International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 14, No.1 (Sep-2023)

http://dx.doi.org/10.12785/ijcds/140162

Door Access System Design Using RFID Technology

Noprianto[1], Rokhimatul Wakhidah[1], Rudy Ariyanto[1] and Yan Watequlis Syaifudin[1]

[1] *Department of information Technology, State Polytechnic of Malang, Malang, Indonesia*

Received 09 Nov. 2022, Revised 21 May 2023, Accepted 31 Jul. 2023, Published 01 Sep. 2023

Abstract: In the past, people had to carry around a thick wallet filled with cash when they wanted to make a payment. But now it can be replaced with an electronic wallet (e-wallet) or electronic card (e-money). E-money is one example of the application of RFID in the financial sector. Also often used for identity cards (e-identity). With RFID technology, we can access a room or class that has an RFID reader installed. In most cases, granting access to a room can be done by directly coming to register the RFID or accessing the reader by accessing a specific URL address. This will cause problems if the number is even hundreds. Another problem is the data communication model to the reader device which is carried out by direct access to the URL or communication socket, especially for communication sockets for users who are still new to it will be very difficult. This study proposes data communication to the reader device via remote (remote) on a local network or long distance (internet) and utilizes web communication model services and Protocol Message Queuing Telemetry Transport (MQTT) to wrap socket communication to RFID reader devices. In addition to socket communication, the communication model between applications uses JWT tokens with SHA-256 hashing algorithms that have been set up for access control to add security so as to avoid unknown requests. Auditing techniques are also a concern so that any data changes can be monitored easily. Additional security for writing and reading cards with key A and key B diversification techniques helps avoid taking or changing data on RFID cards. Furthermore, the test results on the AR-725E reader device show that RFID cards can be detected with a maximum distance of 3 cm.

Keywords: RFID, e-money, e-identity, door access, web sevice, MQTT

1. INTRODUCTION

Information technology that is developing very rapidly makes human life easier, for example when making payments if in the previous era you had to carry a thick wallet with cash but in this era, it can be replaced with an electronic wallet (e-wallet) [1], [2], [3], [4], [5] or electronic card (e-wallet). money). An e-money is an example of the application of RFID in the financial category [6], [7], [8], [9], besides being used in the financial sector, smart cards are also often used for identity cards (e-identity). E-identity can be in the form of identification cards, for example identity cards, student cards, employee cards, and other identification cards [10], [11], [12], [13], [14], [15].

An identification card with RFID technology can be used more widely to access a room or class. In the room where the RFID reader has been installed, authorization has been given according to the user category. For example, for a server room that can only be accessed, there is a lecturer who is assigned to manage the infrastructure, while a student's classroom can access it. In general, giving access to a room is done by directly coming to register the RFID or accessing the reader by accessing according to the URL address. Of course, this cannot be done when there are tens or even hundreds of reader devices in the room. In addition, communication to the device must be done manually or conventionally when the registration process or removal access. Another problem is that the data communication model to the reader device is carried out with direct URL access or socket communication, especially socket communication for new users will be very difficult [16], [17], [18].

This study offers a system consisting of several applications to manage space and limit users. The web application will make it easier for the employee-manager to provide access to certain rooms, the functions offered such as employee management, device management, user reports in accessing rooms, and registering/deactivating employees in certain rooms.

A data communication mechanism to the reader device can be done remotely (remote) resulting in anytime and anywhere if it has a good local or interlocal (internet) connection. The low-level communication model on the RFID reader device will be wrapped using web service technology and the Message Queuing Telemetry Transport (MQTT) protocol, the web service will make it easier for further development because it does not depend on a particular platform. Meanwhile, MQTT is a very lightweight protocol for RFID reader communication with other devices.

E-mail address: noprianto@polinema.ac.id,wakhidah@polinema.ac.id,rudy@polinema.ac.id

2. RELATED WORKS

In the previous year, RFID technology has been used to assist in managing parking lots combined with the internet of things technology [19], the purpose of the system is when the user knows whether the parking location is still available or not. The research claims that the parking system business process is carried out automatically with RFID media to enter and exit the parking area. RFID technology is used because transactions can be carried out offline by communicating using an RFID reader, then the security factor is also important to secure the data contained in the RFID so that the data contained is not modified or reproduced [20]. As a result, researchers are trying to use RFID in improving environmental quality and improving production processes.

Abdulla et al. [21] The researchers presented a system for toll collection using RFID technology, with a method they proposed for road users without having to stop their vehicles to open a barrier. The integrated system has 2 main parts, namely the input of electronic data in the form of a tag attached to a reader and then sending RFID data using Arduino Yun. Then the data in the cloud can be seen in real-time by users in the main office.

Abdulkareem et al. [22] in their paper implements a miniature RFID system in a shopping center in the retail industry to replace barcodes that are considered obsolete, using Radio Frequency Identification (RFID) which is claimed to be faster, easier, and safer. RFID is first registered on every item sold, then when a buyer is about to make a transaction, the RFID is read first at a counter. In this study, it is not known the level of efficiency, accuracy, and measurement of the overall level of customer satisfaction when using RFID.

The same research on RFID was also conducted by Adebiyi et al. [23] in the field of transportation to create an electronic transit payment system at Covenant University. The method proposed in this study is to place an RFID reader at the bus stop which the driver then attaches to the RFID reader to make transactions.

In [24] RFID is used as a multimodal apart from fingerprint and face, the purpose of using multimodal in this study is to increase the recognition rate of biometric identification. In practice, multi-biometrics is useful in reducing False Acceptance Ratio (FAR) and False Rejection Ratio (FRR), which are two accuracy standards in biometric systems. Although it is claimed to have increased the accuracy of the system, there are no criteria such as the time needed to record or read and the amount of data that is done.

