

Securing Smart Buildings Using RFID and Fingerprint Technologies

Vian S.Al-Doori

Al-Rafidain University College
Baghdad, Iraq
vian.kasim@ruc.edu.iq

Abdulqader Faris Abdulqader

Al-Noor University College
Nineveh, Iraq
abdulqader.faris@alnoor.edu.iq

Mohammed Abdul Jaleel Maktoof

Al-Turath University College
Baghdad, Iraq
mohammed.maktoof@turath.edu.iq

Serhii Lienkov

Military Institute of Taras Shevchenko
National University of Kyiv
Kyiv, Ukraine
serhii.lienkov@knu.ua

Abstract — Background: The emergence of smart buildings, heavily affected by Internet of Things (IoT) devices and technology, creates a need for increased security solutions. The vulnerability of large structures to security breaches has become a significant worry as they grow increasingly linked.

Objective: This study aims to investigate the efficacy of combining Radio Frequency Identification (RFID) with fingerprint technology to improve security in smart buildings. The final objective is to create a solid RFID-based fingerprint-building lock mechanism to provide more security.

Methods: A two-pronged research strategy was used to assess the effectiveness of the suggested security solution. Initially, a comprehensive literature review was conducted in order to have a better understanding of the current state of intelligent building security. Subsequently, a detailed examination of an intelligent building incorporating RFID and fingerprint technology offered pragmatic observations regarding their implementation and benefits.

Results: The case study findings indicate a significant increase in security levels after integrating RFID and fingerprint systems, with a significant decrease in security breach incidences. When coupled with these technologies, they provide improved authentication and greatly minimize the possibility of unwanted access.

Conclusion: There is a possible route for fortifying security measures in smart buildings by combining RFID and fingerprint technology. Such integrated techniques improve the safety of building occupants and contribute to protecting building assets, indicating a watershed moment in the field of intelligent building security.

I. INTRODUCTION

Top-tier intelligent building security systems, operable via the premise's Wi-Fi and voice commands, allow extensive remote administration through smartphones. These systems enable receiving alarms, viewing security cameras, and remotely locking/unlocking doors and adjusting illumination, providing constant surveillance of your home or business. Furthermore, they could let you know if any environmental sensors, like smoke alarms, go off [1].

Top-tier intelligent building safety systems often also command "non-security" devices. For example, all of the below-mentioned setups support smart plugs, allowing control of any electronic device in the house to be operated remotely. Utilizing a smart thermostat is a straightforward and efficient method to decrease expenses [2].

The primary function of this entity is to guarantee the security and safety of facilities or other desired areas by preventing unauthorized access. The more safeguards there are in place to prevent theft, the better. In our project, for instance, we layered two forms of identification a card and a fingerprint — to prevent unauthorized access [3], [4].

For the projector to function correctly, we need to replace the sensors with others of high quality in manufacturing, and we need to replace the monitor with a larger one because we cannot write much info in it because of its tiny size and has a large limited words display [5], [6].

Due to the proliferation of Internet of Things (IoT) technology, which has made it feasible to link previously unconnected objects and systems in a building, smart building security systems have gained prominence in recent years. Being able to keep tabs on and adjust several safety settings The remote accessibility of these systems offers excellent comfort and security to building proprietors and occupants [7].

Connectivity to Wi-Fi networks is a significant component of smart building security systems since it facilitates integration capabilities with other smart gadgets and systems. Because of this, people may control their system security from anywhere using their mobile devices or desktop PCs.

These systems also use cameras and sensors to monitor the premises and identify unusual behaviour, such as entering or exiting restricted areas. They may notify the building manager or security staff to take swift action [8].

These systems provide protection and allow for the remote regulation of non-security equipment like lighting and climate,

resulting in reduced utility costs and enhanced living conditions [9], [10].

Although innovative architectural security systems offer numerous advantages, they also face challenges. For instance, there is a risk that sensors and other devices may malfunction due to setup or production flaws, compromising the system's reliability and potentially leading to false alerts or undetected security breaches.[11]

To sum up, high-tech security systems in buildings are a crucial part of today's building management. They provide several safety functions that can be seen and adjusted from a distance, leading to greater ease and comfort. However, any problems with installing or producing sensors and devices must be fixed if these systems are to be relied upon and performed as intended.

A. Aims of Article

This article explores the use of RFID and fingerprint technologies to enhance security in intelligent buildings that rely heavily on Internet of Things (IoT) devices and technologies. The main objective is to design a high-security RFID-based fingerprint-building lock system. The paper outlines the techniques used to gather data, including literature analysis and a case study of an intelligent building that deployed the technologies to determine their effectiveness in strengthening smart building security.

The article provides an overview of top-tier intelligent building security systems that allow remote administration through smartphones, which offer extensive control over security and non-security devices, such as smart plugs and thermostats. The focus then shifts to using RFID and fingerprint technologies to improve security, including a layered authentication approach involving both a card and a fingerprint.

The case study presented in the article shows that the use of RFID and fingerprint technologies in intelligent buildings can lead to increased security and decreased incidents of security breaches. The study concludes that RFID and fingerprint technologies can be effectively utilized to strengthen the security of intelligent buildings, benefitting the safety of individuals and protecting building assets.

This article provides valuable insights into using RFID and fingerprint technologies in intelligent building security systems, highlighting their potential benefits and challenges. It provides a comprehensive review of the current state of the art in intelligent building security. It sets the stage for further studies into the use of these technologies in future intelligent building security systems.

B. Problem Statement

The problem statement addresses the critical challenge of enhancing security measures in smart buildings by integrating RFID (Radio et al.) and fingerprint technologies. With the increasing adoption of intelligent building systems that leverage the Internet of Things (IoT) and automation, the vulnerability to security breaches and unauthorized access becomes a significant concern.

Traditional security systems in buildings, such as access cards and passwords, have shown limitations regarding reliability and susceptibility to breaches. The article recognizes the need for a more robust and efficient security solution to address these shortcomings and provide enhanced protection to occupants, assets, and sensitive information within intelligent buildings.

Integrating RFID and fingerprint technologies offers the potential to overcome these limitations by providing a multifactor authentication approach. By combining RFID tags or cards with biometric fingerprint scanning, the system can ensure higher security, mitigating the risk of unauthorized access and identity fraud.

The problem statement delves into the specific challenges the proposed system aims to address, including ensuring seamless integration of the two technologies, optimizing performance, and reducing false positives or negatives during authentication. Additionally, the article may consider scalability and cost-effectiveness as essential factors for implementing the system on a larger scale.

II. LITERATURE REVIEW

Today's homes, workplaces, retail establishments, and financial institutions need stringent safety measures. Smart lock systems are used to provide security for these areas. Many cutting-edge smart door locks have been developed to secure and open the system. These locks may be opened with a biometric, RFID card, pin, password, or Internet of Things (IoT) device [12], [13]. Users of these fastening systems often enter a PIN, use a biometric, or swipe an RFID card to get access. There is no security hierarchy in place for these systems. To increase security, the user must unbolt the system in a Minimum of two security sequences.

There must be a guest unlocking option in the building's lock system. Intruders may misinterpret the choice and utilize it to gain access to a residence [14]. As a result, we can provide our guests with two levels of protection. For safety reasons, the owner must complete this process. The smart locks can currently be hacked and opened. The proposed solution can overcome the present security problems [15]. The system's three layers of protection help ensure the user's privacy. The primary goal of this system is to provide the user with a safe environment to live, work, or store valuables and documents. Thus, The audience can grasp this project, which will be helpful for future work. This project offers several opportunities for mechanization and modernization. This project may be recreated with a different microcontroller and approach.

