Baghdad Science Journal

Volume 23 | Issue 1 Article 25

1-14-2026

Developing Campus Accurate Access Control System Using Network Facilities and Internet Services

Najmadin Wahid Boskany
Department of Computer, College of Science, University of Sulaimani, Sulaimani, Iraq, najm.wahid@univsul.edu.iq

How to Cite this Article

Boskany, Najmadin Wahid (2026) "Developing Campus Accurate Access Control System Using Network Facilities and Internet Services," *Baghdad Science Journal*: Vol. 23: Iss. 1, Article 25.
DOI: https://doi.org/10.21123/2411-7986.5187

Scan the QR to view the full-text article on the journal website

RESEARCH ARTICLE

Developing Campus Accurate Access Control System Using Network Facilities and Internet Services

Najmadin Wahid Boskany

Department of Computer, College of Science, University of Sulaimani, Sulaimani, Iraq

ABSTRACT

With the fast innovation and transformation that happen in our lives, security systems play an essential role in guaranteeing our safety and have become important part of protecting assets, houses, and campuses. The potential for theft and intrusions is increasing every day, making efficient access control for visitors coming in and out of facilities more critical. This paper focuses on developing an accurate access control system for special campus entrance doors with sensitive missions. The proposed system controls the entry of individuals to the campus by permitting authorized persons to enter while denying unauthenticated persons and notifying security guards via the GSM network. The system mainly consists of two Arduino microcontrollers connected to sensors that control security. Network facilities (GSM and Wi-Fi) as well as Internet services (website and Telegram bot) are integrated into the system to exchange information and save visitor information within the system. Arduino boards serve as activity centers to receive visitors' input (fingerprint codes, photos from cameras, position data from ultrasonic sensors), which are then analyzed and processed to accept or reject visitors. Finally, the system sends output to connected servers (Telegram bot, MySQL database, webserver). After testing the proposed system many times, results indicate that better authentication performance can be achieved with average time of only 8 seconds. The multi-channel communication used by this system makes it far more capable than others do while also improving security through two-factor authentication to verify a visitor's identity. However, one of the aforementioned channels requires 24/7 Internet services.

Keywords: Access control, Arduino microcontroller, GSM shield, Multi-factor security, Network facility

Introduction

Security is a very important and beneficial aspect of our lives, especially given the daily increase in widespread crime. People are compelled to use different types of security systems, but unfortunately, some of them are expensive and have limited capability in protection.[1] Various security control mechanisms have been developed over the years to prevent unauthorized access to sensitive assets. The primary reason for locking our structures (such as homes, offices, schools, and campuses) is to ensure the safety of our lives. Today, security and safety are becoming increasingly popular, and they are improving and being used for our convenience. The security systems are separated into two types: one that used a traditional system and the other that employed an electronic automated identification system.[2] Physical access control for any organization is a critical daily activity, as the safety and proper execution of events taking place there often depend on it. Many residential areas, offices, and campuses still rely on manual security systems with guard services, which can be expensive and time-consuming when it comes to identifying and permitting entry. Misunderstandings can also occur among owners, guards, and visitors. On the other hand, traditional access control techniques like ID cards may encounter issues such as phishing, theft,

Received 26 March 2024; revised 6 October 2024; accepted 8 October 2024.
Available online 14 January 2026

E-mail address: najm.wahid@univsul.edu.iq (N. W. Boskany).

https://doi.org/10.21123/2411-7986.5187

and intrusion. However, the emergence of new access control systems—such as those based on fingerprint and image processing, known for being easy-to-use, inexpensive, reliable, and powerful—are enabling the implementation of robust security systems and for discriminating attacks at the early stage. These systems offer significant advantages over legacy control systems in presenting and proving the identity.[3,4] A person's knowledge, most often a code such as a PIN or a password, and a method of ownership, such as a token - can be used to prove identity. For example, an NFC tag, an RFID card, or biometric methods like fingerprint, iris, or retina scans.[5] Arduino microcontroller technology is a prudent choice for designing and implementing the aforementioned system.

In general, any organization can use Arduino technology to control the security easily and flexibly and activities of its employees within their buildings.[6] Arduino board designs incorporate a variety of microprocessors and controllers, equipped with sets of digital and analog input/output pins that can connect to various expansion shields, breadboards, and other circuits. Arduino-based access control offers several advantageous features on an inexpensive embedded hardware platform. It consumes less power, is easy to operate, and simple to install compared to other existing access control and intrusion detection systems.[7] For the proposed system, the Arduino microcontroller is a highly suitable option because it can effectively achieve the goal of controlling access.