Then [25] conducted a study to monitor the activities of a student in and out of a boarding school in ensuring their safety and security. A student who will carry out official school activities must attach an RFID to the RFID reader installed at the main entrance of the school complex, then the departure and arrival time data will be sent via Arduino to the database. Simultaneously, the system also sends notifications in the form of WhatsApp messages to all parent numbers. The system is a means of adequately managing student outings because each activity must be registered in advance so that its implementation can be strictly monitored by the school authorities.

This study offers a data communication mechanism to the reader device that can be done remotely (remote) so that at any time and anywhere if it has a good local or interlocal (internet) connection. Low-level communication models such as the socket protocol will be wrapped using web service technology and the Message Queuing Telemetry Transport (MQTT) protocol, the web service will make it easier for further development because it does not depend on a particular platform. Meanwhile, MQTT is a very lightweight protocol for RFID reader communication with other devices.

3. PROPOSED SYSTEM

In this section, the main architecture related to the door access system using RFID with the MQTT protocol will be explained which can be seen in Figure 1. The system that the researcher proposes consists of several parts, starting from the Access reader, Local App, Backend App, and Frontend App.

The flow of the system from the user side, from an employee registering on the system to getting an access card, can be seen in Figure 2. The process begins with an employee (1) registering on the website application (Frontend) and entering all their information (2). Next, the employee proceeds to the RFID card data generation section using the Card Management System application (3) where they obtain an RFID card (4) that can be used to access the room. Finally, the employee can also view room access activities (5) and read RFID card data using a mobile application (6).

A. *Access reader*

The specification of the reader used is AR725E with the ability to read various types of RFID such as ISO 18000-2, ISO 14443, and ISO 7816-4 which run at a frequency of 125kHz and 13.56MHz. Each reader is installed in the room or door, while communication uses a wired network, namely Ethernet. The communication model that can be done to the reader is HTTP communication and socket communication, meaning that a reader is a server socket that can accept requests with certain commands. Aside from being a server socket, the reader is also a client socket when there is an activity log, that is, it will publish or send the activity log data to a socket server that listens on the reader's IP and port.

B. *Local app*

Local App is a collection of applications that directly interact with reader devices, the Local App consists of Log collector and Service subscriber applications. The log collector itself is an application that oversees receiving all

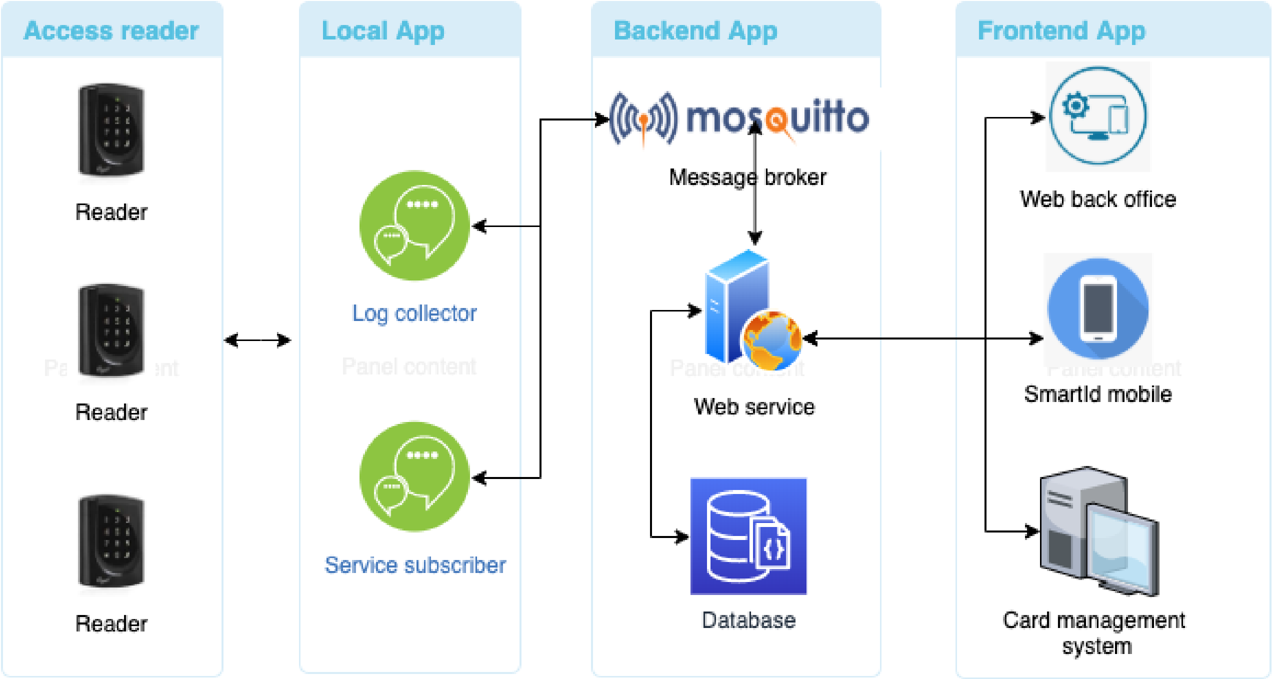


Figure 1. System architecture

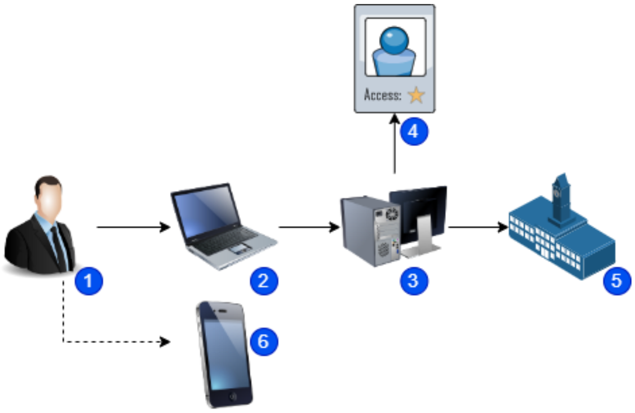


Figure 2. Flow of the system

activity logs or access logs from the reader, the log activity in question is the activity when a user enters or exits by attaching a smart card to the reader or also when the exit button is pressed or touched when going to the reader. out of the room. The protocol used between the log collector and the reader uses a socket so that the log collector is a server socket that is ready to receive activity logs from reader devices at any time. When the log collector gets the activity log data from the reader, it will then publish the data to the Message Broker.

