Smart Door Lock System for ATMs

K. Dhara Lakshmi, M. Deva Kumari, R. Harsha Vardhan, Y. Tanvi, Meena Belwal
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.4cse22218@bl.students.amrita.edu,bl.en.u4cse22237@bl.students.amrita.edu,
bl.en.u4cse22249@bl.students.amrita.edu, bl.en.u4cse22268@bl.students.amrita.edu, b_meena@blr.amrita.edu

***Abstract*—As we are living in the twenty first century, security has become one of the most important aspects of people's and companies' lives. The Smart Door Lock System for ATMs is designed as a secure and flexible mechanism of access control using Arduino Uno and RFID technology, where the system locks a door when a registered RFID card is presented to give restricted access to authorized personnel; otherwise, it unlocks the door when an unregistered card or other objects are sensed, offering controlled flexibility to external users. The system also has a manual override feature in case of emergencies. This project provides a highly reliable, cost-effective and scalable solution for replacing a locking mechanism, making it pretty suitable for ATM facilities as well as other secured environments.**

***Index Terms*—Arduino Uno, RFID sensor, RFID Cards, Relay Module, security, Solenoid Lock**

I. Introduction

A smart door lock system is needed for ATMs in order to improve security by ensuring that only people with approval can enter the building. It offers automatic access control, guards against illegal entrance, and enables real-time notifications and monitoring. Also, by reducing reliance on human checks and traditional keys, this solution improves the efficiency and security of access control. The challenges in implementing the smart door lock system are Traditional lock, Unauthorized Access due to the increased incidences of theft, Integration with Smart Devices.

The latest smart door locks are comprised of a combination of various differing technologies improving security through higher ease of use. Perhaps the most popular ones are IoT-based smart door locks, which, using any smart phone by means of an application remote, one can lock or unlock the entrance to his home and house door. Usually connected to this attached house lock using Bluetooth as well as often Wi-Fi. It can alert unauthorized access in real-time and it can be integrated with smart home devices, hence provides a comprehensive security solution that can be used both on residential and commercial sites.

Another advanced technique is access control using biometric authentication, such as fingerprint or facial recognition. It offers high security by first authenticating a user's unique physical features before allowing access. Biometric smart locks also have the feature of multi-factor authentication, where fingerprint scanning can be combined with PIN codes or smartphone verification for added security. These features make biometric locks suitable for high-security applications, such as research labs and military installations.

Contactless access control can be offered in RFID-based smart door lock systems using RFID cards or tags for access. Since the RFID reader scans its unique ID, it checks whether it is in an authorized list and unlocks the door if found to match. This access is mainly adopted in corporate offices and for ATM security to limit access from specific personnel only. The locks are tamper-resistant, and RFID can be used in conjunction with other technologies like mobile applications or biometric verification.

Further, the use of cloud connectivity in a smart door lock system makes the locking system have the potential for real-time monitoring and data storage. It has the capability to record every single event on access and allow tracking of who accessed the premises and at what time. It further avails remote access management wherein one can grant others temporary or permanent access to the premises. Moreover, cloud integration offers an easy integration of smart locks with other smart security devices such as cameras or alarms to form a total security solution.

However, these techniques looks in Limited Alerts in many systems, features such as notifications if there is an attempted break in are not availed immediately. Complex Setup are Some of the smart lock systems have challenging installation and setup procedures involved in the procedure. The cost can also sometimes pose some restrictions to uptake like in the current world where prices are high.

As there are limited work for ATM, the proposed work aims to Construct a system that will improve the ATM security by giving alerts whenever there was an intrusion. Next, the proposed system needs to be easy to install or even compatible with the usual smart home systems to use. Further, the proposed system tries to be cost-effective such that the larger population of the target audience will be able to access and use it.

The key contributions of this work are:

Enhanced Security: The system of rules furnish improved security by using RFID engineering to allow approach only to authorized personnel, in effect foreclose unauthorized entry.

Automated Access Control: It automate the locking and unlocking process, progress to it more efficient and thin out the reliance on traditional keys.

Emergency Override Capability : It offers a manual override option to yield memory access in emergencies, ensuring

flexibility in critical scenarios.

The rest of the article is organized as follows: Section II discuss the Literature Survey. Section III describes the methodology utilized. Further, the Implementation is explained in Section IV. The Results and analysis is presented in Section V. Finally, Section VI concludes the research.

