Komputika: Jurnal Sistem Komputer
Volume 13, Nomor 1, April 2024, hlm. 73 - 82
Terakreditasi Peringkat 3, SK No. 148/M/KPT/2020
DOI: **10.34010/komputika.v13i1. 11227**

ISSN: 2252-9039 (print)
ISSN: 2655-3198 (online)

Design and Implementation of Bluetooth Low Energy Based Access Control System

Arif Sasongko[1*], Sidartha Prastya[2], Elkhan Julian Brillianshah[3], Muhamad Taruna[4], Abdul Hakim[5]

[1,2,3,4)] Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung, Indonesia 40132

[5)] Infineon Technologies
Jakarta, Indonesia
email: [1]asasongko@itb.ac.id, [2]sidarthatjoa@gmail.com, [3]elkhanj.b@gmail.com, [4]muhamad.taruna@outlook.co.id, [5]Abdul.Hakim@infineon.com

(Naskah masuk: *16 Oktober 2023*; diterima untuk diterbitkan: *9 Januari 2024*)

ABSTRAK *– This paper proposed the design of a Bluetooth Low Energy (BLE) based access control system intended to make access control more practical to implement on areas with high personnel turnover rate by making access rules easy to set and making access keys relatively safe to distribute compared to existing key-based access control systems. The use of BLE technology allows the system to estimate key position within the system by utilizing the curve fitting method for distance estimation and the trilateral method for positioning. The proposed system consists of a server, an admin panel, electronic locks, access keys in the form of a wearable, and access keys in the form of an Android application. The system is designed and proved to have characteristics: adequate accuracy, failsafe mechanism, responsive, adequate accessibility, accountable, enough capacity and resilience. The proposed Bluetooth Low Energy (BLE) access control system with centralized administration for secure key distribution. The system consists of four subsystems: locks, keys, server, and admin panel. Admins manage access rules through the panel, while non-admin users use smartphone keys for electronic locks. The system is effective in high turnover environments, ensuring access control and flexibility. It also offers an indoor positioning feature based on RSSI log analysis.*

Keywords *– access control; BLE; control system; positioning; distance estimation*

1. INTRODUCTION

Implementing access control measures in indoor workplaces with high personnel turnover rates, such as hospital patient rooms, poses a particularly hard challenge. The absence of effective access control significantly heightens the risk of theft, a prevalent issue that can result in substantial financial losses. According to an article, a staggering 95% of businesses in the United States have reported theft-related losses amounting to $50 million annually [1]. An extreme illustration of workplace theft due in part to inadequate access control can be observed in the case of the baby abduction at Hasan Sadikin Hospital (RSHS) in Bandung [2].

Nowadays, the issue of theft in the workplace is commonly handled by implementing access control in the form of access control systems (key card systems, biometric locks, password-based locks, etc.) or the assignment of security personnels [3]. Although these solutions are effective in many cases, they often make physical access control difficult or impractical to implement on areas with high personnel turnover rate. The use of key-based access control system implemented using regular keys, access cards, or password-based locks is impractical to implement on such areas due to need of distributing and collecting access keys from a constantly changing pool of personnels. Furthermore, sharing access keys poses the risk of personnels misplacing their keys, losing their access cards, and accidentally sharing password. Those 3 problems can lead to security breaches and are rather common even in cases where the system is only used by the internal staff [4]. On the other hand, biometric locks are difficult to implement on such areas due to the time it takes to register the personnel's biometrics and for the system administrator to register access rules applicable to the personnel. Security personnels can be assigned to enforce access control on such areas, but that solution is prone to human error and requires constant personnel training and funding to remain effective. Those issues are confirmed by an interview with a RSHS staff who stated that challenges in implementing access control in a hospital's patient room hall stems from the security

risks that comes from implementing key-lending procedures and the unappealing cost of hiring more security personnels. From the previous discussion and implementation in hospital, it can be concluded that:

1. Key-based access control systems (keys, password, access card) are impractical to implement due to the need of distributing and collecting access keys from a constantly changing personnel pool
2. Key-based access control systems (keys, password, access card) poses an additional risk of security breach caused by personnels losing their keys or accidentally sharing their keys
3. Biometric locks are difficult to implement on such areas due to the time needed for registration
4. Enforcing access control with security personnels are expensive and prone to human error

Quite similar problem was tried to be solved in other work such as [5][6]. In A, the researcher proposed to use multiple RFIDs to locate and to manage access for medical staff. This method is effective and relatively low cost especially for the medical staff. Unfortunately, this method is not practical for the patient and their companies/families due to distribution of the RFID tags, utilization for special clothes, and enforcement. The work on [6] combined the concepts of MAC and RBAC, actually this current work is an implementation of that concept.