Nowadays, everyone, whether they are at home or in the workplace, must deal with the protection of corporate property. In today's hostile, cruel world, when individuals have few options for physically protecting their most prized items, security systems are one of the biggest concerns. Instead, they develop a new approach that offers more robust, trustworthy, and dispersed security. In today's interconnected world, information from everywhere is at your fingertips [16]. The risk of having one's data hijacked is very severe. Because of the

potential for these mishaps, it is essential to use some identity verification while entering one's data. Personal identity is becoming more important these days [17]. Passwords and identity cards are the most common forms of standard personal recognition. These techniques are now very unreliable since it is simple to compromise passwords, and ID cards might need to be included [18].

The fingerprint-based locking system's design and implementation are adaptable. This door lock system is less expensive than similar products on the conventional market. Our fingerprint-based lock system has a high accuracy rate and quickly recognizes fingerprints, allowing for perfect user combinations and providing tighter security [19].

In this paper, the project was built in stages, including the writing of the code (driver) that controls the Microcontroller in C language, the implementation of the entire project on a solvent weld testing board, the soldering of the circuits on Vero-boards, and the coupling of the entire project to the casing [20]. The proof of concept project was constructed on a breadboard, the power supply was sourced from a benchtop power source in the electronics lab, and the mechanism may be used more generally on any door with restrictions. A Microcontroller Unit (MCU), the PIC16F628A, was used to create the fingerprint-based security door lock, which only lets in authorized users after reading their fingerprints via a fingerprint scanner. The fingerprint reader is the primary input device for this built-in security mechanism. The microcontroller compares the fingerprints read to those stored in its memory. When a match is found, the microcontroller sends a HIGH signal, which triggers the transistor-relay switching step, which opens and closes the simulated automatic door that allows entrance to the secure building [21]. The functioning status of this integrated security system is shown using an alphanumeric liquid crystal display (LCD) in this configuration. The first prompt prompts the user to provide a fingerprint. Moreover, the message "ACCESS GRANTED" or "ACCESS DENIED" is shown depending on whether or not a match was found.

This study proposes a biometrically protected Building Automation System that is affordable. The suggested system's circuit design, modelling, and experimental analysis are all addressed. In this paper, we present a building automation system wherein users may operate various in-building appliances from afar using Bluetooth technology and an Android app downloaded to a user's Smartphone. The residence is additionally protected with a biometric system that uses fingerprints [22]. Thanks to this security system, only authorized individuals have access to the building's door lock and automation circuits. Push buttons for erasing fingerprints and adding new ones are incorporated for convenience. Building automation is created utilizing an 8051 microcontroller and an HC05 Bluetooth module. Arduino Uno and an R305 fingerprint sensor are used in the biometric system. A relay, LED lights, a DC motor, and a solenoid lock are utilized as loads to show how the system works. Several metrics are used to evaluate prototypes [23].

III. METHODOLOGY

Real-time system protection is provided through fingerprint verification. A fingerprint may be recognized. Information goes to the microcontroller for authentication [24]. RFID technology has found widespread use in the field of security. We used these two algorithms as well. Automated fingerprint system Define the existence of a set of photos, process and extraction from features, as well as matching features and on numerous components [25]. Biometrics is the most reliable way to authenticate someone's identity. Active security is the primary benefit of RFID, Fingerprint, and RFID. RFID can detect almost any kind of item using a wireless transmission frequency. An electrical system that uses radio waves to send and receive data is known as an RFID system. It helps locate, identify, and classify a wide variety of things. The Applicable system includes an LCD screen, a fingerprint scanner, and an RFID reader. RFID scans a person's identification number in this reader. If what you say is accurate, then the only way to provide access to someone is to display that user's name on the display when the green light is on. If it is incorrect, the whole procedure must be redone. With the red light on, it may be turned off. The fingerprint scanner scans the fingerprint when it is legitimate and sends it to the microcontroller for identification. If there is a match between the scanned fingerprint and one of the recorded fingerprints in the database, the microcontroller will allow access [26].

By offering active security protocols that can identify any item or person entering or exiting the facility, the combination of fingerprinting and RFID technologies may strengthen the safety of a building. Although fingerprint technology may provide a trustworthy method of confirming a person's identification, RFID may be used for locating, detecting, and classifying various things.

The system we have discussed uses an automated fingerprint system to identify and verify a person's existence. This system processes and extracts information from the fingerprint before matching it with the database to authenticate the user. A cross-check is performed between the ID number read by the RFID reader and the database saved to confirm the identification of the individual [27].

The system also has an LCD panel that shows the username when access is permitted, and the green colour is switched on. If the individual's identification number or fingerprints do not match, the software will switch off, illuminating a red light [26].

A security system for smart buildings that combines fingerprint and RFID technology may offer a level of protection that is dependable and strong.

Both the passive security procedures supplied by the RFID system and the reliable biometric identification supplied by fingerprint technologies may guarantee that only legally permitted individuals can enter the building, contributing to an overall improvement in the building's level of security and safety.

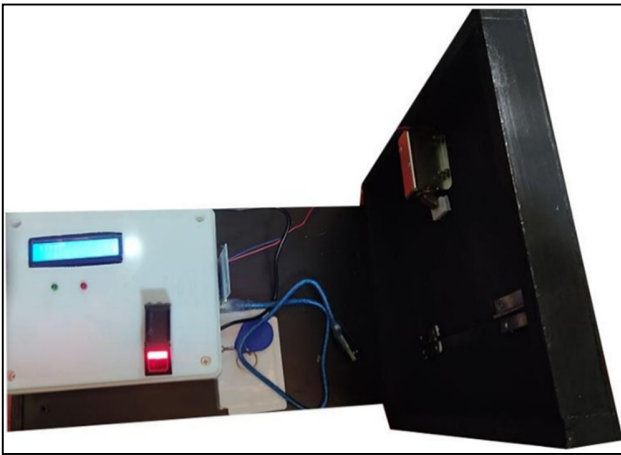


Fig. 1. Final project format

A. Types of protection systems

Home security [2] systems come in various types and configurations, each designed to meet homeowners' unique needs and preferences. From entry sensors and cameras to critical fobs and panic buttons, a wide range of devices and technologies are available to help enhance home security and provide peace of mind to homeowners.

Security camera: Smart security cameras are typically designed to connect to Wi-Fi networks, allowing for remote access and control through a smartphone or computer. By connecting to Wi-Fi, users can live stream footage from their cameras, receive notifications when motion is detected, and even speak to anyone on camera through the two-way audio feature [28]. Many smart security cameras also include night vision capabilities, which can be either infrared or colour-based, allowing for clear footage even in low-light conditions. In addition, these cameras often have cloud or local storage options for storing recorded footage [29]. Smart security cameras can also integrate with other smart home devices and platforms, such as Amazon Alexa or Google Assistant, allowing for voice control and automation. This can include turning the cameras on or off, adjusting settings, and integrating with other smart home devices for a more comprehensive home security system [30].

