Design and Implementation of an IoT-Integrated Smart Locker System utilizing Facial Recognition Technology

Abdulrahman A. Alzhrani
Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
aasalzahrani1@uj.edu.sa (corresponding author)

Mohammed Balfaqih
Department of Computer and Network Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
mabalfaqih@uj.edu.sa

Fadi Alsenani
Department of Computer and Network Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
1947642@uj.edu.sa

Mohemmed Alharthi
Department of Computer and Network Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
1948152@uj.edu.sa

Ali Alshehri
Department of Computer and Network Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
1947652@uj.edu.sa

Zain Balfagih
Computer Science Department, Effat Energy and Technology Research Center, Effat College of Engineering, Effat University, Jeddah P.O. Box 34689, Saudi Arabia
zbalfagih@effatuniversity.edu.sa

Received: 4 May 2024 | Revised: 25 May 2024 and 9 June 2024 | Accepted: 12 June 2024

 DOI: https://doi.org/10.48084/etasr.7737

ABSTRACT

The Internet of Things (IoT) has been widely employed in the development of smart locker systems over the last decade. However, some of these systems are based on authentication methods which lack flexibility. Such systems did not consider the possibility that an authentication method could be unavailable for different reasons, namely access card loss, camera or mice break, etc. Moreover, such systems do not consider dual-authentication methods that enhance security. This paper aims to develop a smart locker system that considers several authentication methods including dual authentication (phone number and One Time Password (OTP)), fingerprint, face recognition, and emergency code utilizing IoT technology. Dual authentication method is the considered base authentication method. The system has been fabricated and evaluated taking into account different scenarios including monitoring door status, ensuring access for authorized users, and denying access to unauthorized users.

Keywords-smart anti-theft system; security system; smart home; Internet of Things; face recognition

I. INTRODUCTION

Lack of security is a major challenge and concern worldwide. According to [1], a home burglary occurs every 13 s in the USA. It is reported also that 88% of the burglaries take place in residential areas while 76% of all crimes are property crimes. This reflects that the traditional home security tools are outdated and easily breakable. Nowadays, Internet of Things (IoT) technology has been involved in almost all life aspects [2-5]. Home security is one of these areas and there are many different gadgets available that may assist in monitoring a residence. Home security entails several systems involving locker systems, which hold significant importance by enhancing convenience for individuals and businesses. Traditional smart lockers are based on passcodes in which the property residents set one code for anyone who wants to unlock the door [6]. Although such systems guarantee security, it is possible to be threatened easily by voyeurism, or eavesdropping. In addition, most smart locker systems are based on only one authentication method, such as security code, voice recognition, fingerprint, or video recognition. This in turn could lead to violation ease or access difficulty, since such systems do not consider the possibility that the authentication method could be unavailable for different reasons (access card loss, camera or mice breaking, etc.). In addition, several systems proposed employing more than one authentication methods in the smart locker system in which the user can employ any of them to guarantee access. Nevertheless, these systems do not consider dual-authentication. This could lead to weak security since it is possible to threaten the locker easily by voyeurism or overhearing the access code [7-20]. Moreover, the possibility of leaving the door unlocked has not been taken into account in the existing systems.

Analyzing the literature on smart locker systems has led to the identification of two critical issues that are addressed in this research. First, the current smart locker systems exhibit a deficiency in flexibility, as they overlook the potential unavailability of the authentication method. Second, the existing systems do not incorporate dual-authentication methods. As an extension of our work in [21], this study aims to create an advanced smart locker system that incorporates multiple authentication methods. The system emphasizes the dual authentication method as the foundational mechanism to enhance locker security. The key contributions of this paper are summarized below:

- An IoT-Integrated smart locker system incorporating diverse authentication methods such as dual authentication (utilizing phone number and One Time Password (OTP)), fingerprint recognition, face recognition, and an emergency code. The system efficiently acquires and processes data related to door access attempts, encompassing phone and code numbers, face recognition, fingerprint recognition, and door status. Continuous monitoring of the door status, facilitated by a magnetic door sensor, ensures secure door locking and prevention of any unauthorized access attempts.
- The system achieves real-time monitoring in smart locker systems through the utilization of face recognition based on the YOLO.V3 algorithm, chosen for its rapid processing capabilities. User faces are captured from video frames, enabling the system to authenticate users and make informed decisions regarding door locking. These decisions are subsequently communicated to the application layer to update users on the door status and any detected unauthorized access attempts.
- The study conducts experiments that affirm the accurate functionality of the system through three distinct scenarios. These scenarios encompass successful monitoring of door status, the effective granting of access to authorized users, and the denial of access to unauthorized users.

II. RELATED WORK

This section discusses the most relevant works to the proposed smart locker system, highlights their limitations, and identifies any open issues. Authors in [7] developed a security system that combines the features of Radio Frequency Identification (RFID), Global System for Mobile Communication (GSM), and password authentication. A person is identified by their RFID tag and authenticated with a temporarily generated 4-digit code, with the system performing satisfactorily upon implementation. In [8], a novel smart home anti-theft system was introduced, which detects intruders using a CCTV camera, even without night vision capability or when the face is partially or fully hidden. This system identifies theft in real-time and sends notifications to the homeowner. Another system utilizing RFID tags and Arduino was developed in [9], where the RFID card reader detects and verifies user access by identifying the card's radio frequency and confirming its authenticity with a beeping sound, LCD display, and LED blinking. A sensor was integrated for nighttime door operation, and the project also includes face recognition technology and an SMS alert system to enhance security. A secured approach for an authentication system using fingerprint and iris recognition was proposed in [10]. Initially, users enroll their fingerprints and eye images, which were stored in a database. The authentication process involves presenting an ID card, entering a password, undergoing fingerprint authentication, and iris recognition. Successful matches provide access to the locker system, while non-matching images require starting the process again. In [11], a door security system was presented, featuring an Arduino controller and GSM for sending alert data. This system performs three main functions: alarm, reminder, and lock. The reminder function activates a buzzer alert when the door is improperly closed. The lock function operates automatically when the door is closed but not locked manually, and the alarm function triggers if the door is interrupted without proper access. A fingerprint-based door lock system was proposed in [12], offering customizable and versatile applications as a cost-effective alternative to existing systems. This system addresses secrecy, integrity, and authentication challenges within heterogeneous IoT and centralized gateways using encryption and blockchain technology to secure data. Blockchain ascertains security and privacy in IoT-based smart door locking systems, with