With that in mind, an access control system that can be centrally configured and allows its keys to be easily and safely distributed to people of interest can make access control more practical to implement on areas with high personnel turnover rate. This paper contributes to solve the access control problem by proposing a BLE-based architecture of a flexible system using both specific key and smartphone. The proposed system allows the system's electronic keys to be distributed safely and easily accessed by users via an Android based mobile application or wearable device. The system can also be controlled centrally via an admin panel which allows the system administrator to easily set applicable access rules. Both of those features make access control more practical to implement by enabling the safe distribution of access keys and by centralizing the control of the system. Furthermore, the use of BLE technology allows further development of access keys to be implemented on ubiquitous devices owned by users thus reducing the risk of access key loss. The use of BLE also enables the system to have indoor positioning capabilities which is useful in places such as a hospital where the staff occasionally needs to locate patients who are not present in their rooms.

The proposed system consists of electronics locks, keys in the form of wearables and an Android based mobile application, and an information system to manage applicable access rules. This paper consists of five chapters which contains the summary of the system's design process. The second chapter of this paper discusses the specifications of the system. The discussion is followed by a summary of the system's design and implementation phase in the third chapter. The last two chapters of this paper contains the system's testing results and the conclusion of this project.

2. METHOD AND MATERIALS

Specification

To ensure the system is up to par with existing access control systems, a list of 8 specifications is made based on interview results, published studies, industry standards, and comparisons to existing access control systems. The list of specifications is as follow:

1. 100% accuracy on identifying users
2. A maximum of three steps to activate the system's failsafe mechanism (Failsafe)
3. A maximum response time of 5 seconds (responsiveness)
4. A maximum of three steps to provide access (Facility)
5. Able to store two days' worth of user activity data
6. Capable of identifying 18.900 unique personnels (Capacity)
7. Scored at least 68/100 on the System Usability Scale
8. Rated IP22 for indoor use (Resilience)

The first specification in set to ensure that every personnel can only access areas authorized said personnel. The second and fourth specification is made to ensure that new personnels can learn how to use the system in a single explanation[7]. The third specification is made to match the performance of an existing access control system. The fifth specification is made so that the system follows a recommendation for data backing practice which is encouraged to be followed by users [8]. The sixth specification is set to ensure that the system is capable of handling traffic generated by daily usage in a hospital which was estimated based on an interview with one of our sources. The seventh specification is made to ensure that the system administrator can easily set applicable access rules which can be indicated by achieving a System Usability Scale (SUS) [9] of at least 68/100 [10]. The last specification is made to ensure that the system can operate in and indoor

environment which can be indicated by achieving an Ingress Protection (IP) [11] rating of IP22 [12].

Design

The proposed system consists of 4 subsystems:

1. Key Subsystem
2. Lock Subsystem
3. Admin Panel Subsystem
4. Server Subsystem

A top level view of the system's architecture is illustrated in Figure 1.

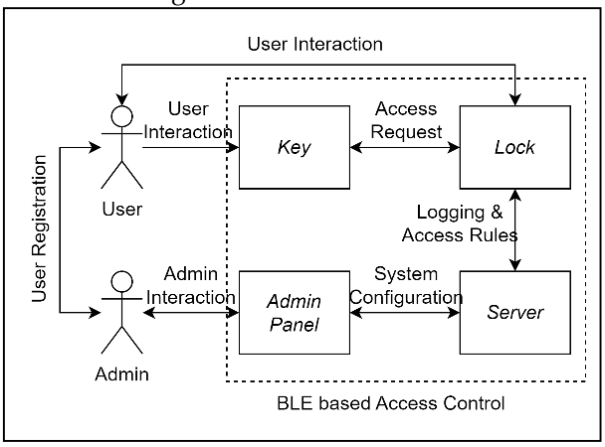

Figure 1. Top Level System Architecture Diagram

There are two main actors in this system which are the administrators (admins) and the users (non-admin users). Users are individuals who utilize the system to request access to a specific room. In contrast, administrators are individuals entrusted with the responsibility of overseeing and regulating users' access permissions within the system. The job of the administrator is to register users and devices into the system and to manage access rules via the admin panel. The admin is also responsible to give non-admin users a key and access to certain locks by the system. The non-admin users may be a staff member of the office, a guest of a patient in a hospital, etc.

The main purpose of the keys subsystem is to serve as a tool used by non-admin users as a digital identification device in controlled areas, as well as an authentication device for granting access. The lock subsystem is an electronic lock that is capable of restricting access to a door according to a list access rules sent by the server. Note that a key can only open a lock if there is an access rule set by an administrator that allows such an operation. Also note that access rules are stored in the lock. This design choice makes it so that the system's locks can still operate if the server is not active.