The entry sensor is designed to detect when doors or windows are opened or closed. These sensors typically consist of two parts: one attached to the door or window and another to the frame. When the door or window is closed, the two parts of the sensor come into contact with each other, completing an electrical circuit. When the door or window is opened, the circuit is broken, and the sensor sends an alert. Entry sensors are essential for home security systems, as they can alert homeowners to potential break-ins or unauthorized entry. These sensors are commonly placed on windows and doors on the ground floor, as these are intruders' most common entry points. Many entry sensors are battery-operated and have adhesive backings, making them easy to install without professional assistance. Some entry sensors may also be connected to a home

security system or smart home hub, allowing for remote monitoring and control [3].

Keypad: Many security systems require a code to be entered on a keypad to arm or disarm the system. The keypad [23] is typically mounted to the wall near the entry point of the home or business and can also be placed on a flat surface. When arming or disarming the security system, the user enters a code on the keypad, typically a sequence of numbers or a combination of letters and numbers. This code serves as a means of verifying the user's identity and ensuring that only authorized individuals can control the security system. In addition to the keypad, some security systems may include other methods of arming or disarming the system, such as a key fob or mobile app. These methods can provide added convenience and flexibility, allowing users to arm or disarm the system remotely without needing a physical keypad.

Key fob: Key fobs are a popular method of arming and disarming security systems, particularly for those who want to avoid using a keypad. Key fobs allow users to control their security system with the touch of a button without needing a code or physical keypad. With a critical fob, users can quickly arm or disarm their security system from a distance, making it convenient for those who may be upstairs or in another area of the home. Key fobs typically range several feet, allowing users to control their security system from a distance [31].

In addition to their convenience, key fobs provide added security, as they can be carried with the user at all times. This means that the security system can be quickly armed or disarmed in an emergency without locating a physical keypad or entering a code.

Panic button: Panic buttons are a valuable addition to home security systems, as they provide an easy and fast way to alert emergency services in an emergency. Panic buttons can be used to call for help from the police, hospital, fire department, or other emergency services. Panic buttons can be installed in various locations throughout the home, such as on a bedside table or near the front door. Some panic buttons may also be wearable, allowing users to carry them anywhere. When a panic button is activated, it sends an alert to a monitoring centre or emergency services, depending on the type of system being used. This alert can help ensure that help is quickly dispatched to the location of the emergency, potentially saving lives or preventing further harm [32].

Base station: Base stations are a vital component of many home security systems, as they serve as the central hub through which all connected devices communicate with the mobile application and each other. Like Grand Central Station, the base station is a central hub or control centre for the home security system, allowing all devices to communicate and work together seamlessly. The base station typically connects to the internet and serves as a bridge between the various devices in the system and the user's mobile application. Through the base station, users can receive notifications and alerts from the various devices in the system, including entry sensors, motion sensors, and

cameras. The base station can also control the system, allowing users to arm or disarm the system, adjust settings, and receive real-time updates on the status of their security system.

Yard signs and/or window stickers: Yard signs and window stickers are a common feature of many home security systems, as they can serve as a visible deterrent to potential burglars or intruders. By prominently displaying a yard sign or window sticker indicating that a home has a security system, homeowners can send a clear message to potential intruders that their home is protected and that any attempt to break in will be met with an alarm or other security measures. This can often deter burglars or intruders from attempting to enter the home, as they may seek out easier targets without visible security measures. Yard signs and window stickers can also provide peace of mind to homeowners, as they serve as a visible reminder of the security measures in place to protect their homes and property [4].

B. Hardware Requirement

The following pieces of equipment are essential for implementing a security system that utilizes RFID and fingerprint technologies in smart buildings:

- 1) The FPM10A, or any similar fingerprint sensor module, takes pictures of fingerprints and runs them through an authentication procedure [33].
- 2) The radio frequency identification (RFID) reader is a device that can read and send RFID tags' identifying numbers.
- 3) A board with a microcontroller, such as an Arduino Uno, works as the system's brain and interprets data from the fingerprint scanner and RFID reader.
- 4) Data such as the current user and system status are shown on this panel (locked or unlocked).
- 5) An LED [34] in the back illuminates the fingerprint reader even in dim lighting.
- 6) The system's components cannot function without a DC power source.
- 7) Connecting the different pieces of hardware requires cables and connectors of the appropriate kind.
- 8) Secure housing for the system's components [35] is essential for preventing tampering and extending the system's useful life.
- 9) Integration of a keypad is proposed to augment the system's security. Including a keypad enhances security by offering additional protection through PIN-based authentication. This innovation enhances the security measures of the RFID tag and fingerprint authentication by introducing a knowledge-based element. A PIN system dramatically strengthens the security infrastructure, establishing a more robust defence against unwanted entry. Additionally, it offers adaptability for situations where RFID or fingerprint authentication may be compromised or impractical. The keypad must incorporate an encrypted connection with the microcontroller to guarantee that the PIN is safely transferred and saved, hence preserving the overall security integrity of the system.
- 10) A secure element is crucial for protecting sensitive data, including cryptographic keys and biometric templates,

by providing secure storage and cryptographic operations. This hardware module executes secure cryptographic operations and offers a tamper-resistant setting for data storage. It guarantees the authenticity and privacy of user data, playing a crucial role in upholding the entire system's security. The system conforms to rigorous security protocols and successfully mitigates potential digital vulnerabilities by including this safe feature.

The hardware prerequisites for establishing a robust RFID and fingerprint-based security system in intelligent structures, accompanied by a PIN-based keypad and secure data management, are generally uncomplicated and readily available. When these components are joined, they create a robust and reliable security system that provides increased peace of mind for smart buildings and their occupants.

The successive stages in constructing a highly secure building lock system that utilizes RFID technology and fingerprint recognition include a thorough and all-encompassing strategy. This method includes researching, creating a detailed plan, selecting appropriate hardware components, designing the necessary software, conducting rigorous system testing, deploying the system, providing training, and ensuring ongoing maintenance. By following this systematic approach, the finished system will offer solid and adequate security measures for the building.

1) *RFID and Fingerprint Smart Building Security using Arduino Uno (R3)*: An improved RFID-based biometric authentication lock system might include the following steps:

Determine the most effective design features and technologies for RFID and fingerprint-based door [2]locking systems presently on the market.

Information-gathering About Needs: Find out what you want from the system regarding security level, number of closed doors, and the like.

Planning: Plan the system's architecture, including the hardware, software, and networking infrastructure, based on the study's results and needs. Choice of Hardware: Determine which hardware components are required for the system to function. RFID readers, fingerprint recognition, locks, and anything else that may be required.

The investigation reveals a notable risk in the RFID communication mechanism, principally stemming from the absence of encryption. In order to tackle this issue, we suggest using cryptographic protocols, with a particular emphasis on NXP's Mifare technology, including the DesFire and Ultralight C protocols. These protocols utilize sophisticated encryption techniques to ensure secure data transmission between the RFID tag and the reader. This encryption safeguards the tag's unique identifier (UID) and guarantees the integrity of the entire communication process. By implementing these protocols, we may significantly mitigate the possibility of illegal tag replication, a prevalent method of attack in RFID systems. This improvement brings our system up to date with the most recent developments in RFID security, guaranteeing a solid defence against eavesdropping and cloning.

Creation of Software: Develop the user interface, databases, and safety protocols to keep the system running smoothly.