permissioned blockchain resolving scalability issues. Anonymity and privacy are maintained by storing the fingerprint of the digital asset instead of the asset itself, and cross-fault tolerance is used to create reliable and secure distributed systems. Simulation results show that this system achieves 97.2% efficiency for pilot security automation in railway engines. In the system presented in [13], the fingerprint reader scans the user's fingerprints and transmits the data to the microcontroller. If the provided identification is valid, the microcontroller grants access; otherwise, the process is halted, and an alert is immediately sent to the authorized user, notifying them of suspicious activity. The authorized user can then take necessary measures, such as locking their card, to prevent unauthorized access. When the user's fingerprint matches the stored identification, a password is sent to the registered user's mobile or email. The user can input this password for machine access. Successful password verification results in the unlocking of the building; otherwise, the system remains unchanged, and alerts are dispatched to the designated person's mobile number. Likewise, a robust secure locker system, as outlined in [14], leverages RFID, fingerprint, password, and GSM technology, making it suitable for deployment in banks, secure offices, and residences. This system ensures that only authorized individuals can access funds from the locker. Biometrics, including fingerprints, serve as a reliable method for identifying and verifying individuals. RFID, or Radio-Frequency Identification, operates by utilizing radio frequency transmissions to identify and track individuals or objects. Essentially, RFID constitutes an electronic means of exchanging data through radio frequency waves, offering a versatile solution for the identification, tracking, and detection of a wide array of objects.

A wireless control system has been introduced in [15] for home accessibility, specifically designed for authenticated individuals. Utilizing ZigBee-based wireless network and PCA-based image processing techniques, the security system ensures restricted access. The integration of ZigBee modules and an electromagnetic door lock module manages door accessibility. Face detection and recognition algorithms, along with a wireless interface, identify visitors and automatically send status alerts to the homeowner via GSM network. The system allows remote control through the owner's mobile phone via AT commands to GSM Modem or authentication through password-protected email. Visitors can be monitored, and door access can be controlled through active web pages. In [16], a comprehensive biometric-based authentication system was proposed for enhancing the security of safety lockers. Addressing the limitation of existing locker systems that rely solely on branch head and user keys, the proposed model incorporates biometric and password authentication. The key features include a two-level authentication process involving both the branch head and the user, ensuring secure individual authentication through biometrics, and restricting access to designated individuals for their respective safety lockers.

TABLE I. A SUMMARY OF THE MOST RELEVANT EXISTING SMART LOCKER SYSTEMS

Ref.	Easy installation	Communication technology	Flexibility of authentication entrance	High security	Reasonable cost	Number of data acquisitions
[9]	√	Cellular network	√	×	√	2
[12]	√	Cellular network	×	√	√	1
[16]	√	-	×	×	√	1
[17]	×	-	×	×	√	1
[22]	√	Cellular network	×	√	√	2
Proposed	√	Wi-Fi	√	√	√	4

A smart door locking system was developed in [17], featuring invisible touch sensors created from passive transducers adopting a simple DIY process involving hybrid geometry copper electrodes on cellulose paper. For enhanced security, the keypad is hidden under paper and spray paint, making it invisible, and the door can only be unlocked by someone who knows both the password and the specific location of each key. The system accurately identifies the correct password pattern without errors, making it suitable for security applications in homes, banks, automobiles, apartments, lockers, and cabinets. In a similar vein, the Intelligent Electronic Password-protected Locker (IEPL) was designed with unique, personalized security features [18]. The IEPL uses single electrode mode triboelectric nanogenerators as self-powered sensors to detect a person's input behavior and habits, providing an unreplicable security layer. The control panel of the IEPL is entirely concealed to boost security and, unlike traditional lockers, it allows for customizable key configurations. Furthermore, the IEPL surface is fingerprint-resistant, and user identification is achieved via the extraction performed through deep learning of the output voltage feature signal, adding an extra security layer.

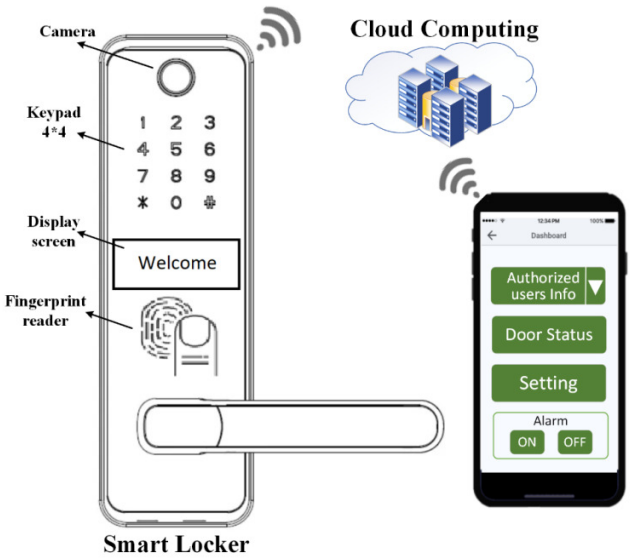

Fig. 1. Architecture of the proposed smart locker system.

It can be concluded that most of the existing systems employ single-factor authentication, so they do not offer a full security system. While many products have already addressed the difficulties with home security systems and suggested solutions, quite a few are based on face recognition, which has a great potential. One of the key factors that the community and smart home systems must consider is house security. The main disadvantages of the widely employed conventional home security systems are that they are mechanical, requiring the user to always use a key to access or close doors, which increases the likelihood of key loss or duplication. Using multiple-factor authentication can increase the security level and also gives the owner multiple ways to enter. Additionally, a lot of home security devices lack system control ease, so the proposed app gives the owner the ability to control the system easily. Table I summarizes the existing smart locker systems and compares them with the proposed system.

III. THE PROPOSED IOT-INTEGRATED SMART LOCKER SYSTEM UTILIZING FACIAL RECOGNITION TECHNOLOGY

This section describes the method followed in this research to achieve the research objectives. A detailed explanation of the proposed smart locker system architecture and sequence diagram is also presented. Figure 1 shows the architecture of the proposed system.