This study aims to design and implement a reliable, easy-to-use, and inexpensive Arduino-based security system for controlling access at a specific campus entrance door. Furthermore, it aims to restructure authentication process for users by designing and implementing an automated system. To apply this, many tools, devices and sensors are required: Arduino microcontrollers (linked with a GSM shield) used as the central units, along with different sensors such as fingerprint scanner, an ultrasonic sensor, buzzer, ESP32CAM security camera, LCD display, keypad, and servo motors. By integrating abovementioned features, the proposed system, introduces reliable security solution. The working processes of system is described as follows:

The Passive Infrared Sensor (PIR) motion sensor detects movement in its vicinity. Ultrasonic sensors accurately measure distances, ensuring detection of individuals approaching the campus entrance door. Fingerprint scanner used to provide secure and controlled access by verifying the identity of authorized visitor before granting entry. Servomotors in turn facilitate automated door operation (i.e.; automatically open the door) and camera positioning, ensuring controlled access for authorized individuals. For additional security, the system uses the ESP32CAM module captures visitor's photo in order to be used in future. The system depends on GSM shield to sends SMS alerts to security guards upon detecting intruders. Integration with Telegram bot, database, and web servers enable data storage and archiving of visitor information. All microcontrollers and sensors powered by a 12V battery connected to a voltage regulator module to ensure smooth operation. This comprehensive setup offers the following contributions:

1- Providing real-time access control solution at the campus entrance.
2- Providing enhanced and expedited authentication processes.
3- Implementing multi-factor security system for heightened protection.
4- Creation of an accurate access control system capable of communicating with security guards via mobile devices when necessary.

The system design is illustrated by the block diagram in Fig. 1.

The remainder of the paper is organized as follows: the next section is dedicated to related works. Following that, the design of the proposed system is described, and then the implementation phase is presented. A flowchart of the proposed system is provided. Before the final section, test results, discussion, and comparison of findings are presented. Finally, the last section is devoted to summarize the main conclusions of the paper.

Related works

This section provides a survey of recent advancements in access control solutions for building and campus doors. Various ideas and techniques are explored, ranging from ID card access control and voice recognition to fingerprint and image processing. Marpaung designed a door security system that allows monitoring and providing early intruder warnings via smart devices. Then the system was developed in some stages involving creation of software and hardware. It successfully implements room security and monitoring, enabling door lock access via a smartphone application.[8] However, the system has limitations in communication with outside the building. Bastari and Wibowo have designed a system for automatic door opening by using voice recognition. Their work was conducted in three phases: prototyping design, implementation, and testing.[9] The system's strength lies in its use of voice recognition, though it is limited by networking and

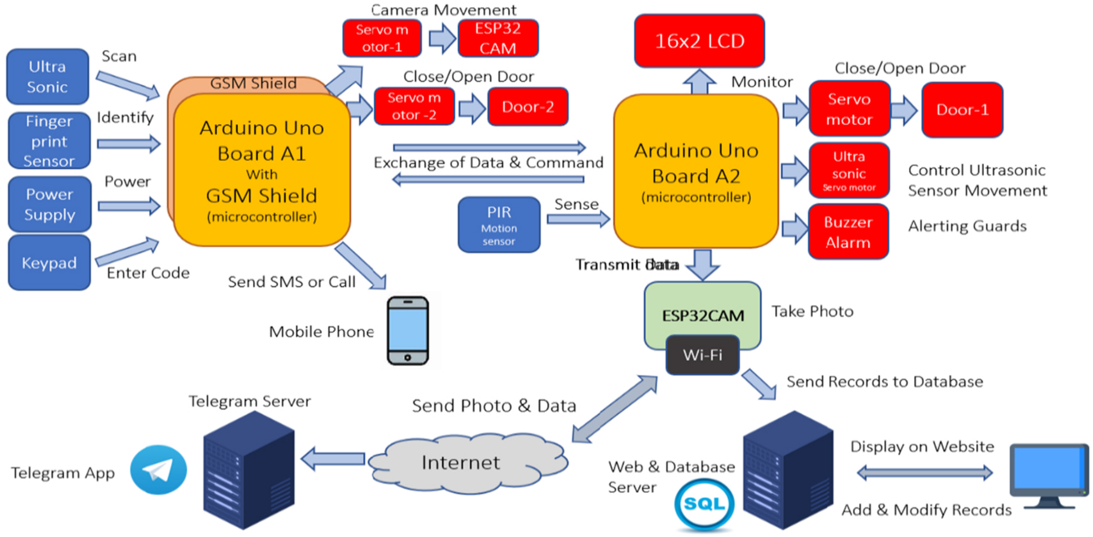

Fig. 1. Block diagram of the proposed system.

communication infrastructure. Communication also plays an important role in security entries. Galina et al. presented a prototype system for controlling gates and garage doors using an Android smartphone application. The system utilizes HC-05 Bluetooth communication to send signals from the smartphone to an Arduino Uno microcontroller, with a micro servo acting as a door locking mechanism. A buzzer used to notify homeowners if the gate or garage door remains open for over 15 seconds. This prototype effectively controls gates and garage doors with an average connection time of approximately 5 seconds. While the system has limitation and lacks data storage capabilities, it offers a viable alternative to enhancing home security systems.[10]

Rajamohan et al. utilized security by using an Arduino-based system for unlocking a door in real-time to avoid illegal and unauthorized access. The hardware and software of the system are designed to be suitable for real-time practical conditions.[11] In designing security systems, especially for access control, two-factor security provides increased assurance in restricting access. Yiru et al. designed a two-factor authentication protocol to verify user identity and enhanced the Attribute-Based Access Control (ABAC) model tailored for smart campuses. They plan to incorporate log records into future iterations of the system.[12]

Design of proposed access control system for special campus

This section is dedicated to present the design of the proposed system for controlling access to a specific campus entrance door using Arduino microcontroller as the foundational platform for various sensors and devices. The system consists of three main components: hardware, software, and network facilities. The roles of each component are described in the following subsections. The circuit diagram of the proposed system, designed using Fritzing[13] application is shown in Fig. 2.