To test, one must verify that the system's features meet the requirements. Levels of testing that may be included include unit testing, integration testing, and user acceptability testing. Deployment entails setting up the system in the structure, which entails installing both the software and the hardware elements and setting the system up to meet specific demands.

End users and system administrators need training on maximizing the system's potential while minimizing any potential risks to its security. Come up with a plan to keep the system running well by doing regular inspections, installing updates, and replacing worn-out components as needed.

In general, developing a high-security RFID-based fingerprint-building lock system involves a method that calls for a comprehensive approach, including study, requirements gathering, designing, hardware choosing, application development, testing, deployment, training, and maintenance. By sticking to this method, the completed system will provide the building with a solid and effective security measure [36].

The Uno board has 14 digital I/O pins, 6 of which may be used as pulse width modulation (PWM) outputs. In addition, it contains a USB port, a power connector, six analogue inputs, a reset button, and an In-Circuit Serial Programming header (ICSP). This makes it a flexible board that may serve in various contexts.

Among the Arduino Uno's [20] many advantages is its user-friendliness. Everything you need to get going is included, including a USB connection that can be used to connect to a computer; an AC-to-DC converter or a battery can power it. For this reason, it is an excellent choice for beginners who still need to become more knowledgeable about electronics and/or programming.

2) *Radio Frequency Identification Reader - MFRC522:* The Radio Frequency Identification (RFID) Reader MFRC522 is a popular component for building security systems that use RFID technology [37]. This reader can read and write data to RFID tags, which can be used to provide access control and authentication in an intelligent building security system.

The MFRC522 reader is easy to use and can connect to a microcontroller board like the Arduino Uno (R3). It operates at a frequency of 13.56 MHz and supports ISO/IEC 14443 Type A and B, MIFARE, and NTAG. To use the MFRC522 reader in a security system for intelligent buildings, it is necessary to connect the reader to the microcontroller [22] board and develop software applications that can manage the data received from the reader.

This includes data processing and authentication algorithms that can be used to validate the RFID tag and grant or deny access accordingly. You can use an RFID system to open a door. For example, only the person with the correct information on his card can enter. An RFID system uses:

One of the least-cost RFID choices is the RC522 RFID module based on NXP's MFRC522 IC, which can be purchased online for less than \$4. RFID card tags and key fob tags with 1KB of storage space are included in the standard package. Most notably, it can create a tag, meaning you may secretly use it to record a message [38].

An antenna and RF circuitry produce an electromagnetic field at high frequencies, making up a Reader. Nonetheless, the tag is often a battery-free passive device. As an alternative, it has a microprocessor to store and process data and an antenna for receiving and sending signals [29].

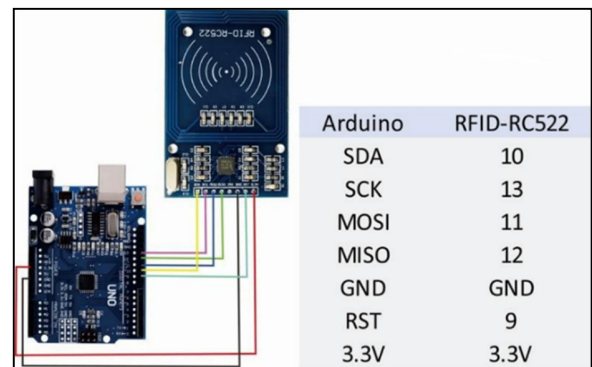


Fig. 2. Connection RFID sensor to Arduino Uno

The RFID reader's read tag data may be logged by downloading the "DumpInfo" script from the MFRC522 library to the Arduino IDE and then accessing the serial monitor.

To scan RFID tags and get their corresponding UIDs, the DumpInfo program talks to the RFID reader using the MFRC522 library. The data is subsequently sent in hexadecimal form to the serial monitor [39].

Putting an RFID tag close to the reader and watching the serial monitor for results is an easy way to test and ensure the operation of the RFID reader. If the reader detects and reads a tag, it will show the tag's unique identifier (UID).

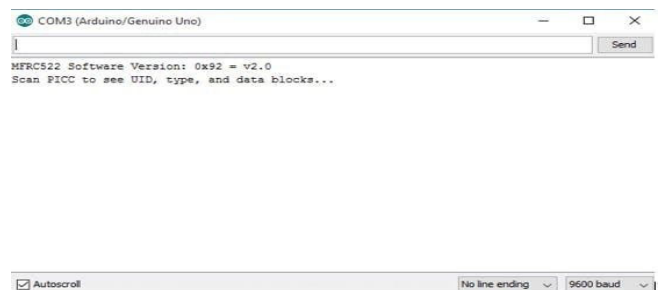


Fig. 3. Reading data from an RFID tag

Bring the RFID tag or keychain close to the reader. Put the tag and the reader together until all the data is visible.

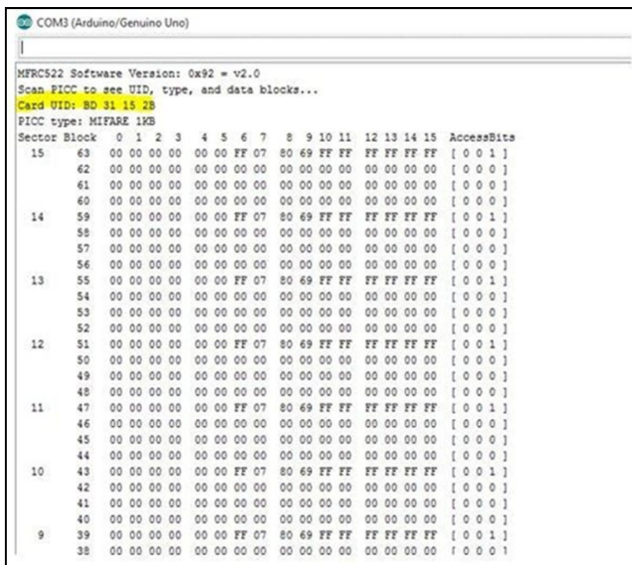


Fig. 4. RFID tag information displayed

The MFR522 RFID reader may read and authenticate RFID tabulate access using the accompanying Arduino code in an intelligent building security system. Code for the Arduino board may be uploaded, and then the RFID tag to which access should be granted can be approximated.

Using the MFR522 library, the code can exchange data with the RFID reader and verify the tag's legitimacy by matching its unique identifier (UID) with one already recorded. If the UIDs match, the program will allow access by turning on an LED on the Arduino board.

Code access requires input of the unique identifier (UID) of the RFID tag for which access is requested. It is possible to achieve this by adjusting the "uid" variable in the co.

You can go relatively close to the reader after you have uploaded the code and configured the UID number. The Arduino board's LED will light up if the UID number read from the tag is the same as the one kept in the database.

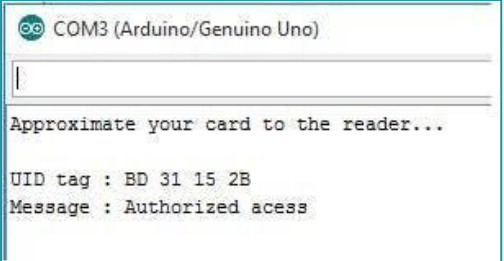


Fig. 5. Radio Frequency Identification tag code

Caption (optional). It is possible to trigger the refusal notice using a tag approximation with a UID that's not yours.