The function of the server is to communicate with the system's locks in order to implement access control, receive access and signal strength logs from the system's locks, and to realize the features visible on the admin panel subsystem. The sole purpose of the admin panel subsystem is to provide an easy-to-use graphical interface intended to be used by the system's administrator in managing access rules, searching for logs, and managing the system's data (lock, key, and personnel data).

In this design, BLE technology is utilized by the system's keys and locks to communicate with each other. Interactions between the server and the admin panel are done via a Representational Stateless Transfer (REST) Application Programmable Interface (API). Communications between the server and the locks within the system are done via a proprietary application layer protocol carried by User Datagram Protocol (UDP) to reduce memory consumption on both the server's side and on the lock's side. The underlying server and network hardware that enables this scheme of communication is assumed to be already installed on the user's building. The design and implementation of each subsystem are discussed in the following sections.

Key Subsystem

The software implementation of Key device is applied on the NRF51822 microprocessor as the main control unit[13]. The microprocessor is programmed using the Arduino IDE application with the C programming language[14]. The software implementation of Key device consists of several sub-modules, including BLE Communications, Control and Processing, and User Input and Output. On the other hand, the hardware implementation of Key device involves the design, printing, and assembly of components. The hardware implementation of Key device comprises several sub-modules, including Circuit Design, and Case Key. The details are as follows.

1) Software Components

The software part of the key subsystem consists of the BLE Communication module, user interface, control and processing. The BLE Communications module is utilized by the Key device to communicate with another device, Lock, through Bluetooth Low Energy. The Key device functions as a peripheral, while the Lock device serves as the Central. A peripheral device is one that can be scanned by a central device.

The user input and output (user interface) module serves the purpose of physically connecting the user with the key device. This submodule has two primary functions: receiving input from the user and providing notifications to the user.

The control and processing module is a subcomponent responsible for managing the key device system. This submodule is tasked with transforming input into output that aligns with the system's objectives and functions, including

decryption using the Advanced Encryption Standard (AES) method.

2) Hardware Component & Integration

The hardware part consists of a circuit and a key case. The key casing implementation involves designing and printing the cover of the key device. The cover design is limited to a maximum length and width of 40mm. The key casing implementation consists of four main parts: the body casing, cover casing, button mechanism, and microUSB protector. Figure 2 displays the assembled result of the key case printing.

Figure 2. Final result of Key's Case

The circuit design process includes the creation of schematic circuits, the development of PCB layouts, and the fabrication of PCBs. The design and implementation process of circuit design has a constraint regarding its dimensions, which should be 37 mm in length and width to allow for assembly within a key case. Circuit design also covers the power management submodule.

The power management submodule is a component of the key device that controls power usage and battery charging. Its primary function is to supply the appropriate power to meet the key device's needs and recharge the battery when power is available. Moreover, this submodule safeguards the key device against potential damages caused by unstable voltage, excessive current, and overcharging.

The PCB implementation includes PCB printing, PCB testing, and the assembly of all components. The PCB layout is designed based on the schematic circuit design and component dimensions. The component sizes were obtained through measurements taken by the author using a caliper. Figure 3 display the assembled PCB resulting from the printing process, along with its components.

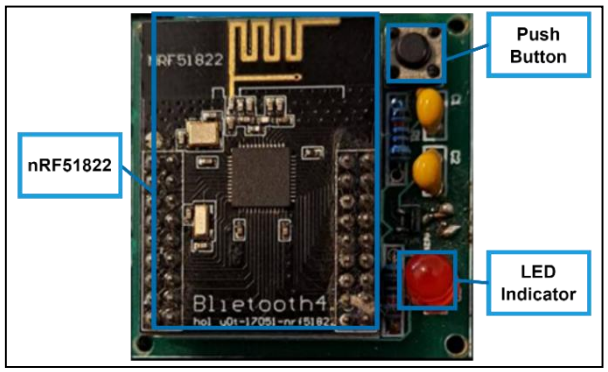

Figure 3. Key device Printed Circuit Board with Components

3) Android Based Application

As claimed in the beginning of this document, it is possible to implement the key subsystem as an Android based mobile application. This implementation has the same behavior as the original design but the button and LED of the key is replaced by user interface buttons and text prompts. The user interface of the application is as shown in the figure below. Figure 4. Android Application Implementation of the Key Subsystem

Lock Subsystem

Lock is a subsystem installed at a door to control user access made using CY8CPROTO-062-4343W microcontroller[15]. Lock subsystem uses magnetic lock as the main mechanism installed on the door. The main reason of using magnetic lock is to prevent door from locking if there is an emergency incident or unexpected behavior of the system. However, this mechanism is used based on hospital circumstances. It still can be changed with another electrical lock mechanism as long as it satisfies the lock power specification which is 5 – 30 VDC input.