A. Architecture of Smart Locker System

The architecture of the smart locker system is composed of four main layers, which are acquisition, communication, processing, and application. Figure 2 depicts the main function of each layer in the proposed system. In the acquisition layer, the system employs a group of sensors to acquire data of the users that want to unlock the door. The sensors included in this layer are a Keypad 4*4 sensor, camera, fingerprint authentication sensor, and magnetic door sensor. In the communication layer, the acquired data are sent to the cloud using the cellular network for storage and further analysis. In the processing layer, the microcontroller and the cloud are employed for data processing and decision-making. The microcontroller will be utilized for face recognition from video frames, fingerprint reading, determining door status, door locking decision, and suspending access attempts. On the other hand, the cloud will be deployed for taking door unlock decisions according to the acquired sensor data, in addition to settings and stored data in it. These decisions are sent to the microcontroller to unlock the door, display messages in the locker display, and run the buzzer. Furthermore, the decisions are sent to the application layer (etc. application and website platforms) to notify the users about door status, and any unauthorized access attempts.

The sensors readings are sent to the microcontroller to obtain the data of door access attempts including entered phone and code numbers, recognized user's face, recognized user's fingerprint, and door status. The processes of face and fingerprint recognition are described in the next subsections. Figure 3 illustrates the workflow sequence diagram of the microcontroller. All these data are forwarded to the cloud for storing and further analysis if required. The predefined smart locker settings, such as emergency code and phone number list of authorized users, are sent from the application platform to the cloud. The latter monitors the door status continuously, through the readings of the magnetic door sensor, to ensure locking the door and preventing any unauthorized access attempt. For this purpose, the process "A" is conducted in which a timer will be set for two minutes upon door opening detection. When the two minutes elapse, a buzzer alarm will be turned on until the door is closed and locked. The microcontroller is always ready to perform any request sent from the cloud. Upon receiving the sensor data, the cloud will store them in the server for logging registration purpose and start the decision making process.

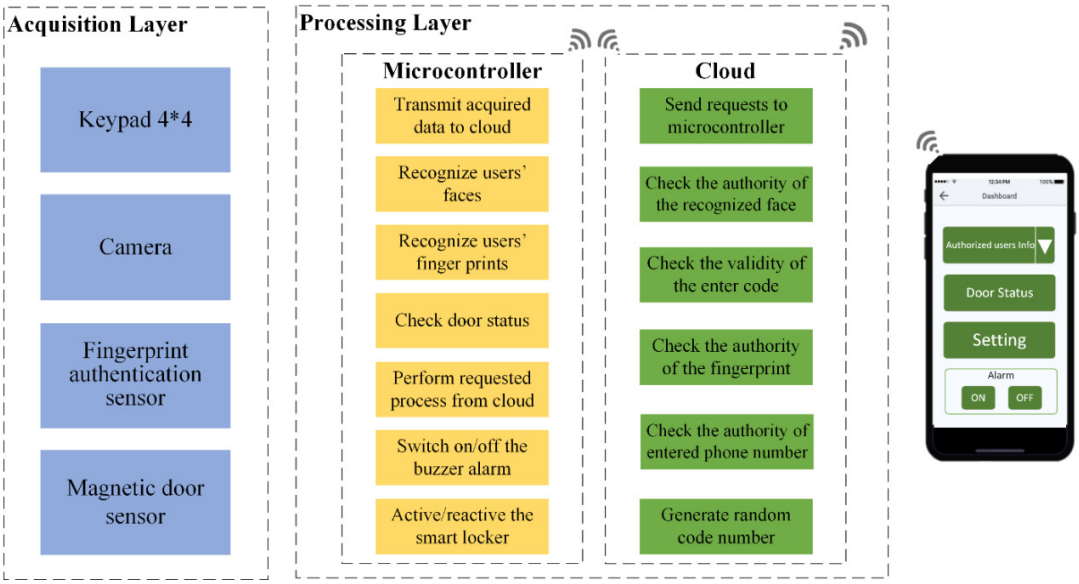

Fig. 2. The main function of each layer in the proposed smart locker system.

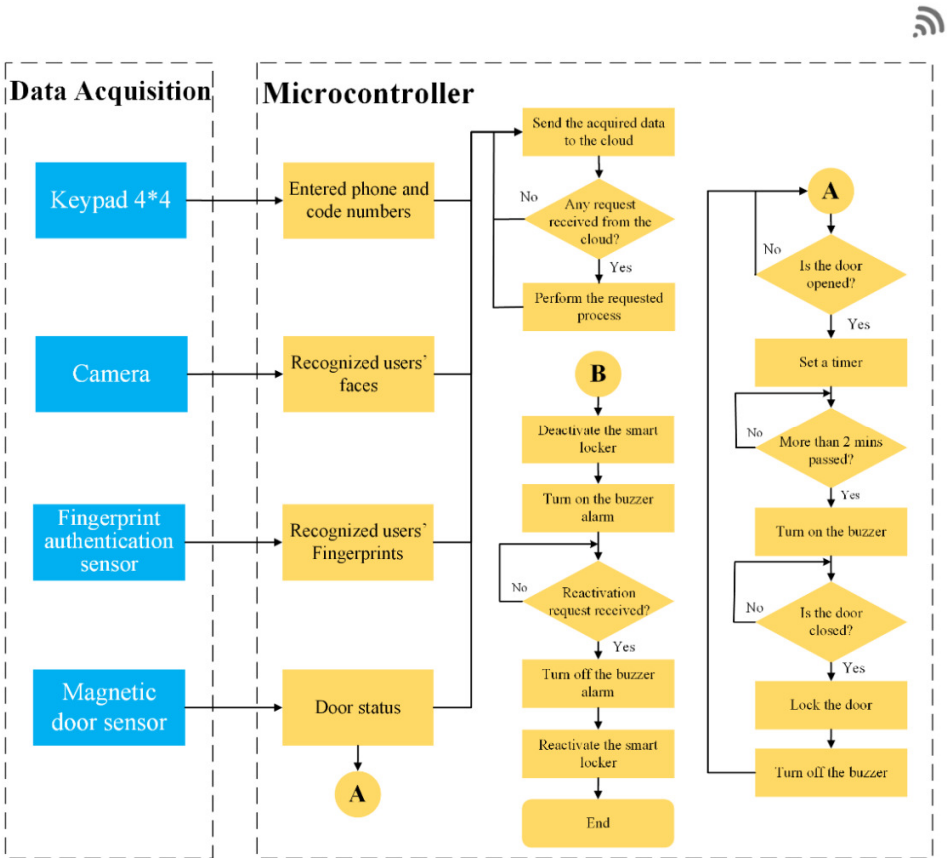

Fig. 3. Workflow sequence diagram of the microcontroller.