II. Literature survey

The work by Shanthini M. et al. [1] examine an Internet of Things (IoT)-based that enables users to operate door lock with an Android smartphone app. The technology can be expanded for commercial use, such as ATMs and vending machines, and intends to offer improved security and accessibility. Venkatasam et al. [2] gave the smart entry padlock organization that is suggested in this paper is dependent on the IoT also combines face recognition, fingerprint, RF card, password, and IoT technologies to improve security and user convenience. With the use of a smartphone app, users may remotely control the system, which is especially user-friendly for senior citizens. Ahmed et al. [3] provided a very secure door lock system useful in essential areas demanded for security, research labs, military institutes, and other such departments. This will be done through the implementation of RFID technology, one-time password, and encryption. The system mainly includes secure wallet Android app, RFID reader, and lock involving the microcontroller base. The work by Kolluru et al. [4] is a voice-activated, fingerprint-recognition, keypad-based smart door lock system that allows self-access to doors in an easy, safe, and convenient manner. The solution integrates voice recognition, fingerprint recognition, and keypad entry with an Arduino microcontroller for three different unlocking options. Mathew et al. [5] proposed on safe and practical access control in homes, workplaces, and other locations, Through a smartphone app, users may remotely operate the system and combine it with other smart home appliances. An output simulation is shown, and potential uses in different fields are discussed. Sivaprasad R. et al. [6] gave a prototype by sustainable double-access biometric validation. Thumb impressions are collected using a biometric scanner, and the system is linked to a real-time database housed in the cloud. In comparison to password- and RFID-based door locks, it has demonstrated competitive performance. Jayaram B. et al. [7] developed technique for locking smart doors that the paper offers improves home security through using image processing and IoT. It takes pictures of people using a camera and detects their presence using a motion sensor. ATM and business buildings can be added to this system. The work by Hou et al. [8] address the need for a lightweight and highly secure temporary key function (TKF), this work offers a unique authentication module for smart entry locks based on elliptic curve cryptography (ECC). The work by Saroha et al. [9] presented a biometric, safe, intelligent Internet of Things door lock system with facial recognition user identification. With a 93.5 percent accuracy rate, the system offers email and mobile notifications, passcode-based verification, and more. It does away with the requirement for keys or RFID cards. The work by Keerthi et al. [10] provided a complete home security system that connects the Smart Safe, Smart Eye, Window/Gate Sensor, and Fire Alarm to a cloud for real-time control and monitoring through Internet of Things technology. Adjusting devices is simple with Dependent Cloud, which is more practical and economical. The work by Hindusree M. et al. [11] address a range of shoulder surfing attacks, including when a hacker simply watches a user enter their PIN in public. The authors here discuss several remedies currently in use against these types of attacks, Thus, technique can be used for stopping shoulder surfing attacks in mobile applications as well as services like ATM, etc. The work by Doshi et al. [12] examined the display of an IoT-based face recognition technology. The face of the visitor is captured through raspberry pi, camera module, and relay module, and the same notification will be directed toward the homeowner's telephone app. Balbin et al. [13] introduced a automobile entry handle thru following then watchful organization by means of GPS knowledge besides IoT-based computer hardware control. A system developed here consists of a GPS module, microcontroller, pneumatic lock, and a battery for power supply that enables users to pathway and television. Do et al. [14] presented a Jetson Nano board-based IoT-based smart lock system with facial recognition abilities. It uses a Raspberry Pi v2 camera to take pictures and processes them in real-time with its automatic training data collection and labeling. Overall, the suggested system provides smart homes and other environments with an affordable, effective, and user-friendly answer for their security needs. Prabakara et al. [15] improved home security and accessibility and is especially made for the elderly and disabled. It makes use of modern technologies to enable remote access control, including a key pad and mobile application. The system requires the proper passcode to be entered in order to get entry, and also notifies users when someone is at the door. The work by Kavde et al. [16] used Bluetooth technology to deliver effective home security and automation through an internet-connected smartphone that controls door locks, offers live video feeds, and can store visitor information. The system was designed to make lives more livable and to simplify matters for working persons and disabled people. The work by Masykuroh et al. [17] designed and developed along with the implementation using a fingerprint sensor and Arduino Uno board with the WiFi module to present secured remote access control by locking doors with fingerprints and issuing a notification to the user by unlocking the room unauthorizedly immediately. The work by Ahtsham et al. [18] showcases that offers safe and remote access control through the useage of an Arduino Uno, a WiFi module and fingerprint sensor. Apart from opening their doors using the fingerprint, the technology gives its users alerts on their Telegram if anyone is attempting to enter the room with malicious intentions. The work by Baikerikar et al. [19] developed a system of high-security door lock, intended to protect stored by a user information and any valuable item. It is able to lock and unlock users' doors using an application of the smartphone, a keypad, a microcontroller, and a server. Methods of hashing and encryption secure any flow of data and prevent unwanted attempts to access. The work by Khan et al. [20] introduced a new variant of the intelligent door