The subscriber application oversees carrying out commands or commands to the reader, the command is obtained by request from the website/portal application. The subscriber application is a consumer of another application or client using the MQTT protocol, while the subscriber application communicates to the reader using a socket. Another important part is the message broker (Mosquitto) is a Server Broker to forward data using the MQTT protocol from the client as a consumer or publisher such as Log Collector, Service Subscriber, and Web service.

The local app has been developed using the Java 8 programming language and the Spring Boot framework version 2.5.6. The libraries used in the development process include Pahomqtt and log4j. Pahomqtt is utilized for communicating with the message broker (MQTT), whereas log4j is employed to debug messages during both the application's development and runtime.

C. Backend app

On the other hand, the Web service module is the most important because this section is responsible for serving all requests from all applications and performing business logic, as well as database storage. The web service also communicates with the message broker when it receives a command or command whose function is to communicate with the door access reader. The data format used to communicate with Web services is to use JavaScript Object Notation (JSON) which is widely used for data communication because by using this format almost all types of programming languages can be supported.

The backend app or web service is developed using the Java 8 programming language with the Spring Boot version 2.5.6 framework and built tools using Maven.

Some of the libraries used include spring-boot-starter-data-mongodb, spring-boot-starter-web, spring-boot-starter-security, java-jwt, and Pahomqtt.

D. Frontend app

Finally, those that fall into the Frontend App category include back-office Web applications, which are web applications that interact with users with the main functions in it being room/device management, activity log monitoring dashboards, employee management, RFID personalization management, and role management. While the Card management system application is a desktop-based application that is used to enter cardholder (employee) data into the RFID, this application will request employee data to the web service application. Back-office web applications and card management systems require a token when communicating with web services, this token is obtained when logging in.

The frontend app is developed using the Java programming language, HTML, and JavaScript with the Spring Boot 2.5.6 framework and Maven as the build tool. The app's libraries include spring-boot-starter-thymeleaf, spring-boot-starter-security, and spring-data-commons. Notably, the spring-boot-starter-thymeleaf library is used as a view for Java-based web applications.

4. System Implementation and Testing

A. Implementation prototype

The hardware used in the proposed system consists of an RFID reader and the RFID itself, the RFID data will be read by the RFID reader which will then be sent to the server.

1) Hardware

A reader device is a device used to detect RFID, when someone enters or accesses a room, they must attach the RFID to a reader. A registered RFID will cause the door to open, whereas if the smart card has not been registered, the door will not open. Figure 3 show the following AR-725E reader. Table I shows the main characteristics of the AR-725E reader.

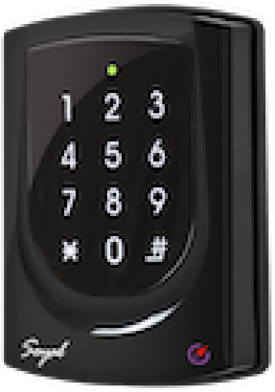


Figure 3. Reader AR-725E

TABLE I. Specification and description of AR-725E reader

Specification	Description
Reading distance	5-15cm
Door relay output (EM lock/electrical lock)	12V/2A, N.O/N.C/COM
Door unlock time interval	Pre-set time 0.1 to 600 sec
Serial port	RS485, 9600, N, 8, 1. TTL UART (4800 115200 bps) X2 (half-duplex)
Power consumption	10-24 VDC. Less than 5W
Host	RS-485 (9600 bps) / TCP/IP
User capacity	16000
Log capacity	32000
Frequency	ISO18000-2, ISO14443 /ISO 7816-4 Mifare Ultralight, Classic, Plus
Dimension (mm)	110 (L) x 79 (W) x 26 (H)
Weight	185 g

Furthermore, RFID is the most important component in the application in this study. Several types are used, including Mifare 1K and Desfire, which use a frequency of 13.56 MHz. Meanwhile, in its application, it is an Indonesian citizen identity card, e-money owned by a bank in Indonesia, and a Mifare 1K card where data is filled (personalization).

Then, for the Mifare 1K card, it is a card that will be filled in with cardholder data using the Card Management System, while for resident cards and e-money, no card data is written because there is no access by the card issuer. Identity cards and e-money only read the UID, which will be registered or paired with the cardholder. Figure 4 and Figure 5 below are prototyping that researcher made to simulate the system so that it could be used before being implemented in a real environment.

Mifare 1K cards are written and read from specific addresses, sectors, and blocks that have been secured using a security key. Key A and key B are used to secure the writing or reading process from unauthorized parties. In addition, the key component is made using the UID Card diversification technique so that each RFID card has a unique key. With this model, employee data can be written on an RFID card without the worry of RFID card data being modified. This also means that reading card data does not require a connection to a server but can be read offline using an RFID card reader.