Figure 4 portrays the workflow sequence diagram in the cloud. Firstly, the cloud will check if any user face was recognized by the microcontroller and if the user has an access authorization. If the user is authorized, a request will be sent to the microcontroller to unlock the door. Otherwise, the cloud will check if the user entered an emergency code and if the entered emergency code is valid. If it is, a request will be sent to the microcontroller to unlock the door. The user will be given three attempts to enter the correct emergency code to alleviate the typo or keypad sensitivity issues. In each invalid attempt, a request will be sent to the controller to display the message "Please enter correct code number". If the user enters three invalid codes, the cloud will request the microcontroller to display the message "The entered code is incorrect", save the user face image in the logging for security purposes, and conduct the process "B" in which the microcontroller will deactivate the smart locker and run the buzzer. Moreover, the user will be notified about the unauthorized access attempt through the application platform where the user can reactivate the smart locker and request the microcontroller to turn off the alarm. If no emergency code is entered, the cloud will check if any fingerprint was read and its authorization. The door will be unlocked if the fingerprint is valid, and the user is authorized to unlock the door. Finally, if none of the previous access methods is attempted, the user will be requested to enter a phone number to check its authorization to unlock the door. If the phone number is authorized, the user will receive an one-time random code through an SMS message and will be asked to enter the code. To check the validity of the code, similar process to emergency code validity will be conducted in which the user will be given a maximum of three attempts to enter a valid code otherwise the smart locker will be deactivated.

B. Face Recognition

Efficient face recognition is crucial for real-time monitoring in smart locker systems. The proposed system utilizes the YOLO algorithm for its rapid processing capabilities. As previously discussed, YOLO is a single-shot detection algorithm that performs feature extraction and classification simultaneously [22]. It predicts four coordinates for each bounding box [2, 22]. The prediction value is positive if the bounding box overlaps a ground truth object more than any other bounding box. The prediction is disregarded if the box lacks the maximum intersection over union but overlaps a ground truth object beyond a certain threshold. YOLO.V3 employs a novel neural network for feature extraction, consisting of 53 convolutional layers, known as Darknet-53 [23]. Upon completing the classification, the fully connected layer is removed from Darknet-53. While there are initially 53 layers, YOLO.V3 expands to 106 layers during detection. Detection in YOLO.V3 occurs in three layers of Darknet-53 (82, 94, 106).

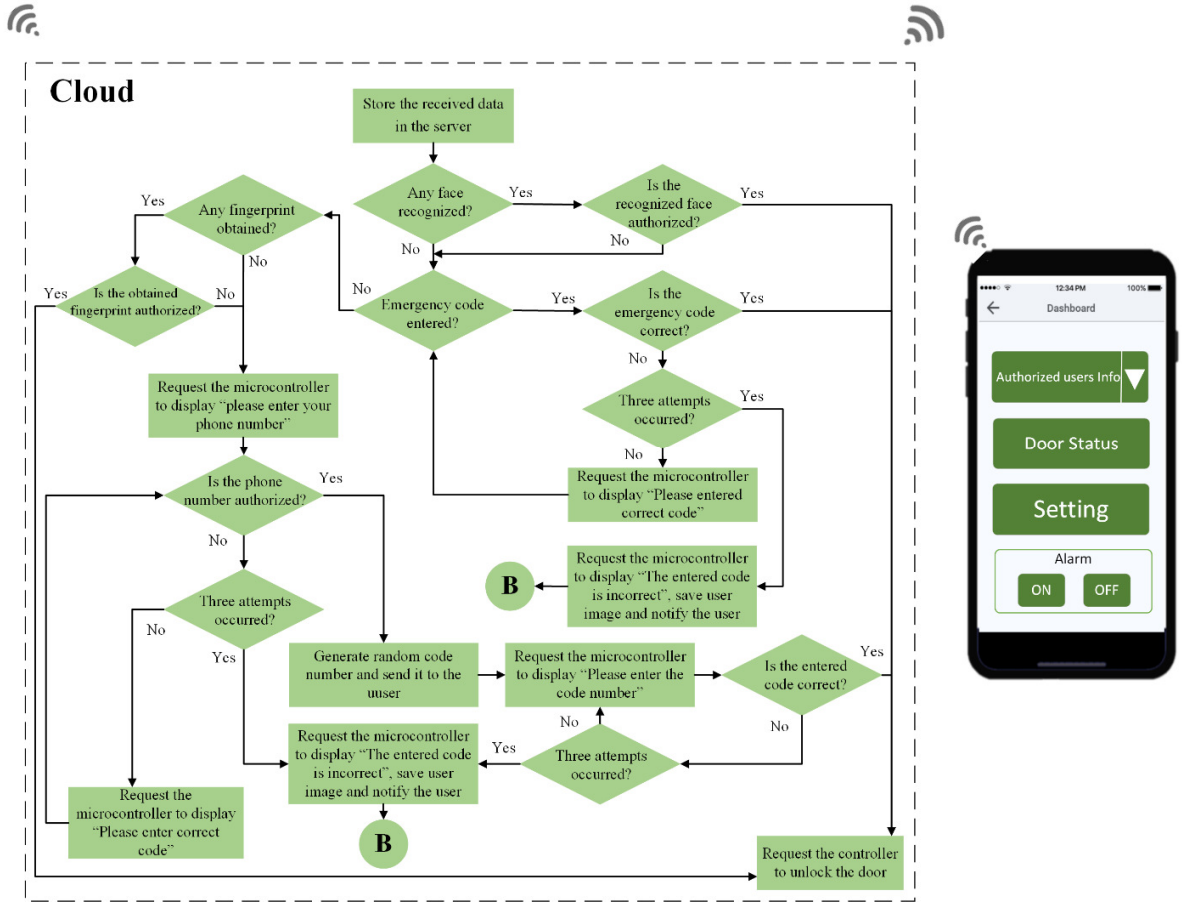

Fig. 4. The workflow sequence diagram in the cloud.