System hardware

The core of the system revolves around the connection between two Arduino Uno microcontroller boards, which manage all operations of the electronic circuits connected to their digital input and output pins. These microcontrollers' process data input from two connected ultrasonic sensors, a fingerprint sensor, and an ESP32CAM. Additionally, they can send alert SMS messages to the security department via a GSM shield when necessary.

Moreover, the system transmits user data (ID code, photo, and information) to connected servers using various network facilities such as Wi-Fi and Internet services like Telegram and websites. The entire system can be integrated and mounted above the campus entrance door as a unified package. The specifications of the main hardware units are detailed as follows:

- **Arduino microcontroller**

Arduino is an open-source electronics platform known for its user-friendly software and hardware capabilities.[5] Arduino boards can interpret inputs such as light from a sensor, a button press, or a Twitter message, and convert them into outputs like activating a motor, illuminating an LED, or publishing

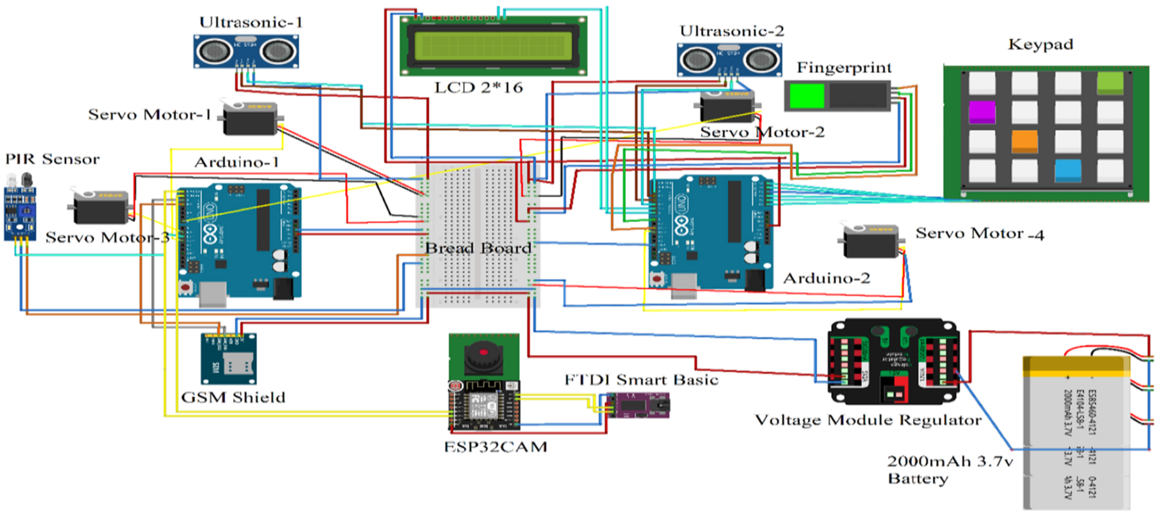

Fig. 2. Circuit diagram of the proposed system.

content online. In the proposed system, both Arduino boards serve as the central control units, coordinating all connected components.

- **GSM shield**

The Global System for Mobile Communications (GSM) is the most common standard for mobile telephone networks. The GSM shield by Arduino enables sending and receiving SMS messages, as well as making and receiving phone calls using a SIM card.[14] In this study, the GSM shield used for notifying the guard's mobile phone by sending SMS messages via the GSM network.

- **Ultrasonic sensor**

Ultrasonic sensor is one of the famous low-cost sensors. It measures distances ranging from 2 to 400 cm. It depends on ultrasonic sound waves that are sent by an electronic device to determine the distance of the object, and the reflected sound is converted into an electronic signal.[15] In this study, two ultrasonic sensors are utilized to scan and detect any person within their coverage area.[6] These sensors are positioned on both sides of the door. When the ultrasonic sensor on the right side detects an object, it reads the position value of its servo motor. If this value exceeds 90^{o}, the attached ESP32CAM camera adjusts its direction to the right to capture photos of the person. This technique is important because solely facing forward may result in missed targets. In the proposed system, the camera can be oriented in three positions: right, left, and forward.

- **ESP32CAM**

This device is an advanced microcontroller integrated with Wi-Fi, Bluetooth, and a camera. It will be used for surveillance monitoring around the buildings. The device can be programmed using the Arduino IDE to send alerts and notifications to the user's smartphone in the event of suspicious activity.[16] In the proposed system, it is utilized for capturing visitor photos for security purposes.