There are 6 modules in Lock Subsystem's architecture which the majority of the modules have been done in software development using C program within FreeRTOS environment, thus every task works as a thread[16].

1) BLE Communication

This module control every activity that held via BLE communication. This module controls the interactions between Key subsystem and Lock subsystem, such as BLE scanning, BLE connection/disconnection, and BLE communication. Lock subsystem detect a key's existence using BLE broadcast by filtering the incoming advertised signal. This signal needs to satisfy the format known by the system to be recognized as a valid key device. The format used is discribed in Table 1.

Table 1. Format of BLE Broadcast from Key Device

Format partition	Number of bytes
UUID broadcast	2 bytes
Manufacturer sign	4 bytes
Key ID	4 bytes
Connectable sign	1 byte

The UUID and manufacturer sign are the same in every key device as a valid product identifier. Meanwhile, Key ID is a unique ID that is given to key device. Then, connectable sign is a single byte which value is either 0x30 or 0x31 to indicate if an access request is being requested. After the format validation process, if the key device is indicated request for access, then the connection is established, and the authentication process is held.

2) Network Interface

This module controls every activity that is held via WiFi UDP network. This module controls the interactions between Lock subsystem and Server subsystem, such as device position logging, access logging, time synchronization, and access rule synchronization. The communication is transmitted to Server in a packet with format described in Table 2.

Table 2. Format of Wifi UDP Packet

Format partition	Number of bytes
Op-code	1 byte
Messages	n bytes
Signature	72 bytes

The op-code is used to declare what action is being done or directed. Messages part is the information contained to be processed. The number of bytes of the messages depends on what information is being transferred. Finally, those op-code and messages are concatenated and encrypted to a digital signature using a secret key that has been automatically generated by the Lock when the first configuration was held. This verification process is discussed in Lock subsystem's authenticator and controller module.

3) Local Storage Management

This module controls every activity that is either saved in or loaded from microSD card, such as WiFi credential, Lock's information, Server's information, access rules and local logs. In installation process, administrator have to plug a micro SD card containing only WifiCredential.txt file which contains the WiFi SSID and WiFi password in. The program then will automatically generate ECDSA private and public key, then the WiFi UDP connection is being held to do cryptographic key exchange between Lock and Server. After that, the Server's IP address and public key is being saved in the ServerInfo.txt file. This information is loaded every time the Lock initiates it's program.

4) Mechanism and Peripherals

This module containing all the Finite State Machines (FSM) of the mechanism and peripherals, such as relay (magnetic lock), LED indicators, buzzer, emergency button, and open button. Emergency button has 2 channel which are normally opened channel and normally closed channel. The power voltage to mechanism is connected to normally closed channel, so in case of emergency and the button is pressed, the mechanism is detached. On the other hand, the normally opened channel is connected to emergency terminal at Lock controller. This will send the emergency signal when the button is pressed. This mechanism is also used to open button which only has normally opened channel. The open button is connected to open terminal at Lock controller.

5) Authenticator and Controller

This module control all of the authentication processes either BLE authentication or network verification. BLE communication is secured using AES-128 CBC. This method requires 5 information which are plaintext, ciphertext, AES key, and AES initial vector. Plaintext is a 16 bytes string as which will be encrypted, whilst the ciphertext is a 16 bytes string after the plaintext being encrypted. This encryption is done using 16 bytes AES key and 16 bytes initial vector. Hence, to break through the BLE secure communication, there are $(2^{256} - 1)$ possible keys needed to break through authentication process.

In authentication process, Lock generates a 16-byte encrypted random string and send it to Key device via BLE characteristic. Then, the Key device have to decrypt it and send the decrypted string back to Lock. If the decrypted string is the same as the original string, then the authentication process is valid and Lock will open the entry access.

On the other hand, network communication is secured using ECDSA (Elliptic Curve Digital Signature Algorithm). The signature is created using the generated private key to a packet being transferred. In signature making process, the original message is hashed using SHA256 algorithm resulting 32-byte digest. Then, the digest is signed using the private key resulting about 68-to-72-byte sized signature. The signature is concatenated to the message becoming a packet that is ready to be transferred to Server.

In reverse, the packet received from Server is extracted to 3 segments: op-code, message, and signature. The signature is verified using Server's public key and compared with the op-code and message segment. After the verification was successful, Lock will process the request action based

on op-code identifier and messages.