Figure 4 above is a prototype door that has been equipped with a reader. When attached to the reader, the door will open and will sound a distinctive sound and a green LED on the reader will indicate when the card is registered. On the other hand, when the card is affixed to

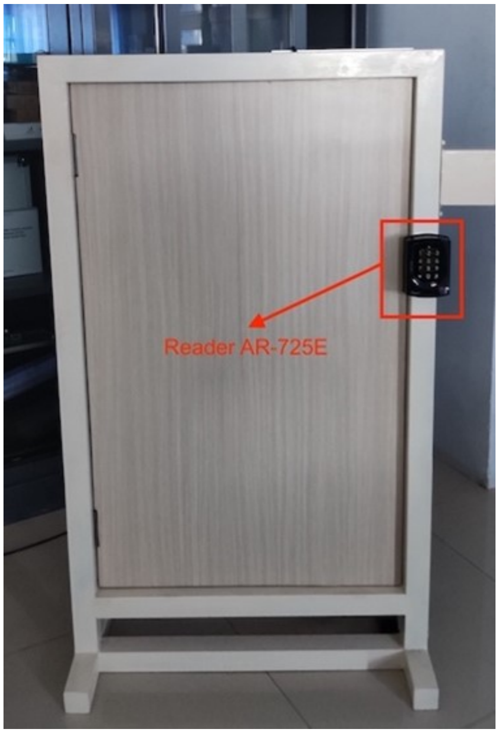


Figure 4. The prototype is seen from the front

the reader, but the door does not open and hides a distinctive sound, and the LED lights up red, which indicates that the card is not registered. Furthermore, in Figure 5, the prototype looks from behind. Below, there is a touch button and an EM-Lock, which is connected to the reader. The touch button is used to open the door from inside the room, and the EM-Lock is a mechanism to lock a door.

2) *Software*

The door access system consists of a Local App, a Backend App, and a Frontend App. The Frontend App runs on the client side using a browser or desktop, while the Backend App runs on the server side. In communicating, Frontend App and Backend App use the REST API, with data formatted using JSON. Then, to perform authentication, a token (JSON Web Token) is needed for exchanging data between Frontend App and Backend App. JSON Web Token is an internet standard mechanism used to transmit data that can be verified by one application to another. To get a token, you must first login by including a username and password, so that each application has a user and password to get a token. Token information can be seen in the following Table II.

To find out token information, it can be decoded by using https://jwt.io/ site. Information token has 3 parts, namely header, payload, and signature. The header contains information on the algorithm used to generate the token, the payload contains the data sent, while the signature is used to verify that the header and payload have not changed. One of the information contained in a payload is expired, expired is the age of the token or validity period. The validity period of the token will expire according to the configuration contained in the web service application, when the token has expired then user can use a refreshtoken or can log back in. In the table above there are roles, roles to determine the limits of a user. Suppose a user can only read data or manipulate data.

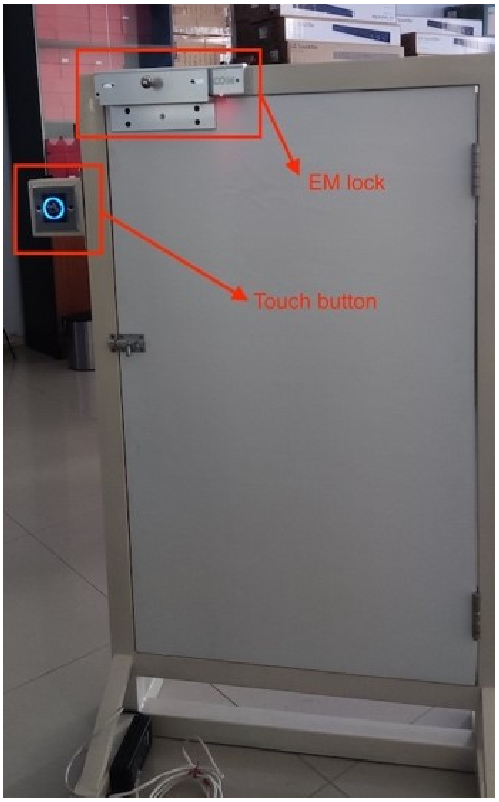


Figure 5. The prototype is seen from the behind

When creating JWT tokens, a hashing algorithm called SHA-256 is used to secure the keys used for communication between applications. Access control is categorized into several rules for each application user to protect the endpoint. There are several endpoints that can be accessed without having to use rules. For example, /api/v1/auth/login is an endpoint that can be accessed by all users without rules, and /api/v1/auth/** has a function to register new users or request a new token if the previous one has expired. /api/v1/user/** is an endpoint that can only be accessed by users with the USER rule. Each application user can have more than one rule depending on the settings and tasks of the application. Auditing is very useful for recording all activities carried out by users, such as when a user changes data. The auditing process has been implemented by recording all activity by application users on data, including who created or modified the data, and when it was created or modified.

TABLE II. Token information

Attribute	Value	Description
Token	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJzZW5vIiwicm9sZXMiOlsiUk9MRV9BRE1JTiIsIlJPTEVfVVNFUiJdLCJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjgwODAvYXBpL3YxL2F1dGgvbG9naW4iLCJleHAiOjE2NTk1OTgzMTR9.XF4C1e82kxdPnoviInBq3QjMxRSEFBVeK7hSoSF4c6o	This token is included when communicating with the web service application
refreshToken	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJzZW5vIiwicm9sZXMiOlsiUk9MRV9BRE1JTiIsIlJPTEVfVVNFUiJdLCJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjgwODAvYXBpL3YxL2F1dGgvbG9naW4iLCJleHiOjE2NTk3NzExMTR9.7YO-WLppNUbf8yqnOi0ouDwU0zcdGBB9Vsoex$_A1piE$	replacement token when it's expired, token lifespan is longer
Type	Bearer	Token type
Username	seno	username used to generate token
Role	`["ROLE_ADMIN","ROLE_USER"]`	access type of username seno

The client application consists of the Card Management System application and the Web Back Office application, the Card Center application is used to enter employee data into the card as well as to synchronize the card data with employee data into a database. Employee data entered the card is in the form of employee number (NIP) and expiration date, the NIP is entered into the card for easy integration into other systems. Then for expiration so that each card can be limited to a maximum age of the card. The card center application does not directly perform data operations in the database but communicates with the Web Service application using a REST API with authentication using a token. The web back-office application display is shown in Figure 6.