3) *Fingerprint Sensor Module (FPM10A)*: The FPM10A fingerprint sensor module must be wired to a microcontroller board such as an Arduino Uno (R3) using the pin configuration detailed in the module's datasheet. Create programs that can handle the data collected by the fingerprint sensor system [40]. This contains techniques for processing data

and authenticating users, which may be used to check whether a fingerprint is legitimate and then allow or restrict access. The fingerprint sensor module may be programmed with the necessary fingerprint templates using the SDK (software development kit). Scan the authorized users' fingerprints using the fingerprint sensor module and save the resultant templates in the system's database to enrol their fingerprints. A fingerprint sensor module will require users to put their finger on it before granting access to a restricted area. The fingerprint will be scanned by the module and compared to the system's database of template fingerprints [41].

If the fingerprint is that of a verified user, entry will be given. Access will be refused if the fingerprint does not match the system's database or the user is not in the database. When biometric authentication is needed for building security systems, the Fingerprint Sensor Module FPM10A is often employed. It requires a power source of less than 120mA and has a voltage input range of DC 3.6 to 6.0V, making it low-power and straightforward to combine with other electrical parts. The module uses the UART interface protocol at a lousy rate of 9600, and a green backlight is included for enhanced visibility. The module's safety rating of 5 (the maximum possible) indicates high protection. With a FAR of less than 0.001% and a FRR of less than 1.0%, it guarantees precise and trustworthy fingerprint identification. In addition, up to 127 unique fingerprints may be stored in the module, allowing a large number of legitimate users to be added to the database. The features of the Fingerprint Sensor Module FPM10A make it an excellent option for security systems that use biometric authentication.

C. *Creating a Smart Building RFID-Based Fingerprint Lock System*

Find the Fingerprint Sensor Module FPM10A's pinout in the product datasheet or with the help of your distributor.

Learn where the power connectors are. The module operates on a DC 3.6 to 6.0V supply, drawing less than 120mA of current. VCC and GND are conventional designations for the power connectors.

Determine the UART interface's pins. The UART in this module operates at 9600 baud. TX and RX refer to the transmitting and receiving signals on a universal asynchronous receiver transmitter (UART) interface [42].

Find the location of the fingerprint reader's pins. The FPM10A sensor's integrated CMOS image sensor takes the fingerprint picture. In most cases, SENSOR EN, SENSOR OUT, and SENSOR IN will identify the fingerprint sensor's input and output and enable pins.

Find the connectors for the backlight. As an added convenience, the FPM10A module glows green in the dark. Typically, LED+ and LED- indicate which pins should be used for the backlight.

Connect the module's pins to the appropriate microcontroller board pins, such as those on an Arduino Uno (R3), using the pin configuration detailed in the datasheet.

It is crucial to your building's security system to be familiar with the pinout of the Fingerprint Sensor Module FPM10A.

Module good operation and reliability may be ensured by following the pinout diagram and attaching the pins to your microcontroller board. The Figure below explains the sensor's six pins.

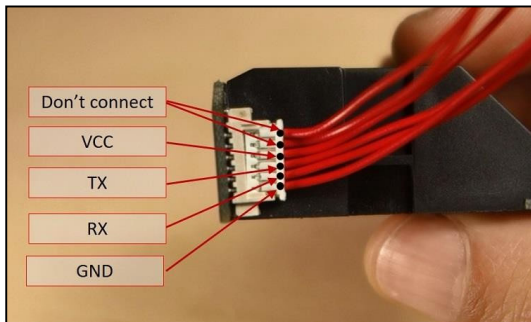


Fig. 6. Sensor pinout

IV. RESULTS

The best approach to operate the fingerprint sensor modules with the Arduino is by utilizing the Adafruit archive for this sensor. Follow the following procedures to download the library:

- 1) Click here to download the Adafruit Fingerprint Sensor library. You should have a .zip folder in your Downloads folder: <https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library>
- 2) Unzip the .zip folder, and you should get the Adafruit-Fingerprint-Sensor- Library-master folder
- 3) Rename your folder to "Adafruit_Fingerprint_Sensor_Library folder."
- 4) Wait for the library to install. You should see a message in the Arduino IDE indicating that the library has been successfully installed.
- 5) To test the installation, go to "File" -> "Examples" -> "Adafruit Fingerprint Sensor Library" -> "fingerprint" and upload the sketch to your Arduino board.
- 6) Open the serial monitor and set the baud rate to 9600. You should see the sensor initializing and prompting you to scan your finger.
- 7) Place your finger on the sensor and wait for the LED to turn green. The sensor will then output a message indicating it has detected your fingerprint.

Having the fingerprint sensor module wired to the Arduino, follow the next steps to enrol a new fingerprint. Make sure you have installed the Adafruit Fingerprint Sensor library previously.

- 1) Connect the fingerprint sensor module to your Arduino board according to the manufacturer's instructions.
- 2) Open the Arduino IDE and go to "File" -> "Examples" -> "Adafruit Fingerprint Sensor Library" -> "Enroll".
- 3) Upload the code to your Arduino board.
- 4) Open the serial monitor by clicking on the magnifying glass icon on the top right of the IDE window or by going to "Tools" -> "Serial Monitor". Make sure the baud rate is set to 9600.
- 5) In the serial monitor, you should see a message prompting you to enter an ID for the fingerprint. Type "1" (without quotes) and press enter.

- 6) The sensor will then prompt you to place your finger on the sensor. Place your finger on the sensor and wait for the LED to turn green.
- 7) Remove your finger from the sensor and repeat the process several times until the sensor has captured a good fingerprint image.
- 8) Once the sensor has successfully captured your fingerprint, you will see a message in the serial monitor indicating that the fingerprint has been enrolled.
- 9) To enrol additional fingerprints, repeat the process with a different ID number.

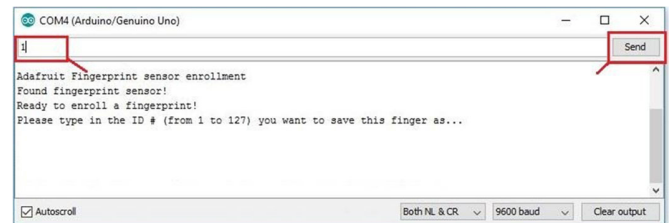


Fig. 7. Saving fingerprint

It is essential to have a thorough understanding of the module's pinout to properly connect it to the microcontroller board per the instructions provided by the manufacturer. When used with an Arduino board, the Adafruit Fingerprint Sensor Library offers a tried-and-true method of controlling the module. Pairing the fingerprint sensor modules to the Arduino board is the first step in enrolling a new fingerprint. Then, the "Enroll" code must be uploaded to the board, and finally, the user must follow the instructions shown on the serial monitor.

In order to recognize a fingerprint, the code for the fingerprint must first be stored on the Arduino board, and then the sensor must be instructed to take a scan of the user's finger. The serial display will show the appropriate ID instead of the fingerprint whenever a fingerprint is correctly matched. The confidence level is also shown; a higher number indicates a better approximation between the fingerprint that was supplied and the one that is already on file.

- 1) Place your finger on the scanner and follow the instructions on the serial monitor.