- **Fingerprint sensor**

The fingerprint sensor is a device that scans and saves fingerprint data in order to compare it later with other fingerprint data. It is a key technology for privacy and security. This sensor is suitable for projects that require security systems or entry systems for a location or specific database.[17] In the proposed system, it is employed to control visitor access. The system Administrator uses a keypad to enter authorized people's codes into the system, which are then linked to the MySQL.

- **Server computer (MySQL database and Web site) and Telegram bot**

The connected servers for MySQL database, website, and Telegram bot are utilized to save, archive, and present visitors' data and photos.

System software

Operating and controlling the aforementioned hardware units involves the use of various software, libraries, codes, and applications. The open-source Arduino IDE (Integrated Development Environment) is used for programming the two microcontrollers. Data transfer between the Arduino boards employs two common protocols: serial communication and I2C (Inter-Integrated Circuit) communication. I2C facilitates communication between integrated circuits

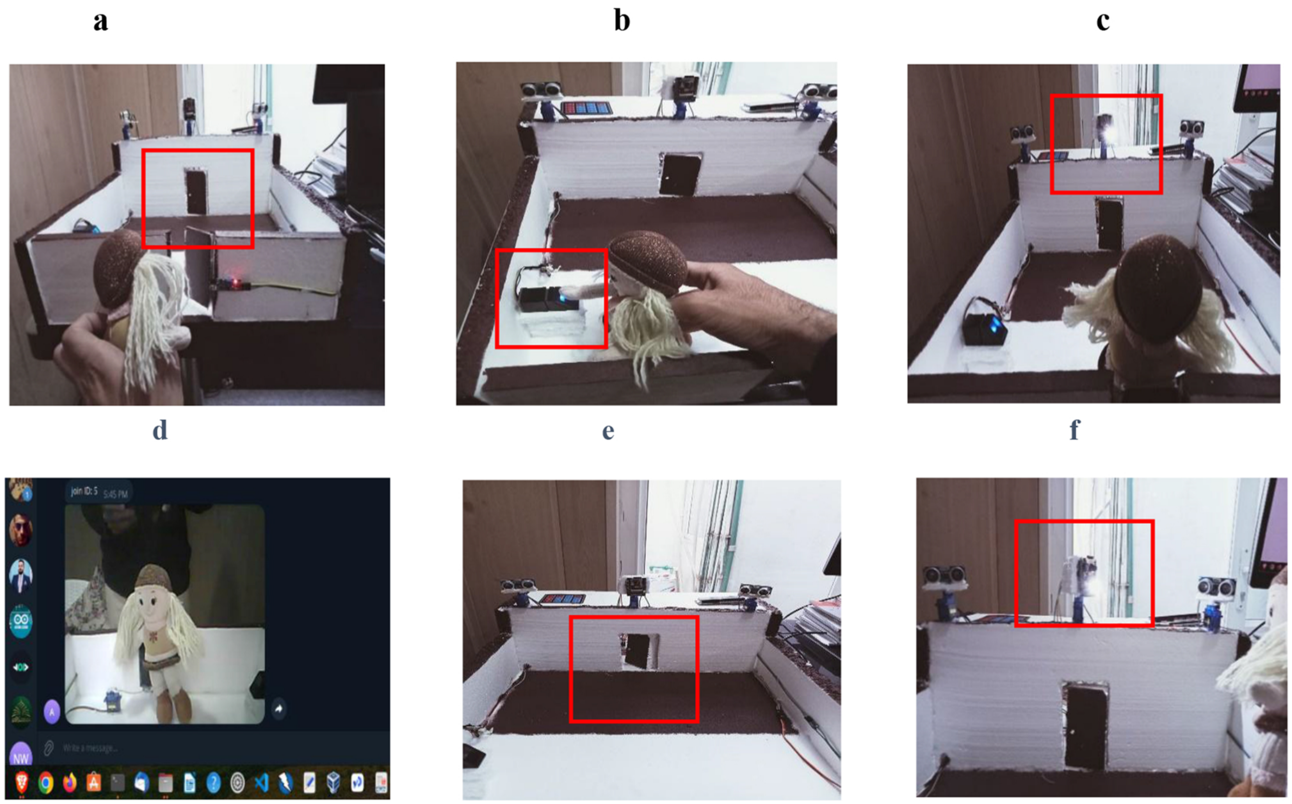

Fig. 3. Implementation of proposed access control system for special campus.

on a circuit board or across different boards, while serial communication is utilized for data transfer between Arduino-2 and ESP32CAM.

Multiprocessing is employed to execute multiple tasks concurrently within a single application. The millis() function in Arduino is a built-in function that is frequently used for multitasking, allowing the programmer to implement code that executes simultaneously. Unlike the delay() function, which pauses other operations, the millis() function ensures continuous operation even when the door opens, preventing slowdowns in connected devices. The Ubuntu (Linux) serves as the open-source operating system for holding MySQL database, website, and Telegram applications.