Desktop-based card center application developed using the Java programming language, the front page is shown in Figure 7 which is a form for personalization. Personalization is a process of entering employee data into a card, employee data that is entered into a smart card, one of which is an employee number or NIP. The employee data that will be personalized is obtained from the previous web portal application as shown in Figure 8, the same as the web portal application for data communication to the web service application using tokens. The type of card used is Mifare 1K and other types of cards that run at a frequency of 125kHz and 13.56MHz. Especially for the Mifare 1K type card, before the employee data is entered into the smart card, the smart card must first be configured for security to perform authentication so that the card data cannot be directly read using a smart card reader. While for other types of cards, employee data is not written but only Unique Identifier (UID) card data is taken. Unique Identifier (UID) card is unique information on each card, UID will be combined with employee data in the database.

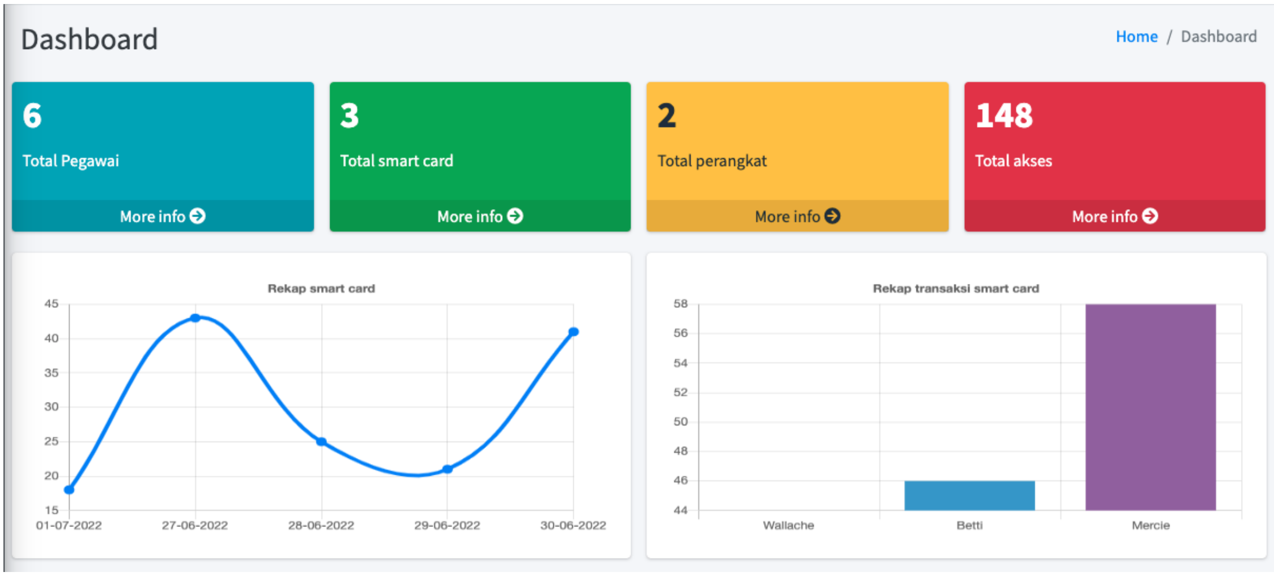
TABLE III. Command example

Command	Data (hex)
Remove user	7E 08 01 85 00 01 00 01 7B 03
Add user	7E 1F 01 84 01 00 01 00 00 00 00 6E C5 6A C9 00 00 00 00 58 00 FF FF 63 0C 1F 00 00 00 00 00 5A 2B

Some server applications such as web service applications, log collector applications, and subscriber applications doesn't have display model because it runs as a service and runs on server background. Web service application is the main application that serves all applications that consists of client applications and server applications. In this application, data communication on web service application is directly connected to the database to perform data manipulation.

An important task performed by the Subscriber Application is to send commands directly to the reader sent to reader using a socket obtained from the Web Service application with the MQTT protocol. Subscriber App bridge to communicate with the reader, so the application does not have to directly communicate with the other reader uses the socket protocol but only provides the data needed to be sent to the reader. The table III an example of the command used to communicate to a reader in socket communication.

The table above are examples of commands used in deleting users (RFID) and adding users, in each command, there are sections such as headers, data lengths, commands, devices, data parameters, XOR operations, and SUM operations. The following table IV shows a detailed description of a command.

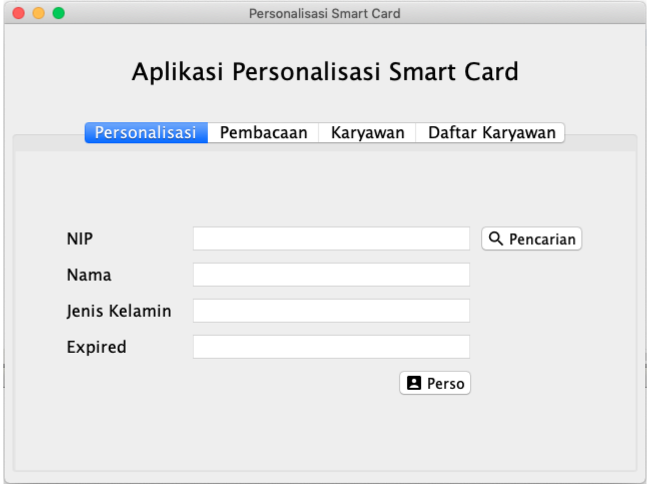


Dashboard

Home / Dashboard

6	3	2	148
Total Pegawai	Total smart card	Total perangkat	Total akses
More info ➜	More info ➜	More info ➜	More info ➜