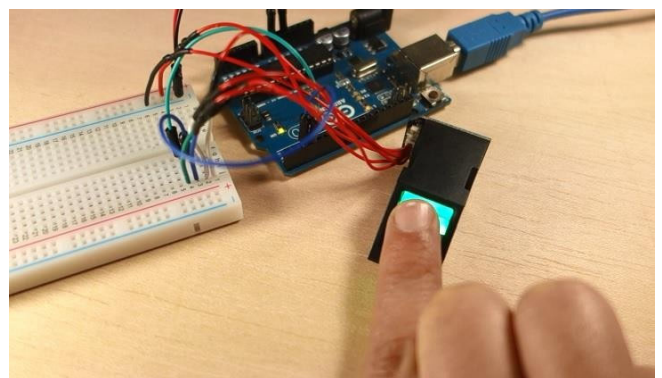
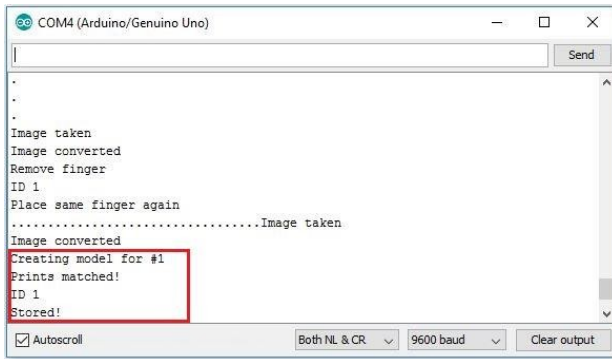


Fig. 8. Save the first fingerprint

After being instructed to scan the same finger twice, the fingerprint was successfully saved if you got the "Prints

matched!" notification. If not, try again and keep trying until you get it right.



```

COM4 (Arduino/Genuino Uno)
.
.
.
Image taken
Image converted
Remove finger
ID 1
Place same finger again
.....Image taken
Image converted
Creating model for #1
Prints matched!
ID 1
Stored!
Autoscroll Both NL & CR 9600 baud Clear output

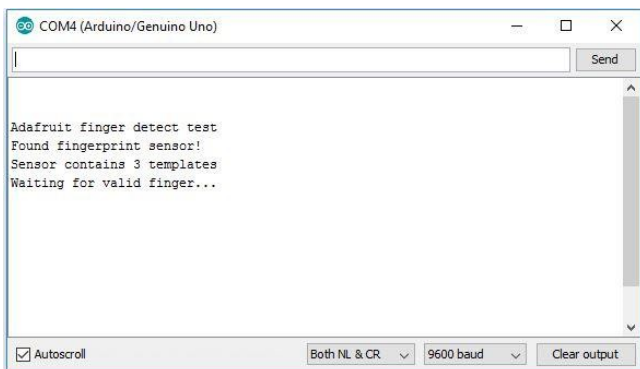
```

Fig. 9. Place finger for scanner

The module successfully captures the fingerprint picture and is then assigned a one-of-a-kind identification number. The same procedure may be used to enrol more than one fingerprint at a time [25].

Then, Open the Arduino IDE, go to file> Examples > Adafruit Fingerprint Sensor Library > Fingerprint, and upload the code to your Arduino board.

- 1) Open the Serial Monitor at a baud rate of 9600. You should see the following message:



```

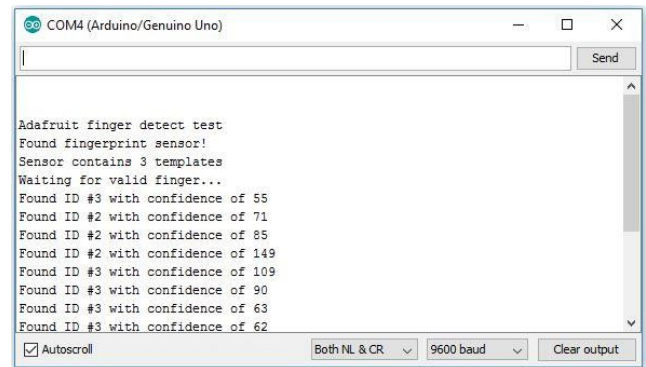
COM4 (Arduino/Genuino Uno)
Adafruit fingerprint detect test
Found fingerprint sensor!
Sensor contains 3 templates
Waiting for valid finger...
Autoscroll Both NL & CR 9600 baud Clear output

```

Fig. 10. Finding a match

In order to recognize a fingerprint, the code for the fingerprint must first be stored on the Arduino board, and then the sensor must be instructed to take a scan of the user's finger. The serial display will show the appropriate ID instead of the fingerprint whenever a fingerprint is correctly matched. The confidence level is also shown; a higher number indicates a better approximation between the fingerprint that was supplied and the one that is already on file.

- 2) Put the finger you want to identify on the scanner.
- 3) When a fingerprint is successfully matched, the corresponding ID appears on the serial display. The confidence level is also shown, with a more excellent value indicating a closer match between the submitted fingerprint and the one on file.



```

COM4 (Arduino/Genuino Uno)
Adafruit fingerprint detect test
Found fingerprint sensor!
Sensor contains 3 templates
Waiting for valid finger...
Found ID #3 with confidence of 55
Found ID #2 with confidence of 71
Found ID #2 with confidence of 85
Found ID #2 with confidence of 149
Found ID #3 with confidence of 109
Found ID #3 with confidence of 90
Found ID #3 with confidence of 63
Found ID #3 with confidence of 62
Autoscroll Both NL & CR 9600 baud Clear output

```

Fig. 11. ID matches the fingerprint

Connect the circuit:

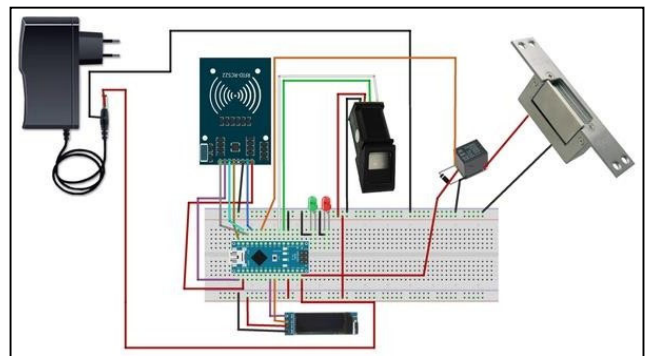


Fig. 12. Connect the circuit

At long last, the components of the system are assembled, and a test is performed. The RFID Door, Entry Control System, may manage access to a building by reading information from an RFID card or a fingerprint and comparing it to data already saved in the microcontroller. If the statistics are consistent, the LCD module will indicate that the door can be opened since it is unlocked. If the data do not match, the red light will blink, and the word "Rejected" will display to indicate that the input has been denied.

In conclusion, this paper presents a detailed walkthrough for assembling a Smart Building RFID-Based Fingerprint Lock System using the Fingerprint Sensor Module FPM10A. According to the findings, the component is dependable and accurate, and the system is efficient in managing entry to a facility and recording any suspicious activities. Further improvements to the system are possible by implementing further safety precautions and functions.

V. DISCUSSION

The article explores the application of RFID and fingerprint technologies to enhance security in smart buildings. Smart buildings with various IoT devices offer numerous benefits such as improved energy efficiency and convenience. However, they also present security challenges that need to be addressed to safeguard the privacy and safety of occupants. This paper proposes the integration of RFID and fingerprint technologies as potential solutions to enhance intelligent building security.