As high-level languages two main programming languages, Python and C++ are used in this work. Some necessary libraries (i.e.; flask) are utilized for developing application software and acting as a scripting language to integrate existing components. Flask is utilized for building web applications in Python. HTML and CSS are used for website design customization, and JavaScript used as enhancer for web pages to be more dynamic and interactive. Furthermore, Bootstrap is chosen for creating responsive and mobile-friendly web pages. Finally, the Telegram bot functions as a cloud-based messaging platform, enabling developers and programmers to create bots capable of interacting with users by exchanging messages, providing information, and responding to user input.

Network and internet services

Various network and Internet facilities and services are used for sending and saving visitor identification codes, photos, notification messages, and commands. Their functions are described below:

- GSM network: GSM shield directly connected to Arduino-1 microcontroller, it communicates with the security guard's mobile phone and gives notification when unauthorized user (visitor) attempts to enter the campus door.
- Wi-Fi network: Connected to ESP32CAM and Telegram bot via a Wi-Fi shield, facilitating communication between Arduino and the Telegram app. It enables capturing and sending visitor photos for security purposes.
- MySQL and Website: Connected to the system through the network, these services are used for saving and archiving visitors' data.

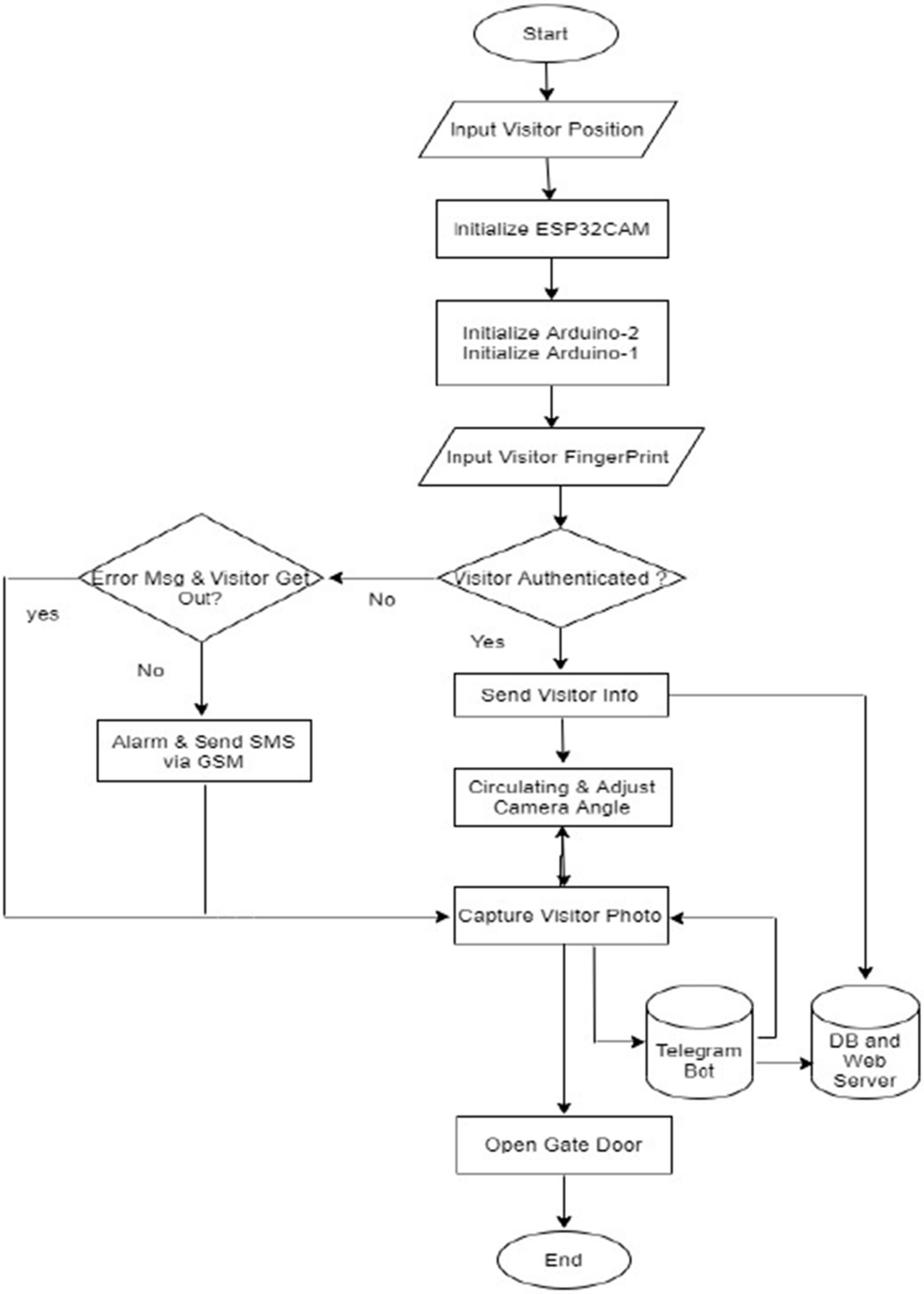

Fig. 4. System flowchart.

- Telegram bot: An Internet service utilized for capturing and saving visitors' photos for security purposes.