Figure 6. Dashboard interface



Personalisasi Smart Card

Aplikasi Personalisasi Smart Card

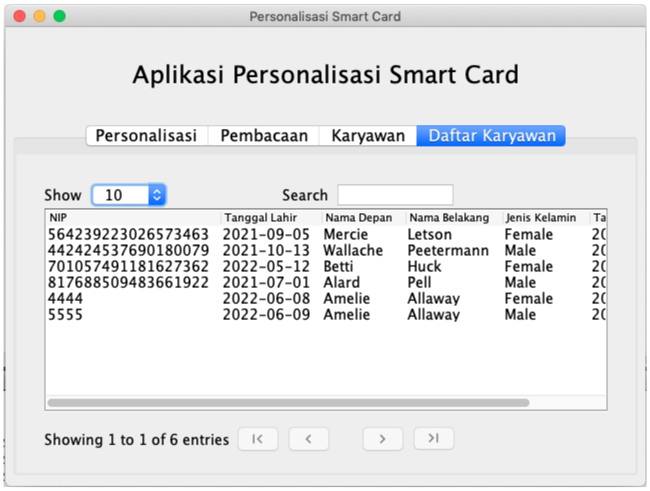
NIP

Nama

Jenis Kelamin

Expired

Figure 7. Front page



Personalisasi Smart Card

Aplikasi Personalisasi Smart Card

Show 10 Search

NIP	Tanggal Lahir	Nama Depan	Nama Belakang	Jenis Kelamin	Ta
564239223026573463	2021-09-05	Mercie	Letson	Female	2(
442424537690180079	2021-10-13	Wallache	Peetermann	Male	2(
701057491181627362	2022-05-12	Betti	Huck	Female	2(
817688509483661922	2021-07-01	Alard	Pell	Male	2(
4444	2022-06-08	Amelie	Allaway	Female	2(
5555	2022-06-09	Amelie	Allaway	Male	2(

Showing 1 to 1 of 6 entries

Figure 8. Employee list page

TABLE IV. Details of the command

Component command	Value (hex)	Description
Header	7E	Constant value
Data length	08	Data length from device to SUM
Device	01	Device code or Node id
Command code	85	Code for command
Data	00 01 00 01	Data parameters used
XOR	7B	XOR operation result
SUM	03	SUM operation result

Furthermore, after giving a command to a reader, it will then get a response as Acknowledgment (ACK) when it succeeds, while if it fails, it will get an Unacknowledged (NACK) response. The process of sending commands to get a response time takes 100 milliseconds to 6 seconds depends on the parameters of the data sent. When data send successfully to the reader, it will then send a notification via the MQTT protocol to be received by the web service application.

Furthermore, the main function of the Log Collector is to receive all activity logs from the reader, one of which is to read activity when pasting a card. The activity log obtained will be published using the MQTT protocol, and the activity log will be subscribed to by a web service application, which will then be stored in a database. The communication

TABLE V. The data format used by the reader

Activity	Data (hex)	Data (ASCII)
Tap card	32 32 27 30 37 2F 32 39 20 31 32 3A 35 34 3A 33 39 20 5B 30 30 31 2E 31 37 3A 30 42 5D 28 30 29 32 33 35 37 36 3A 30 35 36 36 34 20 20 20 20 20 4E 6F 20 53 75 70 70 6F 72 74 65 64 20 28 4D 31 31 29 4E 6F 72 6D 61 6C 20 41 63 63 65 73 73 0A	22’07/29 12:54:39 001.17:0B23576:05664 No Supported (M11)Normal Access

used between the Log Collector and the reader is socket communication, where the reader is the server socket while the log collector is a client socket. Reader researchers do not do application development but only use the reader. There is a mechanism to send (publish) to the connected client socket when there is an activity. The Table V shows the data format used by the reader.

The card log data in the Table V is 84 bytes in size and then converted into ASCII format, with the information contained in the card number and the time when the card taps or pastes the card. Another piece of information is the status when pasting the card. The card status can be successful or not. Success means that the card is recognized by a reader, while failure means that the card failed to be recognized nor has not been registered by the reader. Normal Access indicates that the card was successfully recognized or registered.

B. Testing

In this section, we perform a functional test of application functions to ensure the system can run as expected. Each component has been tested, from the Web service to Card Management System.

1) Web service

Web service testing uses unit tests by requesting certain endpoints, and then the application will provide response data in the form of JSON. When the Web service has responded according to the desired data, it can be said to be successful. Table VI shows the test scenario.

2) Web back office

A web service is said to be successful before being displayed on a certain page when the functions and operations that can be performed are appropriate. Table VII shows the test scenario.

TABLE VI. Functionality test for web service app

No	Test Case	Expected Result	Result
1	Dashboard page API endpoint	Access data based on date, device, and RFID will appear in JSON format	Succeed
2	Access page API endpoint	The function of storing, updating, deleting, and retrieving RFID access data can be done then the response data is in JSON form	Succeed
3	Authentication page API endpoint	The token creation and refresh token functions can work then the response data is in JSON form	Succeed
4	Device page API endpoint	The function of saving, updating, deleting, and retrieving device data can work then response data in JSON form	Succeed
5	Employees page API endpoint	The function of saving, updating, deleting, and retrieving employee data can work then response data in JSON form	Succeed
6	Personalization page API endpoint	The function of saving, updating, deleting, and retrieving personalization data can work then response data in JSON form	Succeed
7	User page API endpoint	The function of saving, updating, deleting, and retrieving user data can function then response data in JSON form	Succeed

3) Card management system

Testing on the Card Management System to ensure the operation functions on the RFID can run, the operation is like reading or writing RFID with employee data. It is said to be successful when the employee data written on the card appears when it is read. Table VIII shows the test scenario.