Facial attribute extraction involves the RAF, FER2013, and AFEW datasets. The FER2013 dataset comprises 28,709 training images, 3,589 validation images, and 3,589 testing images, providing ample data for training and evaluation. The RAF dataset, with 12,271 training samples and 3,068 testing samples, facilitates thorough facial attribute analysis. The AFEW dataset, used for dynamic temporal facial expressions, contains 957 samples across six expression classes. This dataset encompasses varied elements, including neutral expressions, natural head movements, occlusions, and diverse demographic traits, such as race, gender, and age, within cinematic settings.

C. Fingerprint Recognition

The developed system employs R307 fingerprint sensor for fingerprint recognition [24]. The R307 fingerprint sensor module, equipped with an optical sensor, efficiently captures and recognizes fingerprints implementing a robust algorithm for quick and accurate identification. With a capacity to store up to 1000 fingerprints in its internal memory, the sensor boasts a Universal Asynchronous Receiver/Transmitter (UART) interface, enabling seamless integration with microcontrollers supporting the UART communication protocol. The sensor operates through a two-step process involving enrollment and verification for fingerprint matching. During the enrollment, an individual's fingerprint is captured multiple times, converted into a secure digital template, and stored alongside their identity. Subsequent verification requires the individual to place his finger on the sensor, comparing the captured fingerprint to the stored template. Access is granted if a match is found and denied otherwise. The system's sensitivity is adjustable through threshold settings, allowing customization of the required similarity level for a match.

IV. SYSTEM IMPLEMENTATION AND RESULTS

The proposed smart locker system was fabricated and its performance was evaluated. Multiple electronic hardware devices are utilized to construct the proposed smart locker system. The Arduino UNO is selected to be employed as microcontroller due to its capability to support machine learning techniques. The additional components consist of a relay module, 16-key 4*4 type Keypad, optical fingerprint reader (R307 sensor), door magnetic sensor, MC-38 solenoid electric door locker, active buzzer, transducer, ESP32 Camera, ESP32 Development board, and DC power cable. KiCad software was deployed to draw the expected schematic and confirm the electrical rules check [25]. In addition, the Telegram bot is configured for the ESP32, interfacing with the Passive Infrared Sensor (PIR) motion sensor. Upon detecting motion, the ESP32 triggers a notification message to the associated Telegram account, alerting the user of the detected motion by sending corresponding notifications.

Figure 5 shows the circuit diagram of the hardware componentes of the system. The Arduino Uno establishes connections as follows: The GND input is linked with the blue wire to power various devices like the relay module, ESP32-camera, and the magnetic sensor. Additionally, an analog In connection using the yellow wire is established from A2 to the relay module. Power connections are made by the red wire from the 5V input to the relay module and the Espressif systems, including the female power supply input. Lastly, the white wire connects the -10 input to the GND input and the Espressif systems.

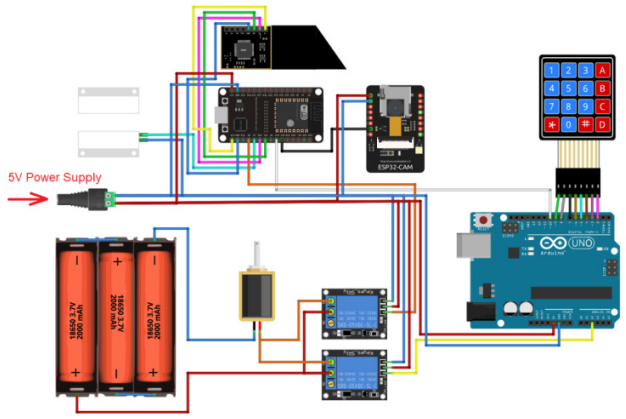

Fig. 5. Circuit diagram of the hardware components of the proposed smart locker system.

For the Espressif Systems ESP32: Various connections are established with multiple wires. The black wire links the 12 input to the 102 input in the ESP32 Cam, whereas the green wire connects the 18 input to the 102 input in the fingerprint. The pink wire connects the 5 input to the 102 input in the fingerprint. The light blue wire links the 17 input to the magnetic sensor, the orange wire connects the 16 input to the Relay Module inputs, the blue wire connects the D0 input to the 102 input in the fingerprint, and the yellow wire connects the CLK input to the 102 input in the fingerprint. The Keypad connects to the Arduino Uno using various colored wires: the pink wire connects to the 2 input, the purple wire to the -3 input, the dark brown wire to the 4 input, the light blue wire to the -5 input, the light brown wire to the -6 input, the black wire to the 7 input, the grey wire to the 8 input, and the green wire to the -9 input. Figure 6 displays the proof-of-concept set-up of the proposed smart locker system.

The performance of face recognition in YOLO was examined with FER2013 dataset. The training experiment demonstrated that the precision scores of standard YOLOv3 is 70.31%. The YOLOv3 experiment indicated that the YOLOv3 could detect many face instances in the images. Furthermore, a mAP was measured on the validation training data as represented in (1):

$$mAP = \sum_q^Q AveP(q) \Big/ q \quad (1)$$

(a)

(b)

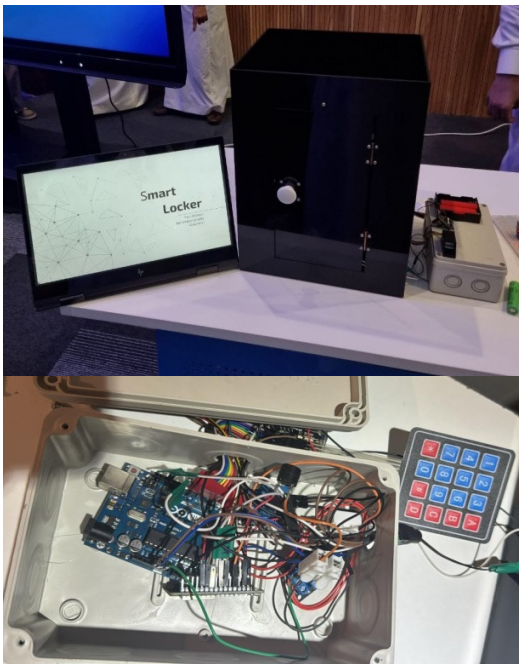

Fig. 6. Proof-of-concept set-up of the proposed smart locker system.