locking system with a keypad interface, microcontroller, and server programmed to provide some secure remote access control. This can easily be achieved by locking or unlocking doors with an OTP received in their mobile phones, all the while availing a service to chat with guests. Abhijith S. et al. [21] described an IoT-based system to improve the security of automated teller machines against electronic threats. With the number of ATMs being on the rise, this system secures ATMs from being tampered with hacked. The system is reasonably priced, cost-effective, and security personnel can monitor the ATM machines from an off-site location. The work by Telluri et al. [22] developed nation in constructing a much more reliable public transport system. Instead of the paper tickets of the legacy, the reusable RFID tags should be used for automatic identification of passengers and fare deduction according to distance traveled through GPS. The work by malla et al. [23] presented novel object-level mapping of indoor environments combining RFID technology with INS. It considered indoor spaces, which are dynamic over time; hence, traditional mapping techniques may neglect some of the important fluctuations by just altering the position of the objects. The work by Gokul et al. [24] detailed the biometric smart ATM system that increases security with RFID and fingerprint authentication. The system utilizes RFID cards and fingerprints that replace PINs for real-time identification validation. The ATM scans the RFID card and fingerprint, showing access information to the card holder. Sensor and IoT have been used in several other fields also for controlling and monitoring the physical parameters [25].

However, there are some limitations in the literature presented in this section. There is insufficient end to end testing for scalability, performance, and security including a rather confined focus on possible security threats and vulnerabilities such as regarding cloud database and Bluetooth. Furthermore, many systems fail to provide thorough evaluation of power and energy requirement, and evaluation of scalability for use in the commercial context. Also, the integration of the system with other IoT devices is not very promising, so is the authentication which is limited to a simple username password or single biometric verification. Finally, very few papers tend to compare the proposed solution with readable text door lock systems and therefore the scope for further development in terms of security and usability of the system is high. This work is another step in the similar direction.

III. METHODOLOGY & IMPLEMENTATION

A. System Architecture

Fig. 1 depicts the architecture of the proposed smart door lock system for ATMs.

The proposed smart door lock system on ATMs will be adding more security. It works such that the users will only have access if given authority. Its core proposition primarily relies on the integration of RFID technology with an Arduino microcontroller processing different inputs from various components in the control of the locking mechanism. It works in such a way that it detects an RFID card and locks or unlocks the door, whether the presented card is found in the list of

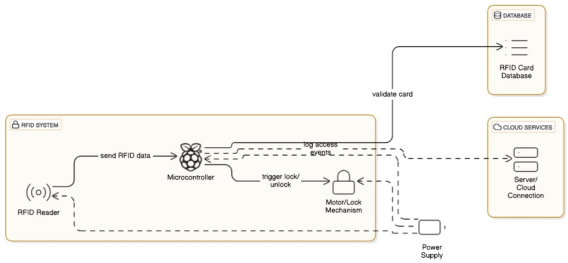

Fig. 1. Architecture of the proposed smart door lock system for ATMs

accepted cards that have been previously set or not. This denies admission to any unauthorized person using the ATM premises since only those with an admittance-whether bank employees and security guards-can lock the door.

This system of smart door lock will be concentrated intensively to secure the ATMs by applying a locking mechanism based on RFID. The presentation of an authorized RFID card from the user causes the system to lock the door. The door unlocks if some kind of unauthorized card or any other object is presented, thus blocking the entry way. It will add an extra priceless security feature if installed in an ATM facility, that overcomes the vulnerability of traditional locks, which is weak and also easy to compromise. The system, using RFID technology, provides a good and tamper-proof access control solution.

This smart door lock system consists of many parts, and each one of them has a function. The Arduino Uno really is a system that integrates the core portion into one place: inputting and providing outputs. All the data gained from the RFID reader are passed on to the system to work upon; this is then executed by the LEDs and locking mechanism, if available for input conditions. There is use of an MFRC522 RFID reader. It detects RFID tags or cards and their unique identification number. It's connected to the Arduino via a set of special pins hardcoded in the sketch using SPI communication protocol. LEDs are used as visual indicators for access. In such a case, if access is granted, then the green LED lights up because it indicates that the card presented here has been authorized. If the access is not granted, then the red LED lights up as it indicates an unauthorized card has been detected.

This design puts pins as an input and output. At the initialization stage, it also configures the RFID reader to have itself prepared for card detection. Then, the Arduino starts a polling loop that it checks repeatedly to determine whether an RFID card is available in the system. In this way, the system is always ready to detect the card and shall then take the proper action later on. Pre-initialization is very important since it normally sets up its hardware components and prepares the system for scanning continuously.