6) Power Management

This module assigned as voltage divider between mechanism and microcontroller. In this case, the controller using 5V as the input voltage whereas the magnetic lock using 12 V input. This module also connected to emergency button in case of emergency to cut off the electricity, so the magnetic lock is automatically opened.

The power divider is managed using LM2596. This module is adaptively lower the higher DC voltage and set it to 5V output. In other words, by this design, another type of locking mechanism can be implemented by the same controller as long as its required voltage ranged between 5 to 30V.

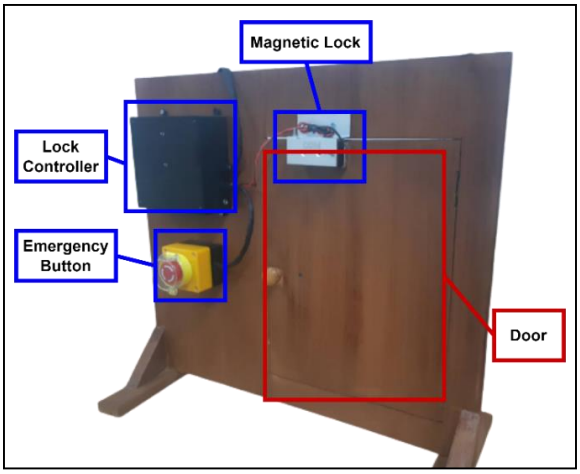

Figure 5 Lock subsystem installed at door miniature prototype (front view)

There are 3 components at the front side of the door (on the other side of the door) which are Lock controller, emergency button, and magnetic lock. The position of each component is flexible, but ideally the Lock controller needs to be installed as high as possible to avoid BLE signal blocked by any object.

Admin Panel Subsystem

In order to serve its purpose, the Admin Panel must provide these features:

1. Searching, registering, editing, and deleting personnel data within the system.
2. Searching, registering, editing, and deleting key data within the system.
3. Searching, editing, and status checking lock data within the system.
4. Searching, registering, editing, and deleting access rules within the system.
5. Searching, registering, editing, and deleting personnel data within the system.
6. Searching and streaming of access log data
7. Visualize the location of locks installed within the system.

This subsystem is implemented by a JavaScript based client-side web application. Each feature listed above are manifested by pages and forms in the web application. To abide by user interface best practices and thus provide good user experience, the system's user interface follows the Material Design Guidelines of creating user interfaces. The admin panel is distributed as static files that will be hosted by the server subsystem in production. A few pages of the admin panel's user interface can be seen in the appendix section of this paper.

Figure 6 Physical positions of locks and access keys (red circles indicates locks, black circles indicates access keys)

Figure 7 Admin panel's indoor positioning page (red circles indicates locks position, black circles indicates access key position)

As an additional feature, the admin panel is capable of estimating detected keys location based on the received BLE signal strength as shown in the above figures. The physical positions of locks and access keys involved in the positioning feature can be seen in Figure 6 whilst the position estimation result can be seen on the map of the room in Figure 7. In this implementation, indoor positioning is achieved by estimating the distances between access keys and locks using a model created with the curve fitting method [17]. The aforementioned estimations can then be used to estimate an access key's position within the vicinity using the trilateral method [18].
The aforementioned model is created by collecting RSSI data measured at a distance of 0,5m; 1m; 2m; 3m; 4m; 5m; and 6m. Outliers are then removed and the data is then fitted to a curve with the equation as shown below.

$$d = 10^{\frac{C-RSSI}{10n}} \quad (1)$$

The variables:
D = estimated distance
C = the RSSI value measured at 1 meter in dBm,
RSSI = the measured RSSI (at dBm)
N = scaling factor

The formula fundamentally is attenuation formula by distance (negative exponential). After testing, the distance estimation error is found to be in the in range of 1,729m – 1,836m with a 95% confidence interval and has a maximum range of 6 meters. The positioning error of this system is measured to be around 2 meters under ideal conditions (no movement and no signal barriers between locks and keys). The positioning's relatively low accuracy makes this feature unsuitable for indoor positioning that requires a high level of accuracy. Nevertheless, the accuracy achieved is adequate to detect the location of a personnel on sections of a building.

Server Subsystem

This subsystem is implemented with the Go Programming Language, a programming language with built-in concurrent features which is ideal for developing a network based software such as this [19]. The system's data is stored on a locally hosted PostgreSQL database. This software is distributed as executables files that is available for computers with a Linux operating system and utilizing x86_64, i386, or ARM Central Processing Unit (CPU) architecture. Brief explanations related to the implementation of this subsystem are discussed in the next three parts which corresponds to the three submodules that makes up this subsystem.