For the face detection task, the YOLOv3 model with the highest mAP@0.5 validation was 88.69 %. The loss of the model is less than 0.1 at 300 epochs. For the face detection-testing task, precision, mAP, and recall were also used to evaluate the performance of the trained model. The average precision is 0.904, while mAP and recall were 0.821 and 0.667, respectively. In the training and validation test, the overall recall was 70.31% with 88.69% mAP. Moreover, in the testing phase, the face recognition model achieved high precision and mAP scores of 0.718 and 0.822, respectively. Figure 7 provides an example of the face recognition processes.

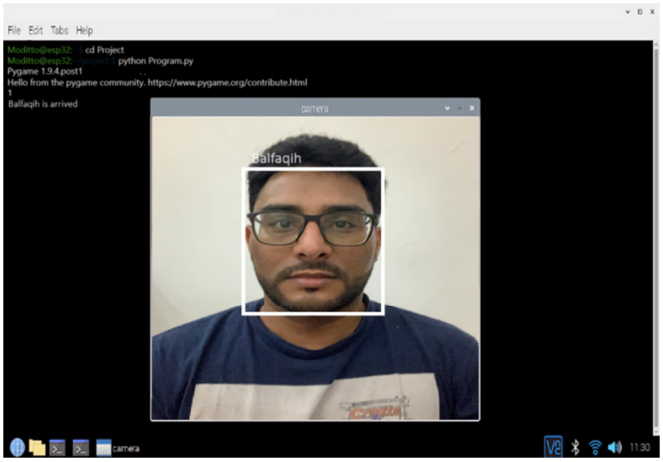

Fig. 7. An example of face recognition processes (author No. 2: Mohammed Bafaqih).

The proposed system was tested on three scenarios. The first scenario aims to validate the accurate monitoring of the door status, confirming that the system appropriately responds

to requests for door opening and closing. The test also includes verifying the reception of notification messages. For instance, upon door opening, a notification message is dispatched to the user via Telegram, as illustrated in Figure 8. The implemented system demonstrates that a notification is sent to the user when the door is opened. If the door remains open for two minutes, an alert is generated, notifying the user of the extended open duration with a message such as "Door Open – [Intruder Alert!!]". Lastly, a notification is dispatched upon successfully closing the door, indicating that the door is now closed.

The second scenario was designed to validate the effective granting of access to authorized users through various methods, including emergency code, face recognition, fingerprint recognition, or OTP. The objective was to ensure the accurate transition of the door status and the proper updating of events and logs. Figures 9 and 10 serve as examples illustrating the successful access granting to an authorized user through OTP and facial recognition, respectively. In the OTP process as evidenced in Figure 9, the user receives a four-digit code after entering his phone number. Upon entering the received code, the door opens, and a notification confirming the door opening is received. This demonstrates the seamless access authorization process using different authentication methods. In the facial recognition process, depicted in Figure 10, the door will automatically open upon detecting the face of an authorized user. Simultaneously, a notification message confirming the door's status as open is promptly sent to the user.

```
void loop() {
  readSensors();
  if (state == 0 && flag_door_state == 1 && flag_door_opened == 1) {
    flag_door_state = 0;
    flag_door_opened = 0;
    bot.sendMessage(chat_id_1, "Door Closed");
  }
  if (state == 0){
    flag_door_opened = 0;
    digitalWrite(buzzer, 0);
  }
  if (state == 1) {
    if(flag_door_opened == 0){
      flag_door_opened = 1;
      flag_door_state == 1
      opened_door_timer_start = millis();
    }
    if (flag_door_state == 1) {
      bot.sendMessage(chat_id_1, "Door Open");
      delay(5000);
      if(flag_door_open == 1 && ((millis() - opened_door_timer_start ) >= 120000))
      {
        bot.sendMessage(chat_id_1, "Door Open - [Introder Alert!!]");
        digitalWrite(buzzer, 1);
      }
    }
```

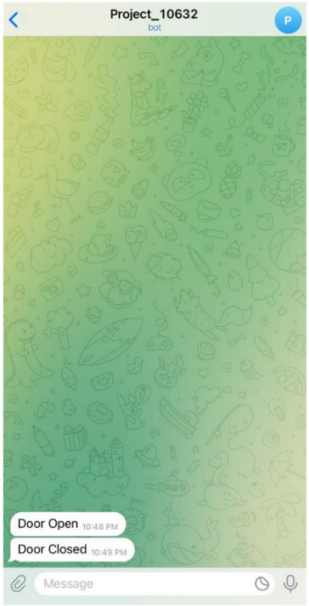

Fig. 8. Door status is detected, and a notification message is sent to the user.

```
p = face.faceSearch();
if (p == FACERECOGNITION_OK) {
  Serial.println("Found a face match!");
  digitalWrite(relay, 1);
  bot.sendMessage(chat_id_1, "Access Granted - [Facerecognied OK]");
  flag_door_state = 1;
  delay(5000);
  digitalWrite(relay, 0);
} else if (p == FACERECOGNITION_PACKETRECIEVEERR) {
  Serial.println("Communication error");
  return -1;
} else if (p == FACERECOGNITION_NOTFOUND) {
  Serial.println("Did not find a match");
  bot.sendMessage(chat_id_1, "Access Denied - [Face Not Found!!]");
  return -1;
} else {
  Serial.println("Unknown error");
  return -1;
}
```

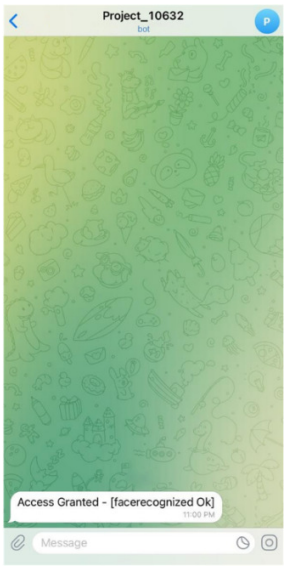

Fig. 9. An example of successful access granting to an authorized user by recognizing an authorized face.

```
lcd.setCursor(0,1);
lcd.print("Please enter your phone number");
phone_attempts = 0;
correct_code = false;
while(phone_attempts < 3)
{
  if(isPhoneAuthorised())
  {
    phone_attempts = phone_attempts + 1;
    random_code = random(1000,9999);
    bot.sendMessage(chat_id_2n  , random_code);
    code_attempts = 0;
    lcd.setCursor(0,1);
    lcd.print("Please enter the code number");
    while(!correct_code && attempts <3){
      code_attempts = code_attempts + 1;
      if(getCode() == random_code){
        bot.sendMessage(chat_id_1, "Access Granted - [Passcode OK]");
        correct_code = true;
    }
    if(!correct_code && code_attempts >= 3){
      lcd.setCursor(0,1);
      lcd.print("The entered code is not correct");
      captureImg(240,340);
    }
  }
}
```