Implementation of proposed access control system for special campus

By installing this system on the campus entrance door, unauthorized access can be controlled. The system implementation begins with continuous monitoring of the entrance door using a PIR sensor, two ultrasonic sensors covering 180^{o} each, and an ESP32CAM security camera. When someone needs to visit any of the campus buildings, they go through a series of processes at the entrance doors. First, the PIR motion sensor detects the person approaching and triggers the opening of door 1, as illustrated in Fig. 3.a, a doll model face is used in place of a real

Table 1. Normal conditions system test.

No.	Code	Visitor Names	Time	Date	Status	Note	Phone No.
21	00801	Omed Kamal	09:23	2023-06-28	Accept	Recognized	077*******
22	00910	Rzgar Sardar	09:38	2023-06-28	Accept	Recognized	077*******
23	00501	Amjad Othman	09:53	2023-06-28	Accept	Recognized	077*******
24	00211	Hemn Ali	10:03	2023-06-28	Accept	Recognized	077*******
25	00101	Mohamad Akram	10:12	2023-06-28	Accept	Recognized	077*******
26	00101	Mohamad Akram	10;13	2023-06-28	Accept	Recognized	077*******
27	00211	Hemn Ali	11:01	2023-06-28	Accept	Recognized	077*******
28	00401	Ari Azad	11:02	2023-06-28	Accept	Recognized	075*******
29	00401	Ari Azad	11:54	2023-06-28	Accept	Recognized	075*******
01	#####	####	09:09	2023-06-29	Reject	Unrecognized	##########
02	00910	Rzgar Sardar	09:10	2023-06-29	Accept	Recognized	077*******
03	#####	####	09:11	2023-06-29	Reject	Unrecognized	##########
04	00401	Ari Azad	09:18	2023-06-29	Accept	Recognized	075*******
05	00601	Aras Mahmood	09:22	2023-06-29	Accept	Recognized	077*******
06	00101	Mohamad Akram	09:29	2023-06-29	Accept	Recognized	077*******
07	#####	####	09:39	2023-06-29	Reject	Unrecognized	##########
08	00010	Kardo Jamil	09:39	2023-06-29	Accept	Recognized	078*******
09	00310	Saman Ahmed	09:52	2023-06-29	Accept	Recognized	077*******
10	00011	Barham Taha	10:09	2023-06-29	Accept	Recognized	078*******

Table 2. Authentication process duration.

No.	Code	Status	Auth. duration
01	#####	Reject	10 sec
02	00910	Accept	8 sec
03	00101	Accept	9 sec
04	00211	Accept	8 sec
05	00101	Accept	8 sec
06	00101	Accept	9 sec
07	00211	Accept	8 sec
08	00401	Accept	8 sec
09	00401	Accept	8 sec
10	#####	Reject	10 sec
11	#####	Reject	12 sec
12	#####	Reject	12 sec

human face due to the small size of the proposed model. The person then proceeds to the next step and verifies their identity by scanning their fingerprint on the fingerprint scanner, as shown in Fig. 3.b. There are two possible scenarios: In Case 1, if the system detects that the person is a campus employee, meaning their fingerprint is already recorded in the database, the system automatically opens door 2 using the installed servo motor to allow entry into the campus. The person then approaches door 2, where the installed ultrasonic sensors measure the distance from door 1 to door 2. Simultaneously, the circulating ESP32CAM camera takes a photo. The system sends both the person's photo and fingerprint code (ID) to the MySQL database server and Telegram bot for security logging, as shown in Fig. 3.c,d. Finally, door 2 opens, allowing the person to enter the campus buildings, as depicted in Fig. 3.e. In Case 2, if the visitor is not an employee and their fingerprint is not recorded in the database, and they attempt to enter door 2 without scanning their fingerprint, the system follows these steps: First, the two ultrasonic sensors detect the visitor, and their data (unrecognized fingerprint) is sent to Arduino-2, instructing the ESP32CAM camera to take a photo of the visitor, as shown in Fig. 3.f. Door 2 remains closed, and the system notifies the visitor via an LCD banner to return and leave the area. If the person attempts unauthorized entry (intrusion) by manually opening the door, the system responds as follows: 1- The circulating ESP32CAM camera sends the intruder's photo and a message to the Telegram bot via the Wi-Fi chip. 2- The system alerts the security department (guards) by activating LED lights, a buzzer, and sending an SMS alert through the GSM network.

System flowchart

The data flow and processes between the Ultrasonic sensors illustrates in Fig. 4, ESP32CAM, and Fingerprint scanner (as input sensors), and the MySQL server, Web server, and Telegram bot (as output storage devices), utilizing wireless and GSM networks for data exchange and commands. Initially, the proposed system initializes its parameters by reading inputs. ESP32CAM, Arduino-1, and Arduino-2 are then initialized in sequence. The visitor proceeds to input their fingerprint into the system. If the fingerprint is unrecognized, the system rejects the user, triggers an alarm, and notifies the security department. If the fingerprint is recognized, the system proceeds to send visitor information (fingerprint code and visitor's photo) to the database and Telegram. Finally, the door automatically opens for the authorized person to enter the campus.