4) RFID Reader AR-725E

Tests are conducted on RFID cards and card readers to ensure that the latter can detect the former. Various scenarios are simulated by attaching the cards from different distances between the card reader and the RFID card.

Table IX indicates that the AR-725E reader is capable of detecting RFID cards with a maximum limit of 3 cm. However, when two RFID cards are stacked or placed close,

TABLE VII. Functionality test for web back office

No	Test Case	Expected Result	Result
1	Dashboard page	Data access based on date, device, and RFID will be displayed	Succeed
2	Access page	The function of storing, updating, deleting, and retrieving RFID access data can work	Succeed
3	Login page	The function to enter the system can be done	Succeed
4	Device page	The save, update, delete, and retrieved device data functions can work	Succeed
5	Employee page	The save, update, delete, and retrieved employee data functions can work	Succeed
6	Personalization page	The save, update, delete, and retrieved personalization data functions can work	Succeed

TABLE VIII. Functionality test for card management system

No	Test Case	Expected Result	Result
1	Personalization page	RFID has been successfully filled in employee data and read according to the written data	Succeed
2	RFID data reading page	On the RFID reading menu will display employee information	Succeed
3	Employee list page	Employee data will appear and match what is displayed on the website	Succeed

TABLE IX. RFID reader test

No	Card UID (dec)	Test Case	Result
1	31294:14596	Bring the RFID tag within a distance of 1 cm from the RFID reader	Detected
2	31294:14596	Bring the RFID tag within a distance of 3 cm from the RFID reader	Detected
3	31294:14596	Bring the RFID tag within a distance of 5 cm from the RFID reader	Not detected
4	07434:10511	Bring the RFID tag within a distance of 1 cm from the RFID reader	Detected
5	07434:10511	Bring the RFID tag within a distance of 3 cm from the RFID reader	Detected
6	07434:10511	Bring the RFID tag within a distance of 5 cm from the RFID reader	Not detected
7	36284:42921	Bring the RFID tag within a distance of 1 cm from the RFID reader	Detected
8	36284:42921	Bring the RFID tag within a distance of 3 cm from the RFID reader	Detected
9	36284:42921	Bring the RFID tag within a distance of 5 cm from the RFID reader	Not detected
10	31294:14596 and 07434:10511	Bringing 2 RFID close to the RFID reader by stacking them	The detected RFID card is the second card

the reader is only able to detect the top or back RFID card due to signal interference or collision.

5. Conclusions and Future Work

In this research, a door access system has been designed using IoT concept and Micro Service development. Several applications that run on the client and server side are used as a unit to display information. card user activity data and manage smart card usage. Communicating with the reader is made easier by simply knowing the required data parameters. If the previous one had to know the complete socket protocol with the required data frame arrangement, in addition, transaction data on card usage in accessing rooms can also be used to predict which rooms are widely used and track the whereabouts of an employee or teacher on campus. The use of authentication contained in the smart card prevents copying the data in it, resulting in the reading process, especially rewriting, being difficult to do. From the application side, communicating is also not easy to do because it requires a token, which every time user log in, it always changes and has a time limit of tokens. However, in this study, the focus is on the features. For example, by using pupils or detecting faces indoor access, additional security features can then be developed, which, of course, will add security compared to RFID.

6. Acknowledgements

The researcher expresses his deepest gratitude to Mr. Badrus, who has made and installed it. Door access prototype and don't forget to also thank the Malang State Polytechnic for providing Booth or place at the 40th-anniversary event to display the door access RFID system.

References

[1] Vishawjyoti, "E-wallet," *Blockchain for Business: How it Works and Creates Value*, pp. 97–111, 1 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/9781119711063.ch5

[2] N. Syifa and V. Tohang, "The use of e-wallet system," *Proceedings of 2020 International Conference on Information Management and Technology, ICIMTech 2020*, pp. 342–347, 8 2020.

[3] D. S. Soegoto and M. P. Tampubolon, "E-wallet as a payment instrument in the millennial era," *IOP Conference Series: Materials Science and Engineering*, vol. 879, p. 012139, 7 2020. [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/879/1/012139

[4] M. Yang, A. A. Mamun, M. Mohiuddin, N. C. Nawi, and N. R. Zainol, "Cashless transactions: A study on intention and adoption of e-wallets," *Sustainability 2021, Vol. 13, Page 831*, vol. 13, p. 831, 1 2021. [Online]. Available: https://www.mdpi.com/2071-1050/13/2/831/htmhttps://www.mdpi.com/2071-1050/13/2/831

[5] N. B. P. Duy and N. T. P. Giang, "Contactless payments through e-wallets on mobile devices in the context of covid 19 at vietnam," *2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022*, pp. 385–392, 2022.

[6] N. Ya'Acob, A. L. Yusoff, S. S. Sarnin, D. M. Ali, N. F. Naim, M. Kassim, and N. A. B. M. Azni, "A cashless payment transaction (cpat) using rfid technology," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, pp. 191–199, 10 2019. [Online]. Available: https://ijeecs.iaescore.com/index.php/IJEECS/article/view/19961

[7] M. A. A. Putra, M. Q. Huda, and E. Fetrina, "An evaluation of e-money products using utaut 2 model (the case of bank mandiri)," *2019 7th International Conference on Cyber and IT Service Management, CITSM 2019*, 11 2019.

[8] D. Octabriyantiningtyas, E. Suryani, and A. R. Jatmiko, "Modeling customer satisfaction with the service quality of e-money in increasing profit of pt. telekomunikasi indonesia," *Procedia Computer Science*, vol. 161, pp. 943–950, 1 2019.

[9] E. Budianita, O. Okfalisa, and M. R. Assiddiki, "The prediction of e-money circulation: Backpropagation with genetic algorithm adoption," *2021 International Congress of Advanced Technology and Engineering, ICOTEN 2021*, 7 2021.