1) Admin Panel Service

This submodule is the part of the server that interacts with the admin panel. The admin panel service's primary concern is to realize the features displayed in the admin panel subsystem. Therefore, all of the endpoints provided by this submodule are designed according to the admin panel's feature. The endpoints provided by this submodule can be summarized as shown in the points below:

1. Authentication and authorization endpoint
2. Personnel data management endpoints
3. Lock data management endpoints
4. Key data management endpoints
5. Access rule management endpoints
6. Access log data search endpoint
7. Posisition log data stream endpoint

This API is secured using JSON Web Token (JWT) [20]. authorization scheme to meet REST API constraints [21]. The full API specification and testing results can be found on the Postman documentation page which can be accessed via a hyperlink in this paper's appendix

2) Logging Service

Logging service is a submodule that is created to handle incoming log data from locks within the system and to request log data to locks within the system. To ensure that the incoming log data are from actual locks, an Elliptic Curve Digital Signature (ECDSA) [22] is included in every UDP packet is sent from a lock. ECDSA is chosen over RSA as because it offers the same level of security for a shorter signature length [23]. As hinted in the previous section, there are 3 kinds of log data coming from the lock subsystem which are the position log (contains detected BLE signal strength from the key subsystem), access log (contains the identity and time of access), and healthcheck log (contains information related to the status of a lock). Besides logging, this subsystem also handles automatic lock registration in the form of a public key exchange request coming from a newly installed lock. With that, we implemented 4 use case handlers within this submodule which are:

- Key Exchange Handler
- Log Access Event Handler
- Log RSSI Event Handler
- Log Healthcheck Event

The submodule is found to be capable of handling key exchanges and logs properly. The performance of the submodule is found to worsen as the frequency of logs increases which results in higher latency on the indoor positioning feature. The issue can be resolved by configuring more worker threads to handle incoming packets. Another possible solution to address this issue is to use a more efficient message verification scheme in place of the ECDSA to reduce to the time needed to verify every incoming packet.

3) Access Rule Service

Access rule service is a submodule that is created to tell locks to store new access rules, edit existing access rules, and to delete existing access rules. In order to ensure that the locks will not be affected by packets that are not coming from the server, an ECDSA signature is included in every UDP packet sent from the server to the locks. Besides sending packets, this submodule also provides a handler for incoming access rule synchronization requests sent by a registered lock. With that, 4 use case handlers are implemented in this submodule, which are:

- Add Access Rule Handler
- Edit Access Rule Handler
- Delete Access Rule Handler
- Sync (Synchronize) Access Rule Handler

3. TESTING AND ANALYSIS

Accuracy

This test was conducted using access rules use case presented in Table 3.

Table 3 List of access rules for testing

Lock	Access Rules
Lock A	Key A, Key B
Lock B	Key A

The results shown in Table 4 reflect the accuracy test's findings encompassing all potential test cases.

Table 4. Authentication accuracy result

No.	Testcase	Expected Result	Passed?
1.	Key A to Lock A	Door opened	✓
2.	Key A to Lock B	Door opened	✓
3.	Key B to Lock A	Door opened	✓
4.	Key B to Lock B	Access denied	✓

The system's authentication accuracy attained a perfect score of 100% as observed from the testing outcomes documented in Table 4.

Failsafe Standard Procedure

Table 5. Failsafe Standard Operational Procedure

Step	Step Details
1	The user approaches the door of the room to be accessed.
2	The user presses the emergency button
3	The user pushes the door and enters the room.

The result documented in Table 5 represents the calculation output of the number of steps in the failsafe SOP for granting access, along with the detailed steps involved. Based on the above result, the required number of steps is three. Since the number of steps is not more than three, the specification of the Standard Operational Procedure Failsafe has been achieved.

Responsiveness

Based on the experiment results, the average time taken to grant access from the moment a user requests it is 2.471 seconds, considering a total of ten experiments. The standard deviation of these results is 0.52214 seconds. The longest delay is 2.98 second while the fastest is 1.4 s. From the results and analysis of the system responsiveness testing, all experimental results have response times of less than five seconds. This indicates that the system responsiveness specification has been achieved.

Accesability

Table 6. Accessibility test from outside

Step	Step Details
1	The user approaches the door of the room to be accessed.
2	The user presses the button on the key device
3	The user pushes the door and enters the room.

The results documented in Table 6 present the calculation and detailed steps required to open access from outside the room. The number of steps required is three. Since the number of steps required is not more than three, the accessibility specification from outside the room has been fulfilled.

Table 7. Accessibility test from inside

Step	Step Details
1	The user approaches the door of the room to be accessed.
2	The user presses the door open button located near the door
3	The user pushes the door and enters the room.