Table 3. Proposed system comparison with other research works.

Reference	Authentication Type	Reliability	Security-level	Location	Connection with Outside	Year of Publication
8	Android application	Medium	one factor	room door	No	2018
9	voice recognition	low	one factor	room door	No	2022
10	Android application	medium	one factor	house gate	Yes	2022
11	enter key	Low	one factor	campus gate	Yes	2022
Proposed System	GSM + Wi-Fi	High	two factors	campus door	Yes	2024

Results and discussion

In this section, the system undergoes testing to evaluate its accuracy and identify any potential errors. After implementation and testing at various dates and times, the system yielded specific results. When a visitor attempts to enter the campus, the system processes the instruction to permit authorized individuals and reject unauthorized ones. Already registered visitors need only about 8 seconds to do authentication process, while unrecognized visitors need 10-12 seconds till the system process their request and deny them to enter. Table 1 presents data for visitors during specific time durations, showing recorded details (e.g., code, name, phone number) to demonstrate the system's accuracy in accepting known individuals and rejecting those not in the database. While Table 2 presents data for visitors in specific time durations, showing authentication duration for both recognized and unrecognized visitors. Furthermore, comparing the proposed system with similar works referenced in the state-of-the-art literature reveals both strong points and limitations. Despite its useful features, such as efficient authorization processes, the system faces challenges, including the use of a lower-quality camera for capturing visitor photos. Table 3 provides a comparative analysis of the proposed system against other related research.

Conclusions

This study, proposes a new access control system. The research goals are to introduce a multi-factors authentication access control system specified for a specific campus, enhancing user authentication level by significantly reducing processing time to 8 seconds. Moreover, it improves the availability and then reliability of access control systems compared to other security measures, by utilizing network and Internet facilities. Experimental tests conducted present the system's fast ability to differentiate between authenticated, unauthenticated, and intruding individual visitors to the campus. Their information and photos can be taken and then archived for future reference. Sampling tests indicate a 100% success rate in distinguishing known visitors from unknown ones. For future work enhancements, the system could integrate object identification to enhance precision. Moreover, replacing the Arduino UNO with a Raspberry Pi, which offers superior hardware specifications such as network interfaces and processors, would benefit tasks requiring higher processing capacity such as data analysis, identification and AI. Furthermore, small adaptations could allow the system to be use for attendance tracking in various environments, including workplaces or correctional facilities.

Acknowledgment

Special thanks to the College of Science/Computer department at the University of Sulaimani for providing a suitable environment to complete this study.

Authors' declaration

- Conflicts of Interest: None.
- I hereby confirm that all the figures and tables in the manuscript are mine. Furthermore, any figures and images, that are not mine, have been included with the necessary permission for re-publication, which is attached to the manuscript.
- No animal studies are present in the manuscript.
- No human studies are present in the manuscript.
- Ethical Clearance: The study was approved by the local ethical committee at university of Sulaimani.

References

1. Haraa RH, Jinan NS, Abdul-Rahman I. Arduino microcontroller based building security system. Eng Technol. 2017;35(5):532–536. https://doi.org/10.30684/etj.35.5A.13.
2. Makanjuola PO, Shokenu ES, Araromi HO, Idowu PO, Babatunde JD. An Rfid-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System.

J Eng Res Reports. 2022;22(11):7–17. https://doi.org/10.9734/JERR/2022/v22i1117574.