Fig. 10. An example of successful access granted to an authorized user by OTP.

```
if (key) {
  Serial.println(key);
  if (key == '*') {
    input_password = "";  // reset the input password
  } else if (key == '#') {
    if (input_password == emergency_code) {
      Serial.println("The password is correct, unlocking the door in 20 seconds");
      digitalWrite(sendData,HIGH);
      Open();
      delay(5000);
      digitalWrite(sendData,LOW);
      Closee();
      attempts = 0;
      digitalWrite(buzzer, 0);
    } else {
      attempts = attempts + 1;
      Serial.println("The password is incorrect, try again");
      lcd.setCursor(0,1);
      lcd.print("Please enter correct code");
      digitalWrite(sendData,LOW);
      if (attempts >= 3)
      {
        lcd.setCursor(0,1);
        lcd.print("The entered code is incorrect");
        captureImg(320,240);
      }
```

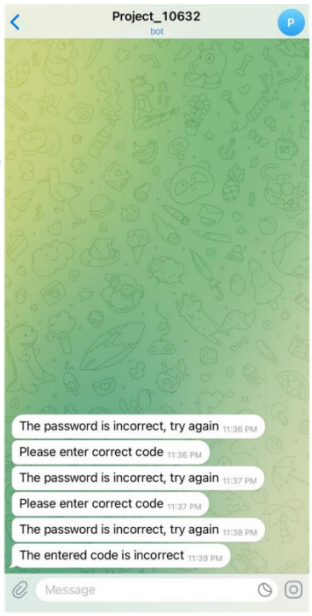

Fig. 11. An example of access denial to an unauthorized user due to incorrect emergency code.

The third scenario tests access denial to unauthorized users and sending related notification messages. Figures 11 and 12 show examples of access denial to an unauthorized user due to unrecognized fingerprint and incorrect emergency code. During the fingerprint recognition process, observed in Figure 11, access was denied since the recognized fingerprint was unauthorized. Consequently, a message was sent to the user indicating "Access Denied – [Fingerprint Not Found!!]". Similarly, the attempt to gain access using an emergency code was denied due to an incorrect password, as exhibited in Figure 12. In this scenario, the user received messages such as "The password is incorrect, try again" and "Please enter the correct code" for three or fewer attempts. If the user exceeded three attempts, a message stating "The entered code is incorrect" was relayed to the user.

```
p = finger.fingerSearch();
if (p == FINGERPRINT_OK) {
  Serial.println("Found a print match!");
  digitalWrite(relay, 1);
  bot.sendMessage(chat_id_1, "Access Granted - [Fingerprint OK]");
  flag_door_state = 1;
  delay(5000);
  digitalWrite(relay, 0);
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  Serial.println("Communication error");
  return -1;
} else if (p == FINGERPRINT_NOTFOUND) {
  Serial.println("Did not find a match");
  bot.sendMessage(chat_id_1, "Access Denied - [Fingerprint Not Found!!]");
  return -1;
} else {
  Serial.println("Unknown error");
  return -1;
}
```

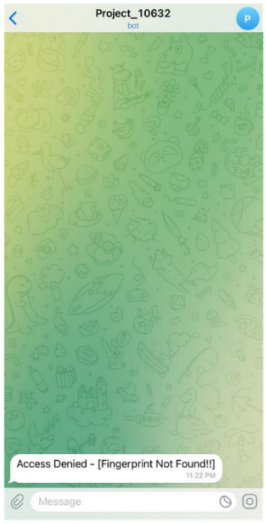

Fig. 12. An example of access denial to an unauthorized user due to unrecognized fingerprint.

V. CONCLUSIONS

This study addressed significant knowledge gaps in the design and implementation of smart locker systems, particularly concerning the limitations of existing single authentication methods. An IoT-integrated smart locker system was developed trough utilizing multiple authentication methods, including dual authentication (phone number and one-time password), fingerprint recognition, face recognition, and emergency codes. The present work stands out for its approach of emphasizing dual authentication as the foundational security mechanism, enhancing the system's robustness against potential security threats such as voyeurism and code interception. The functionalities of the proposed system were tested and validated through three scenarios including monitoring the door status, ensuring access for authorized users, and denying access to unauthorized users. The results of the system testing confirm that the system introduced effectively monitors door status, grants access to authorized users, and denies access to unauthorized users. These results underline the practical applicability of the proposed system in real-world settings.

ACKNOWLEDGMENT

This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. (UJ-23-DR-204). The authors, therefore, acknowledge and thank the University of Jedah for its technical and financial support.

REFERENCES

[1] "42 Home Burglary Statistics 2024 You Wish to Know Earlier." https://reolink.com/blog/home-burglary-crime-statistics/.

[2] M. Balfaqih, "A Hybrid Movies Recommendation System Based on Demographics and Facial Expression Analysis using Machine Learning," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 11, pp. 765–774, 2023, https://doi.org/10.14569/IJACSA.2023.0141177.

[3] A. A. Almohammedi, M. Balfaqih, S. Nahas, A. Bokhari, and A. Alqudsi, "Design and Implementation of IoT-Enabled Intelligent Fire Detection System Using Neural Networks," in *International Conference on AI and Mobile Services*, Hawaii, HI, USA, Sep. 2023, pp. 63–70, https://doi.org/10.1007/978-3-031-45140-9_6.

[4] M. Balfaqih, Z. Balfagih, M. D. Lytras, K. M. Alfawaz, A. A. Alshdadi, and E. Alsolami, "A Blockchain-Enabled IoT Logistics System for Efficient Tracking and Management of High-Price Shipments: A Resilient, Scalable and Sustainable Approach to Smart Cities," *Sustainability*, vol. 15, no. 18, Jan. 2023, Art. no. 13971, https://doi.org/10.3390/su151813971.