The results documented in Table 7 present the calculation and detailed steps required to open access from inside the room. The number of steps required is three. Since the number of steps required is not more than three, the accessibility specification from inside the room has been fulfilled. From the two results above, the accessibility specification has been achieved.

User Activity Data Logging

Storage capacity for user activity data is tested by generating dummy data and saving said data to the system. Assuming that there will be 1 position log reported every second and 1 access log reported every minute, the number of logs related to user activity in a 48 hour times period is equal to 172.800 rows of position log data and 2.880 rows of access log data. By generating and executing a Structured Query Language (SQL) query file according to those numbers, the achievement of this specification can be determined. The test result of this specification can be seen on the appendix section of this paper. Based on the test result, the system is capable of storing all of the generated data which means that the system fully meets the specifications for user activity data storage.

User Identification Capacity

The number of uniquely identifiable users is tested similarly to the previous specification. A SQL query file containing 18.900 unique users and 378.000

unique access rules (20 for each personel) is generated and executed. The database is then checked to see whether or not all of the data is stored in the database. The test result can be seen on the appendix section of this paper. Based on the test result, the system is capable of storing all of the generated data which means that the system fully meets the specifications for number of recognizable users. Although the specification is met, the testing of this specification does not guarantee that 18.900 unique users can physically use the system at the same time. Further testing is needed to determine the number of BLE keys the system can handle at one time.

Facility

Ease of access is measured using the System Usability Scale (SUS) method [9]. The survey is done by briefing the respondents about how the proposed system works, asking the respondents to use the admin panel, and asking the respondents to fill a standard SUS form.

The survey results shows that 5 out of 10 respondents gave a calculated score of below 68/100 with the lowest score being 60/100 which indicates that the usability of the system is adequate[10]. The specification for ease of use is only met if all of the respondents gave a score greater than 68/100. Based on the test results, it can be concluded that the specification for ease of use is partially met. Further development is required to fully meet this specification.

System Resiliance

1) Keys Subsystem

All openings on the key device have dimensions less than 12.5 mm. In other words, objects larger than 12.5 mm cannot reach the critical parts of the key device. This means that forced access to the critical parts from outside the key devAice would require the use of an object smaller than 12.5 mm, requiring specialized equipment [24]. Based on these results, the key device has an IP2X security rating.

After the IPX2 testing, the tissue placed inside the key device showed some areas that were exposed to water. These areas are near the button hole and the MicroUSB hole. This can occur due to gaps between the holes and the cover components, button mechanism, and MicroUSB shield. These gaps arise from the design and printing process of the key case, which may introduce errors. If these errors are not accounted for in the design and printing process of the key case, the case cannot be assembled as intended, the button cannot be pressed due to frictional resistance, and the MicroUSB shield cannot be installed due to hole dimensions mismatching. As the tissue has wet areas, the key device does not have an IPX2 security rating.

Based on the test results, the key device partially meets the specifications for water and particle resistance. It meets the IP2X rating but does not meet the IPX2 rating. Further improvements in the casing design are required to meet this specification.

2) Lock Subsystem

The step used to test the IP rating for the Lock was the same as those conducted to Key's. Solid object same or below the IP2X standard cannot passed through any hole or gap at the Lock case. Unfortunately, when water poured with the IP2X standard, a little water passed some tiny holes, such as speaker hole, cable hole, and some gaps at the cover. Therefore, it only meets the IP2X rating. However, it will not affect the functionality of Lock in the system.

4. CONCLUSION

This paper proposed the design of a BLE based access control system which enables the administrator to centrally control the system and allows its access keys to be easily and safely distributed. The system comprises of 4 subsystems which are the locks, keys, server, dan admin panel subsystem. The admin panel is used by the system administrator to manage access rules whilst the keys are used by non-admin users to access the system's electronic locks. The server communicates with the admin panel and the locks which enable access rules enforced by the locks to be set remotely by the system administrator. Access keys in the system can be implemented on ubiquitous devices such as smartphones which allows easy and safe distribution of access keys.

The test and evaluation of the system indicate that the system has adequate level of accuracy, responsiveness, accessibility, accountability (logging), capacity, and resilience as designed.

By processing recorded RSSI log, the system is able to provide an additional indoor positioning feature with accuracy suitable for section-based positioning.

This paper has presented also experiment result of positioning prediction using Bluetooth BLE technology.

ACKNOWLEGDEMENT

This project is made possible by Infineon, who provided material and intellectual support during the course of this project from beginning to end.

The writers of this paper are very grateful to Infineon for all their precious help in providing funding, microcontrollers, components, technical support, and insights during in this project.

