation has been conducted in the context of automatic door locks and an iOS software has been developed to unlock a door based on user proximity. This has provided a wealth of information about Bluetooth compatibility. Automatic door locks use Low Energy and the iOS platform has both limitations and opportunities for creating BLE applications.

Karthik A Patil et.al [12] discussed about whether in family groups or at work the general public has long serious concerns about the concept of security. To overcome these problems various proven approaches are available. It is suggested that this business develop a smart lock framework utilizing the IOT. Although traditional key locks have been used since the dawn of time, there is a considerable risk of key loss or theft into the wrong hands. In order to increase the security of their homes or places of business, many people now prefer biometric locks over standard key locks. In Modern biometric locks which employ a biometric sensor rather than a key to close or unlock the door in contrast to conventional locks which still use a key. Our endeavor is an Arduino Nano-based device. Benefits of fingerprint locks are enormous Comparatively speaking to keyless keypad locks, card reader door locks, combination door locks and traditional keyed door locks. Fingerprint door locks provide greater security, comfort, and quickness. The biometric technology that is most developed and tested is fingerprint reader scanning. Recent biometric research have demonstrated that the fingerprint is more accurate and reliable than the manual technique. The likelihood of replicating biometric data using fingerprint technology is extremely low—only one in a billion. A positive way of user identification using something that cannot be misplaced, copied or stolen is guaranteed by biometric security. This system's versatility and ease of installation along with its low cost make it incredibly valuable. It's got a lot of potential. Users will be able to bypass their standard password and just utilize their mobile device to access the required area. Future development of the system will add more extensions and make it as portable as possible.

IV. CONCLUSION

Security is an important aspect of the day-to-day life. It is a monotonous process to reach the lock every time if there is a need to lock or unlock the door. The lock's main purpose is to provide security to the home. An improved version of a traditional lock is a smart lock. In this work, a comprehensive review of various currently available smart locks in the market has been discussed. After this literature survey, we inferred that there are many smart lock systems available which provide certain features like application interface, biometric accessibility, smart user interface etc. Each security system in the referred paper has a special feature that make the system unique and efficient. The suitable features of these lock can be adapted to our proposed door lock system.

V. REFERENCE

[1] Ho, Grant et al. (2016). "Smart Locks: Lessons for Securing Commodity Internet of Things Devices", Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. DOI: 10.1145/2897845.2897886.

[2] J. Liu, C. Chen, Y. Ma and Y. Xu (2013). "Energy Analysis of Device Discovery for Bluetooth Low Energy", IEEE 78th Vehicular Technology Conference (VTC Fall). DOI: 10.1109/VTCFall.2013.6692181.

[3] Aluri, Diamond Celestine. (2020). "Smart Lock Systems: An Overview",International Journal of Computer Applications. DOI: 10.5120/ijca2020919882.

[4] Kavde, Siddhi & Kavde, Riddhi & Bodare, Sonali & Bhagat,Gauri. (2017)."Smart digital door lock system using Bluetooth technology".International Conference On Information, Communication & Embedded Systems (ICICES).DOI: 978-1-5090-6135-8/17/.

[5] N. H. Ismail, Z. Tukiran, N. N. Shamsuddin and E. I. S. Saadon (2014). "Android-based home door locks application via Bluetooth for disabled people" IEEE International Conference on Control System, Computing and Engineering (ICCSCE). DOI: 10.1109/ICCSCE.2014.7072720.

[6] Jayant Dabhade, Amirush Javare, Tushar Gayal, Ankur Shelar, Ankita Gupta (2017). "Smart Door Lock System: Improving Home Security using Bluetooth Technology", International Journal of Computer Applications. DOI:10.5120/ijca2017913058.

[7] J W. Elmannai, I. Paige, R. Rexha and M. Rivera (2020)."A Highly Secure Platform that Supports Smart Locks", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE).DOI:10.1109/CCECE47787.2020.9255801.

[8] Aziz Makandar, Rekha Biradar, Shobha Talawar (2021). "Digital door lock security system using Arduino UNO", International Research Journal of Modernization in Engineering Technology and Science.Volume:03,e-ISSN:2582-5208.

[9] Andrea Lacava, Valerio Zottola, Alessio Bonaldo, Francesca Cuomo, Stefano Basagni (2021). "Securing Bluetooth Low Energy networking: An overview of security procedures and threats", Sapienza University of Rome, Italy.Volume:211, ISSN 1389-1286.

[10] M. S. Hadis, E. Palantei, A. A. Ilham and A. Hendra (2018)."Design of smart lock system for doors with special features using Bluetooth technology" International Conference on Information and Communications Technology (ICOIACT).DOI: 10.1109/ICOIACT.2018.8350.

[11] Andersson Tim (2014). "Bluetooth Low Energy and Smartphones for Proximity-Based Automatic Door Locks", Linköpings University of Sweden. Corpus ID: 17308618.

[12] Karthik A Patil, Niteen Vittalkar, Pavan Hiremath, Manoj A Murthy (2020). "Smart Door Locking System using IoT", International Research Journal of Engineering and Technology.Volume:07, e-ISSN: 2395-00