[5] M. Balfaqih, Z. Balfagih, A. A. Almohammedi, and K. M. Alfawaz, "A Smart and Privacy-Preserving Logistics System Based on IoT and Blockchain Technologies," in *1st International Conference on Advanced Innovations in Smart Cities*, Jeddah, Saudi Arabia, Jan. 2023, pp. 1–5, https://doi.org/10.1109/ICAISC56366.2023.10255090.

[6] A. Siswanto, A. Efendi, Z. Hasrin, and B. Arifin, "Two-Factor Authentication for Safe Deposit Box Based on Embedded System," in *International conference on smart computing and cyber security: strategic foresight, security challenges and innovation*, South Korea, Korea, Jun. 2021, pp. 194–206, https://doi.org/10.1007/978-981-16-9480-6_18.

[7] S. O. Anaza, J. D. Jiya, and Y. S. Haruna, "Development of a prototype RFID-GSM based lock system," *International Journal of Engineering Applied Sciences and Technology*, vol. 4, no. 12, pp. 77–84, Apr. 2020.

[8] S. Pandya *et al.*, "Smart Home Anti-Theft System: A Novel Approach for Near Real-Time Monitoring and Smart Home Security for Wellness Protocol," *Applied System Innovation*, vol. 1, no. 4, Dec. 2018, Art. no. 42, https://doi.org/10.3390/asi1040042.

[9] J. Guntur, S. S. Raju, T. Niranjan, S. K. Kilaru, R. Dronavalli, and N. S. S. Kumar, "IoT-Enhanced Smart Door Locking System with Security," *SN Computer Science*, vol. 4, no. 2, Feb. 2023, Art. no. 209, https://doi.org/10.1007/s42979-022-01641-9.

[10] D. S. Goud, I. Md, and P. J. Saritha, "A Secured Approach for Authentication system using fingerprint and iris.," *Global Journal of Advanced Engineering Technology*, vol. 3, 2012.

[11] M. S. M. Effendi, Z. Shayfull, M. S. Saad, S. M. Nasir, and A. H. B. Azmi, "A new invention of alarm reminder locking (ARL) security system," *International Journal of Engineering and Technology*, vol. 8, no. 1, pp. 465–472, 2016.

[12] K. Sujatha *et al.*, "Smart Door Locking System Using IoT—A Security for Railway Engine Pilots," in *Sentiment Analysis and Deep Learning*, S. Shakya, K.-L. Du, and K. Ntalianis, Eds. New York, NY, USA: Springer, 2023, pp. 263–271.

[13] M. S. Divya and M. N. Rao, "Centralized Authentication Smart Locking System using RFID, Fingerprint, Password and GSM," *International Journal of Engineering & Technology*, vol. 7, no. 3.12, pp. 516–520, Jul. 2018, https://doi.org/10.14419/ijet.v7i3.12.16170.

[14] H. S. Detroja, P. J. Vasoya, D. D. Kotadiya, and C. B. Bambhroliya, "GSM Based Bank Locker Security System using RFID, Password and Fingerprint Technology," *International Journal for Innovative Research in Science & Technology*, vol. 2, no. 11, pp. 110–115, 2016.

[15] M. Sahani, C. Nanda, A. K. Sahu, and B. Pattnaik, "Web-based online embedded door access control and home security system based on face recognition," in *International Conference on Circuits, Power and Computing Technologies*, Nagercoil, India, Mar. 2015, pp. 1–6, https://doi.org/10.1109/ICCPCT.2015.7159473.

[16] M. Q. Mehmood, M. S. Malik, M. H. Zulfiqar, M. A. Khan, M. Zubair, and Y. Massoud, "Invisible touch sensors-based smart and disposable door locking system for security applications," *Heliyon*, vol. 9, no. 2, Feb. 2023, Art. no. e13586, https://doi.org/10.1016/j.heliyon.2023.e13586.

[17] X. Huo *et al.*, "Intelligent electronic passworded locker with unique and personalized security barriers for home security," *Nano Research*, vol. 16, no. 5, pp. 7568–7574, May 2023, https://doi.org/10.1007/s12274-022-5321-3.

[18] S. Sridharan, "Authenticated secure bio-metric based access to the bank safety lockers," in *International Conference on Information Communication and Embedded Systems*, Chennai, India, Feb. 2014, pp. 1–7, https://doi.org/10.1109/ICICES.2014.7034063.

[19] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, Apr. 2020, https://doi.org/10.48084/etasr.3394.

[20] V. Tiwari, A. Keskar, and N. C. Shivaprakash, "Design of an IoT Enabled Local Network Based Home Monitoring System with a Priority Scheme," *Engineering, Technology & Applied Science Research*, vol. 7, no. 2, pp. 1464–1472, Apr. 2017, https://doi.org/10.48084/etasr.1033.

[21] M. Balfaqih, "Enhancing Security and Flexibility in Smart Locker Systems: A Multi-Authentication Approach with IoT Integration," in *21st Learning and Technology Conference*, Jeddah, Saudi Arabia, Jan. 2024, pp. 325–329, https://doi.org/10.1109/LT60077.2024.10469610.

[22] C. Jiang *et al.*, "Object detection from UAV thermal infrared images and videos using YOLO models," *International Journal of Applied Earth Observation and Geoinformation*, vol. 112, Aug. 2022, Art. no. 102912, https://doi.org/10.1016/j.jag.2022.102912.

[23] Y. Rahayu, L. Afif, and P. J. Soh, "Design and development of smart lock system based QR-Code for library locker at Faculty of Engineering, Universitas Riau," *SINERGI*, vol. 26, no. 3, pp. 379–384, Oct. 2022, https://doi.org/10.22441/sinergi.2022.3.013.

[24] Rajguru Electronics, "R307 Fingerprint Module." https://www.rajguruelectronics.com/Product/1276/R307%20Fingerprint%20Module.pdf.

[25] T. Ahmad, U. Morelli, S. Ranise, and N. Zannone, "Extending access control in AWS IoT through event-driven functions: an experimental evaluation using a smart lock system," *International Journal of Information Security*, vol. 21, no. 2, pp. 379–408, Apr. 2022, https://doi.org/10.1007/s10207-021-00558-3.