REFERENCES

[1] A. Zuckernan, "39 Employee Theft Statistics: 2020/2021 Impact & Cost to Business", CompareCamp, May 29, 2020. [Online]. Available: https://comparecamp.com/employee-theft-statistics/.

[2] R. Kuswandi and F. Assifa, "Kronologi Penculikan Bayi di RS Hasan Sadikin Halaman all - Kompas.com," 26 Maret 2014. [Online]. Available: https://regional.kompas.com/read/2014/03/26/1651542/Kronologi.Penculikan.Bayi.di.RS.Hasan.Sadikin?page=all.

[3] J. Moore, "The 2022 State of Physical Access Control Report," Austin, 2022.

[4] L. Bauer, L. F. Cranor, R. W. Reeder, M. K. Reiter and K. Vaniea, "Real life challenges in access-control management," *in Association for Computing Machinery*, Boston, 2009.

[5] G. Luo, X. Duan, Z. Sun, M. Yin, B. Jiao, "Design of a Passive Multi-Tag RFID Hospital Entry/Exit Detection System based on Data Mining Method", *in Proceeding of 2017 International Conference on Sensing, Diagnostics, Prognostics, and Control*, pp 438-443, 2017.

[6] Dae-Kyoo Kim, Hua Ming, and Lunjin Lu , "Reflection on Building Hybrid Access Control by Configuring RBAC and MAC Features", *in Proceeding of 2020 IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pp 522-529, 2020

[7] N. Cowan, "The Magical Mystery Four: How is Working Memory Capacity Limited, and Why?," *HHS Author Manuscripts*, vol. 19, no. 1, pp. 51 - 57, 2010.

[8] K. Herrod, "Defining Frequency for Server Level Backups – Explained - Managed Services Provider | I.T. Outsourcing | Herrod Tech," Herrod Technology, 30 March 2021. [Online]. Available: https://herrodtech.com/defining-frequency-for-server-level-backups-explained/. [Accessed 21 June 2023].

[9] J. Brooke, "SUS - A quick and dirty usability scale," Earley, 1995.

[10] J. Sauro, "Measuring Usability with the System Usability Scale (SUS)," Febuary 3, 2011. [Online]. Available: https://measuringu.com/sus/.

[11] "Ingress Protection Rating". IEC 60529, 2013.

[12] M. Olsen, "Waterproof Ratings: What the IP Numbers Really Mean," *Impact*, October 25, 2016. [Online]. Available: https://www.impactcomms.com/blog/how-waterproof-is-your-microphone/. [Accessed 21 June 2023].

[13] Nordic, "nRF51822 Product Brief Version 2.5," [Online]. Available: https://nsscprodmedia.blob.core.windows.net/prod/software-and-other-downloads/product-briefs/nrf51822-product-brief.pdf. [Accessed 25 June 2023].

[14] S. Mistry, "Arduino-BLEPeripheral," 29 January 2018. [Online]. Available: https://github.com/sandeepmistry/arduino-BLEPeripheral/tree/master. [Accessed 25 June 2023].

[15] Cypress Semiconductor, "CY8CPROTO-062-4343W PSoC 6 Wi-Fi BT Prototyping Kit Guide," *Cypress Semiconductor*, San Jose, 2019.

[16] R. Barry, "Mastering The FreeRTOS Real Time Kernel," 2016. [Online]. Available: https://www.freertos.org/fr-content-src/uploads/2018/07/FreeRTOS_Reference_Manual_V10.0.0.pdf. [Accessed 22 June 2023].

[17] F. Zafari, I. Papapanagiotou, M. Devetsikiotis and T. J. Hacker, "Enhancing the Accuracy of iBeacons for Indoor," 2017.

[18] Y. Bae, "Robust Localization for Robot and IoT Using RSSI," *Energies*, vol. 12, no. 11, 2019.

[19] Google, "Go for Cloud & Network Services," Google, October 4, 2019. [Online]. Available: https://go.dev/solutions/cloud. [Accessed 22 June 2023].

[20] M. Jones and S. N. Bradley J, "IETF," May 2015. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7519. [Accessed 21 Mei 2023].

[21] L. Gupta, "REST Architectural Constraints," REST API Tutorial, April 7, 2022. [Online]. Available: https://restfulapi.net/rest-architectural-constraints/. [Accessed 21 June 2023].

[22] D. Johnson and A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," University of Waterloo, Waterloo, 2000.

[23] G. Huston, "ECDSA vs RSA for DNSSEC," APNIC, November 2021. [Online]. Available: https://blog.apnic.net/2021/11/10/rsa-vs-ecdsa-for-dnssec/. [Accessed 21 June 2023].

[24] "Ingress Protection Rating". *IEC 60529*, 2013.