The discussion in the article highlights the benefits and challenges of implementing RFID and fingerprint technologies in intelligent buildings. RFID tags and readers can effectively manage access control systems, ensuring only authorized personnel can enter restricted areas [11], [18]. The article emphasizes that RFID technology enables real-time tracking of personnel and assets, thus enhancing overall security and efficiency within the building premises [9].

Integrating fingerprint technologies adds an extra layer of biometric security, offering a unique and reliable method for personal identification and access control [24]. Fingerprint technology's ability to provide high precision and accuracy in real-time tracking of personnel and assets is acknowledged [25], [26]. Combined with RFID technology, fingerprint-based access control systems can prevent unauthorized access to sensitive areas [12].

The paper also discusses potential challenges in implementing these technologies. Issues like data privacy and security are raised, emphasizing the need for robust encryption and authentication protocols to safeguard sensitive information [13], [16], [30]. Deploying RFID and fingerprint technologies in large-scale innovative building environments necessitates careful planning and consideration of potential interference and integration challenges [36], [37].

Another aspect addressed is the potential cost implications of implementing such security measures. RFID and fingerprint technologies often require upfront investments in hardware and infrastructure [38]. The long-term benefits, such as increased security and operational efficiency, are believed to outweigh the initial costs [35], [39].

The article highlights how the research community has actively explored and proposed innovative solutions to address the limitations and challenges of RFID and fingerprint technologies. Integrating AI and machine learning algorithms is suggested to enhance security and data analytics [1], [2]. Moreover, ongoing advancements in hardware and software are expected to improve the performance and applicability of these technologies [26], [39].

The article offers valuable insights into the potential of RFID and fingerprint technologies in enhancing security in intelligent buildings. The article draws from various reputable sources, contributing to the credibility and reliability of the proposed solutions. While there are challenges to address, the benefits of improved security, real-time tracking, and access control justify the continued exploration and adoption of these technologies in the rapidly evolving landscape of smart buildings. As technology advances, RFID and fingerprint technologies will likely play an increasingly important role in ensuring the safety and efficiency of smart buildings and the people within them.

VI. CONCLUSIONS

Increasing the level of safety in intelligent buildings may be accomplished exceptionally efficiently via technologies such as RFID and fingerprint scanning. The case study described in this article illustrates how using these technological solutions may lead to an increase in security and a reduction in the number of instances in which security has been compromised.

Nevertheless, employing these systems brings several difficulties that must be handled appropriately. These difficulties include the potential for false benefits and drawbacks, the expense of setting up and maintaining them, and issues around privacy.

It is necessary to do more study to investigate the possibilities these technologies have for improving the safety of intelligent buildings. This might entail the creation of more sophisticated authenticating algorithms, integrating such innovations with other innovative construction methods, and assessing their effectiveness in situations that are representative of the outside world. In the end, the use of technologies like RFID and fingerprint scanning provides a potential route toward creating safer and more secure intelligent buildings.

In addition, the study emphasizes the significance of ensuring that intelligent building security systems are connected to Wi-Fi networks. It makes it possible to integrate with other intelligent devices and systems, making it possible to exercise remote control over both security and non-security equipment. It is also emphasized that using sensors and cameras to monitor the premises and spot any odd activity, such as unlawful access or departure from confined spaces, is essential to smart building system security. For example, unauthorized access or exit from limited areas.

There are still certain obstacles that need to be overcome, in spite of the many benefits that may be gained by using RFID and fingerprint technology in intelligent building security systems. For example, there is always a danger that the sensors and other devices used in these systems may need to perform more effectively owing to manufacturing or setup difficulties. This decreases the system's dependability and increases the probability of false alarms or security breaches.

In conclusion, the evidence presented in this paper demonstrates that technologies such as RFID and fingerprint recognition may be applied successfully to improve the safety of intelligent buildings. It has presented a detailed analysis of the current state of the art in intelligent building security systems. Specifically, it has highlighted the advantages of remote control of security and non-security equipment, the usage of cameras and sensors, and the significance of Wi-Fi connection. The case study described in this article demonstrates that the use of these technologies may lead to enhanced security and a reduction in the number of instances when security has been breached. Incorporating technologies such as RFID and fingerprint scanning into intelligent building security systems has the potential to enhance the protection afforded to humans and the valuables inside buildings.

REFERENCE

- [1] K. H. Lam, W. M. To, and P. K. C. Lee: "Smart Building Management System (SBMS) for Commercial Buildings—Key Attributes and Usage Intentions from Building Professionals—Perspective", *Sustainability*, 15, (1), 2023, pp. 80
- [2] S. Marrapu, S. Satyanarayana, V. Arun Kumar, and J. D. S. K. Teja: "Smart home-based security system for door access control using smartphone", *International Journal of Engineering and Technology(UAE)*, 7, 2018, pp. 249-51
- [3] O. I. Yurii Khlaponin, Nameer Hashim Qasim, Hanna Krasovska, Kateryna Krasovska: 'Management Risks of Dependence on Key