[10] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight rfid protocol for medical privacy protection in iot," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 1656–1665, 4 2018.

[11] N. A. Hussien, S. A. A. A. Alsaidi, I. K. Ajlan, M. F. M. Firdhous, and H. T. A. Rikabi, "Smart shopping system with rfid technology based on internet of things," *International Journal of Interactive Mobile Technologies*, vol. 14, pp. 17–29, 2020.

[12] H. Mansor, T. M. A. M. Fadzir, T. S. Gunawan, and Z. Janin, "Safety and security solution for school bus through rfid and gsm technologies," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, pp. 804–814, 2 2020. [Online]. Available: https://ijeecs.iaescore.com/index.php/IJEECS/article/view/20652

[13] R. A. Gining, S. S. Fauzi, I. M. Ayub, M. N. Jamaluddin, I. Puspitasari, and Okfalisa, "Design and development of activity attendance monitoring system based on rfid," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, pp. 500–507, 1 2020. [Online]. Available: https://ijeecs.iaescore.com/index.php/IJEECS/article/view/19413

[14] D. Eridani, E. D. Widianto, I. P. Windasari, W. B. Bawono, and N. F. Gunarto, "Internet of things based attendance system design and development in a smart classroom," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, pp. 1432–1439, 9 2021. [Online]. Available: https://ijeecs.iaescore.com/index.php/IJEECS/article/view/25848

[15] H. A. Khan, R. Abdulla, S. K. Selvaperumal, and A. Bathich, "Iot based on secure personal healthcare using rfid technology and steganography," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, pp. 3300–3309, 8 2021. [Online]. Available: https://ijece.iaescore.com/index.php/IJECE/article/view/24618

[16] P. Jiang, K. Yan, H. Chen, and H. Sun, "Building of online evaluation system based on socket protocol," *Computer Science and Information Systems*, vol. 19, pp. 185–204, 1 2022.

[17] A. S. Nugroho, S. A. Arfiyani, A. Nursyahid, T. A. Setyawan, Helmy, and S. H. W. Sasono, "Implementation of transfer control protocol(tcp) sockets to monitor soil moisture using star topology on agricultural land," *2021 8th International Conference on Information Technology, Computer and Electrical Engineering, ICITACEE 2021*, pp. 213–218, 2021.

[18] H. Si, C. Sun, B. Chen, L. Shi, and H. Qiao, "Analysis of socket communication technology based on machine learning algorithms under tcp/ip protocol in network virtual laboratory system," *IEEE Access*, vol. 7, pp. 80 453–80 464, 2019.

[19] D. Puspitasari, Noprianto, M. A. Hendrawan, and R. A. Asmara, "Development of smart parking system using internet of things concept," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, pp. 611–620, 10 2021. [Online]. Available: https://ijeecs.iaescore.com/index.php/IJEECS/article/view/25856

[20] N. Noprianto and V. N. Wijayaningrum, "Smart card security mechanism with dynamic key," *JURNAL INFOTEL*, vol. 13, pp. 197–204, 12 2021. [Online]. Available: https://ejournal.st3telkom.ac.id/index.php/infotel/article/view/652

[21] R. Abdulla, A. Abdillahi, and M. K. Abbas, "Electronic toll collection system based on radio frequency identification system," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, pp. 1602–1610, 6 2018. [Online]. Available: https://ijece.iaescore.com/index.php/IJECE/article/view/9321

[22] A. Abdulkareem, A. C. O. A., and T.-O. A. E., "Development and implementation of a miniature rfid system in a shopping mall environment," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, pp. 1374–1378, 4 2019. [Online]. Available: https://ijece.iaescore.com/index.php/IJECE/article/view/10682

[23] M. O. Adebiyi, R. O. Ogundokun, A. I. Nathus, and E. A. Adeniyi, "Smart transit payment for university campus transportation using rfid card system," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, pp. 4353–4360, 10 2021. [Online]. Available: https://ijece.iaescore.com/index.php/IJECE/article/view/22797

[24] M. E. Beqqal, M. Azizi, and J. L. Lanet, "Multimodal access control system combining rfid, fingerprint and facial recognition," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, pp. 405–413, 10 2020. [Online]. Available: https://ijeecs.iaescore.com/index.php/IJEECS/article/view/19756

[25] M. K. K. Wen, N. binti Ahmad, and S. H. binti Ruslan, "Arduino based outing and attendance system for boarding school students," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, pp. 1053–1061, 11 2020. [Online]. Available: https://ijeecs.iaescore.com/index.php/IJEECS/article/view/21908

Noprianto received bachelor degree from the Technical Information, AKAKOM Yogyakarta, in 2011 and master of Engineering (M.Eng.) degree in Electrical and Information Technology Engineering Department, Gadjah Mada University in 2017. His research interests are Computer Vision, Internet of Things, and Software Engineering.

Rokhimatul Wakhidah graduated from State University of Malang with a major in Informatics Education in 2011 and completed master of Informatics degree from Institut Teknologi Bandung in 2015. Her works in education, business and informatics can be found on published conferences and paper.

Rudy Ariyanto graduated from bachelor degree from Brawijaya University majoring in Electrical Engineering majoring in 1997. He completed master's in Computer Science degree from Gadjah Mada University in 2014. He interests in IoT and Data Science.

Yan Watequlis Syaifudin is an associate professor at State Polytechnic of Malang, Indonesia. He received the bachelor's degree in informatics from Bandung Institute of Technology, Indonesia, in 2003 and the master's degree in information technology from Sepuluh Nopember Institute of Technology, Indonesia, in 2011. Finally, in 2021, the Ph.D. degree in information and communication systems was received from Okayama University, Japan, respectively. He is also a reviewer in a journal and conferences held by University of Bahrain. His research interests include technology enhanced learning, intelligent systems, and data analytics.