3. Aya S, Díaz J, Mancipe S, Aranda J, González R, Teran M. A proposal of alternative Campus Access Control systems in the Universidad Sergio Arboleda sergio arboleda campus. 2020:1–6. https://doi.org/10.13140/RG.2.2.15076.60803.
4. Hussien Z, Dhannoon B. Anomaly Detection Approach Based on Deep Neural Network and Dropout. Baghdad Sci. J. 2020 Jun 23;17(2(SI)):0701. https://doi.org/10.21123/bsj.2020.17.2(SI).0701.
5. Lenko F, Velˇas A. possibilities of using modern access control systems for the purposes of research and teaching at university. CBU International Conference on Innovations in Science and Education; Prague, Czech Republic. 2020:146–151. https://doi.org/10.12955/pss.v1.62.
6. Aisyah S, Ali Y, Saharja K, Suhendra S, Sani A. smart door lock system development prototype using rfid technology id-12. JRI. 2022;4(4):379–384. https://doi.org/10.34288/jri.v4i4.433.
7. Jali TMG, kumari R, vidya MSS, raksha MRS. Security System using Arduino. IJCTT. 2018;60(2):120–122. https://doi.org/10.14445/22312803/IJCTT-V60P119.
8. Marpaung RSR. Android Based Door Security Design. Research of Artificial Intelligence, 2022;2(1):26–30. https://doi.org/10.47709/brilliance.v2i1.1535.
9. Bastari WF, Atmiasri APW. Design of Automatic Door Opening Prototype using Recognition Voice. JAETS. 2022;4(1):33–36. https://doi.org/10.36456/best.vol4.no1.5440.
10. Amiliansyah H, Galina M, Welman J. Access Control and Security System Via Bluetooth Application on Android Smartphone. J Eltikom. 2022;6(1):100–108. http://doi.org/10.31961/eltikom.v6i1.475.
11. Rajamohan P, Preethy A, Seow S, Nor A, Talha R. Design and implementation of an Arduino microcontroller based door access control system using RFID technology. Int J Psychosoc Rehabil. 2020;24(6):6255–6270. https://doi.org/10.61841/1rrkws74.
12. Niu Y, Jiang H, Tian B, Xiang H, Liu Y, Xia X, *et al.* An efficient access control scheme for smart campus. EAI. 2022;9(6):1–7. https://doi.org/10.4108/eai.21-3-2022.173712.
13. Fritzing website, Accessed Jul 2023 Online: http://www.fritzing.com.
14. Najmadin WB, Shakhawan HW. Data center environment monitoring and cooling system based on Arduino and GSM network. 2019; ICNS Proceeding: 10–17. https://doi.org/10.31530/17031.
15. Hind ZK, Attarid KA, Abdulkareem S, Senny L, Dwi FH, Rawnaq AM, *et al.* Measurement Enhancement of Ultrasonic Sensor using Pelican Optimization Algorithm for Robotic Application. Indones J Sci Technol. 2024;9(1):145–162. https://doi.org/10.17509/ijost.v9i1.64843.
16. Ivan DT, Arief W, Akhmad A, Jamaaluddin. Home Surveillance Monitoring with Esp32-Cam and SD Card for Data Storage. Journal of Computer Networks, Architecture and High Performance Computing. 2024;6(1):419–429. https://doi.org/10.47709/cnahpc.v6i1.3498.
17. Meftah SM, Arij ME, Mabrouka AA, Laila AE. Electronic Health File System based on Fingerprint Sensor Technology. J Adv Res Appl Sci Eng Technol. 2024;33(2):209–224. https://doi.org/10.37934/araset.33.2.209224.

تطوير نظام دقيق للتحكم في الوصول إلى Campus باستخدام الاتصال بالشبكة وخدمات الإنترنت

نجم الدين واحد بوسكانى

قسم الحاسوب، كلية العلوم، جامعة السليمانية، السليمانية، العراق.

الملخص

مع التحديث والتحول السريع لبيئتنا، تلعب أنظمة الأمن والمراقبة دورًا حيويًا في ضمان سلامتنا وأصبحت جزءًا أساسيًا من حياتنا لحماية ادواتنا ومبانينا. يوصى أن تكون أنظمة الأمان متاحة في كل مكان وفي جميع الأوقات لأن احتمالات المهاجمين واللصوص والمتسللين تتزايد يومًا بعد يوم. يعد تمكين أنظمة الأمان للأماكن الخاصة التي بها موظفين بمهام حساسة أمرًا صعبًا وبالغ الأهمية. تركز هذا البحث على تطوير نظام دقيق للتحكم في الدخول لأبواب مدخل campusالخاصة. يتحكم النظام المقترح في دخول الأشخاص إلى campus. يسمح للأشخاص المصرح لهم بالدخول ولا يسمح للأشخاص غير المصرح لهم (المتسللين) بإخطار حراس الأمن عبر شبكة GSM. يتكون النظام المقترح بشكل رئيسي من اثنين من متحكمات الأردوينو المتصلة ببعض أجهزة الاستشعار التي تتحكم في الأمن. كما تم دمج مرافق الشبكة (GSM وWi-Fi) وخدمات الإنترنت (الموقع الإلكتروني وTelegram bot) مع النظام لتبادل المعلومات وحفظ معلومات الزائر داخل النظام. تعتبر لوحات الأردوينو بمثابة مركز نشاط لاستقبال مدخلات الزوار (الرمز من بصمة الإصبع، الصورة من الكاميرا، والموضع من أجهزة الاستشعار بالموجات فوق الصوتية). ويقوم النظام بتحليلها ومعالجتها لقبول أو رفض الزوار. وأخيرًا، يرسل النظام المخرجات إلى الخوادم المتصلة (Telegram bot، وقاعدة بيانات MySQL، وخادم الويب). وباستخدام هذا النظام للمراقبة المستمرة، يضمن النظام الأمن في الوقت الحقيقي لمباني campus بأكملها وموظفيها. علاوة على ذلك، تشير نتائج الاختبار إلى أنه يمكن تحقيق أداء أفضل للمصادقة بمتوسط وقت يبلغ حوالي 8 ثوانٍ فقط، وتبين أن النظام أكثر قدرة بكثير من الأنظمة الأخرى لأنه يستخدم قنوات متعددة للاتصال. علاوة على ذلك، يعمل على تحسين الأمان لأنه يستخدم المصادقة الثنائية للتحقق من هوية الزائر. ومع ذلك، تتطلب إحدى القنوات المذكورة أعلاه خدمات إنترنت على مدار الساعة طوال أيام الأسبوع.

الكلمات المفتاحية: التحكم في الوصول، متحكم اردوينو، مرفق الشبكة GSM، الأمن متعدد العوامل التحكم في الوصول.