- Employees: Identification of Personnel', in Editor (Ed.)^(Eds.): 'Book Management Risks of Dependence on Key Employees: Identification of Personnel' (CPITS, 2021, ed.), pp. 295-308
- [4] J. Khodadoust, M. A. Medina-Pérez, R. Monroy, A. M. Khodadoust, and S. S. Mirkamali: "A multi-biometric system based on the fusion of fingerprint, finger-vein, and finger-knuckle-print", *Expert Systems with Applications*, 176, 2021, pp. 114687
- [5] K. Bobkowska, K. Nagaty, and M. Przyborski: "Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault", *IET Image Processing*, 13, (13), 2019, pp. 2516-28
- [6] N. Hashim, A. Mohsim, R. Rafeeq, and V. Pyliavskiy: "New approach to the construction of multimedia test signals", *International Journal of Advanced Trends in Computer Science and Engineering*, 8, (6), 2019, pp. 3423-29
- [7] M. Talebkah, A. Sali, M. Marjani, M. Gordan, S. J. Hashim, and F. Z. Rokhani: "IoT and Big Data Applications in Smart Cities: Recent Advances, Challenges, and Critical Issues", *IEEE Access*, 9, 2021, pp. 55465-84
- [8] G. Song, F. Khan, and M. Yang: "Security assessment of process facilities – Intrusion modelling", *Process Safety and Environmental Protection*, 117, 2018, pp. 639-50
- [9] K. Chen, W. Lu, F. Xue, P. Tang, and L. H. Li: "Automatic building information model reconstruction in high-density urban areas: Augmenting multi-source data with architectural knowledge", *Automation in Construction*, 93, 2018, pp. 22-34
- [10] S. Liu, L. Guo, H. Webb, X. Ya, and X. Chang: "Internet of Things Monitoring System of Modern Eco-Agriculture Based on Cloud Computing", *IEEE Access*, 7, 2019, pp. 37050-58
- [11] L. A. Maglaras, K.-H. Kim, H. Janicke, M. A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras, and T. J. Cruz: "Cyber security of critical infrastructures", *ICT Express*, 4, (1), 2018, pp. 42-45
- [12] D. Celestine: "Smart Lock Systems: An Overview", *International Journal of Computer Applications*, 177, (37), 2020
- [13] M. Ahtsham, H. Y. Yan, and U. Ali: 'IoT Based Door Lock Surveillance System Using Cryptographic Algorithms', in Editor (Ed.)^(Eds.): 'Book IoT Based Door Lock Surveillance System Using Cryptographic Algorithms' (2019, ed.), pp. 448-53
- [14] L. Ma, C. W. Sham, C. Y. Lo, and X. Zhong: "An Effective Multi-Mode Iris Authentication System on a Microprocessor-FPGA Heterogeneous Platform With QC-LDPC Codes", *IEEE Access*, 9, 2021, pp. 163665-74
- [15] J. Chen, X. Pu, H. Guo, Q. Tang, L. Feng, X. Wang, and C. Hu: "A self-powered 2D barcode recognition system based on sliding mode triboelectric nanogenerator for personal identification", *Nano Energy*, 43, 2018, pp. 253-58
- [16] A.-R. Sadeghi: "Technical perspective: The real-world dilemma of security and privacy by design", *Commun. ACM*, 64, (10), 2021, pp. 84
- [17] C. Wen, X. Li, T. Zanotti, F. M. Puglisi, Y. Shi, F. Saiz, A. Antidormi, S. Roche, W. Zheng, X. Liang, J. Hu, S. Duhm, J. B. Roldan, T. Wu, V. Chen, E. Pop, B. Garrido, K. Zhu, F. Hui, and M. Lanza: "Advanced Data Encryption using 2D Materials", *Advanced Materials*, 33, (27), 2021, pp. 2100185
- [18] A. Jamal, R. A. A. Helmi, A. S. N. Syahirah, and M. A. Fatima: 'Blockchain-Based Identity Verification System', in Editor (Ed.)^(Eds.): 'Book Blockchain-Based Identity Verification System' (2019, ed.), pp. 253-57
- [19] G. Panchal, D. Samanta, and S. Barman: "Biometric-based cryptography for digital content protection without any key storage", *Multimedia Tools and Applications*, 78, (19), 2019, pp. 26979-7000
- [20] M. Vargas, F. Hoyos, and J. Candeló-Becerra: "Portable and Efficient Fingerprint Authentication System Based on a Microcontroller", *International Journal of Electrical and Computer Engineering (IJECE)*, 9, 2019, pp. 2346
- [21] R. Dwivedi, S. Dey, M. A. Sharma, and A. Goel: "A fingerprint-based crypto-biometric system for secure communication", *Journal of Ambient Intelligence and Humanized Computing*, 11, (4), 2020, pp. 1495-509
- [22] E. Ofoegbu, and O. Ogunmakinde: "A Microcontroller Based Building Automation System for real-time Sensing and Control", 2, 2014, pp. 275-80
- [23] S. Umbarkar, G. Rajput, S. Halder, P. Harmame, and S. Mendgudle: 'Keypad/Bluetooth/GSM Based Digital Door Lock Security System', in Editor (Ed.)^(Eds.): 'Book Keypad/Bluetooth/GSM Based Digital Door Lock Security System' (Atlantis Press, 2016, ed.), pp. 726-34
- [24] V. I. Ivanov, and J. S. Baras: "Authentication of Swipe Fingerprint Scanners", *IEEE Transactions on Information Forensics and Security*, 12, (9), 2017, pp. 2212-26
- [25] I. Bhardwaj, N. D. Londhe, and S. K. Kopparrapu: "Study of Imposter Attacks on Novel Fingerprint Dynamics Based Verification System", *IEEE Access*, 5, 2017, pp. 595-606
- [26] M. Faundez-Zanuy, and J. Fabregas: "Testing report of a fingerprint-based door-opening system", *IEEE Aerospace and Electronic Systems Magazine*, 20, (6), 2005, pp. 18-20
- [27] Z. Niu, W. Huang, and S. Zhu: "Online Identification of Mechanical Systems Using the Simplified Output Error Model", *IEEE Transactions on Industrial Electronics*, 70, (7), 2023, pp. 6653-62
- [28] N. A. Riza: "Low Image Contrast Detection in a Bright Light Interference HDR Scene Using Smart CAOS Camera", *IEEE Photonics Technology Letters*, 35, (6), 2023, pp. 321-24
- [29] S. Zhou, L. Guo, Z. Lu, X. Wen, and Z. Han: "Wi-Monitor: Daily Activity Monitoring Using Commodity Wi-Fi", *IEEE Internet of Things Journal*, 10, (2), 2023, pp. 1588-604
- [30] M. E.-S. M. Essa, A. M. El-safety, A. H. Omar, A. E. Fathi, A. S. A. E. Maref, J. V. W. Lotfy, and M. S. El-Sayed: "Reliable Integration of Neural Network and Internet of Things for Forecasting, Controlling, and Monitoring of Experimental Building Management System", *Sustainability*, 15, (3), 2023, pp. 2168
- [31] D. V. Linh, and V. V. Yem: "Key Generation Technique Based on Channel Characteristics for MIMO-OFDM Wireless Communication Systems", *IEEE Access*, 11, 2023, pp. 7309-19
- [32] M. V, and S. Patil: 'Smart Device for Ensuring Women Safety Using Android App' (2018), pp. 186-97
- [33] J. Mahesh, M. Bodhisatwa, and D. Somnath: "Investigating the impact of thresholding and thinning methods on the performance of partial fingerprint identification systems: a review", *Journal of Electronic Imaging*, 32, (1), 2023, pp. 010901
- [34] V. W. Lee, N. Twu, and I. Kymissis: "Micro-LED Technologies and Applications", *Information Display*, 32, (6), 2016, pp. 16-23
- [35] B. McDowall, and S. Mills: "Cloud-based services for electronic civil registration and vital statistics systems," *Journal of Health, Population and Nutrition*, 38, (1), 2019, pp. 24
- [36] C.-H. Ko: "RFID 3D location sensing algorithms", *Automation in Construction*, 19, (5), 2010, pp. 588-95
- [37] A. E. Oke, A. F. Kineber, O. Akindele, and D. Ekundayo: "Determining the stationary barriers to the implementation of radio frequency identification (RFID) technology in an emerging construction industry", *Journal of Engineering, Design and Technology*, ahead-of-print, (ahead-of-print), 2023
- [38] M. Noman, U. A. Haider, A. M. Hashmi, H. Ullah, A. I. Najam, and F. A. Tahir: "A Novel Design Methodology to Realize a Single Byte Chipless RFID Tag by Loading a Square Open-Loop Resonator With Micro-Metallic Cells," *IEEE Journal of Microwaves*, 3, (1), 2023, pp. 43-51
- [39] B. Wilezkiewicz, P. Jankowski-Mihulowicz, and M. Węglarski: 'Test Platform for Developing Processes of Autonomous Identification in RFID Systems with Proximity-Range Read/Write Devices', in Editor (Ed.)^(Eds.): 'Book Test Platform for Developing Processes of Autonomous Identification in RFID Systems with Proximity-Range Read/Write Devices' (2023, ed.), pp.
- [40] X. Lv: "Application of fingerprint image fuzzy edge recognition algorithm in criminal technology", 13, (1), 2023
- [41] L. Lin, J. Zhang, X. Gao, J. Shi, C. Chen, and N. Huang: "Power fingerprint identification based on the improved V-I trajectory with colour encoding and transferred CBAM-ResNet", *PLOS ONE*, 18, (2), 2023, pp. e0281482
- [42] K.-K. Duan, and S.-Y. Cao: "Emerging RFID technology in structural engineering – A review", *Structures*, 28, 2020, pp. 2404-14