Work by constantly scanning RFID cards with the reader. When it scans a card, it collects that card's identification number and sends that identification to Arduino for processing. Then the program compares the detected UID with the list of authorized UIDs stored in the program. Then, if the UID of that card matches one of the authorized UIDs it allows access through that. It lit up a green LED for pass status. The door

locking mechanism now starts auto-locking and unlocking after some time. It actually locks during this short time to enhance security but in a controlled way.

The system denies the access if the detected UID does not appear in the list of authorized UIDs. The red LED blinks, in this case, the system indicates denial of access. To the user, the response given is that the card presented cannot be allowed to close the door. In this respect, the system enhances user awareness through the use of visual feedback mechanisms while at the same time providing clarity on whether they will access the door.

The smart door lock system presents various benefits which make it greatly practical as an instrument in the improvement of ATM security. To begin with, the system ensures that control is properly maintained in accessing through RFID cards, making it hard to modify. The presence of visual feedback provides users with proper knowledge of their access statuses and thus enhances reliance on the general system. With a manual override integration, flexibility and preparedness in case of emergencies will be there. The security at the point of access will reduce with a cut in the need, hence improvement and efficiency on consistency in maintaining secure ATM environments due to automation.

B. Circuit Diagram

The circuit diagram of the proposed smart door lock system for ATMs is presented in Fig. 2.

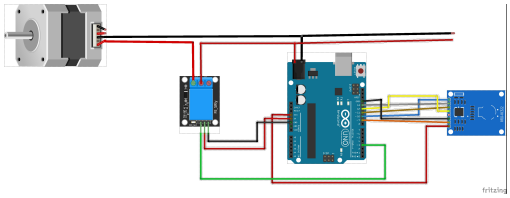

Fig. 2. Circuit Diagram of smart door lock system for ATMs

- Arduino UNO Board: There is a microcontroller sheet based on the ATmega328P in the middle of Arduino UNO and puts the other part of the circuit under its control. This board has countless pins, some used as grounding, others for the power supply, and others for communication purposes with modules attached to it.
- Stepper Motor: There is a stepper motor in the circuit diagram which is actually a type of brushless DC motor. It breakdowns up total rotation into several identical steps, so that angular movement is under very precise control. The driver module controls the speed of rotation of the motor into the system through signals from the Arduino.
- Relay Module: The relay module is used here as the actuator that enables to control with low power signal originating from the Arduino board a high power component in this case a stepper motor. The relay is driven through Arduino, and this relay's input pin receives the signal that would make the relay on or off; after which, the stepper motor connected to it is controlled.
- RFID Module: RFID reader module is another very vital part of the system. It is used to read RFID tags. In most cases, the module communicates with the Arduino board through multiple pins that are connected using an SPI protocol as shown with MOSI, MISO, SCK, and RST connected. The module can read data that come from RFID tags brought near to it, so it can be used for different types of applications like access control or ID.
- Power and Ground Connections: These black wires represent the ground connection. These red ones represent power connections. The system has to be grounded very well so that it operates stably, and power has to be provided to every component for it to work.

C. Hardware Setup

- Hardware Components: Arduino Uno, RFID Reader, RFID Cards, Relay Module, Electronic Door Lock, Power Supply. The hardware setup is presented in Fig. 3.

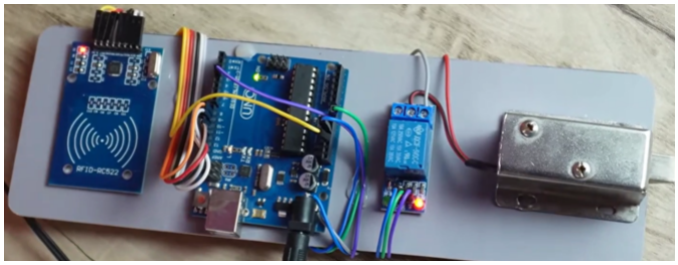

Fig. 3. Hardware Setup for smart door lock system for ATMs

Fig. 4 is the basic hardware configuration of the RFID card scanning system for the smart door lock in ATM access control.

In an ATM smart door lock system, integration of the RFID technology will allow better security and management of access control. The authorized access to the ATM is available by scanning the RFID card, bringing safe, contactless entry into the area as shown in Fig. 4.

Fig. 4. Card Scanning for smart door lock system for ATMs

D. Software Setup

- Software Components: Arduino IDE, SPI Library, Serial Monitor, Custom Code Implementation.

The Fig. 5 shows the readings generated after scanning the RFID card in the serial monitor. These data have been provided in relation to major parameters such as the ID of the card, the access status, and the scan time. All these readings ensure authenticity of the card to approve or disapprove the entry in the ATM area. The information is logged by the system to refer to it later on for the efficient and safe monitoring of

access attempts. It refers that only authorized people should get inside the restricted ATM spaces.

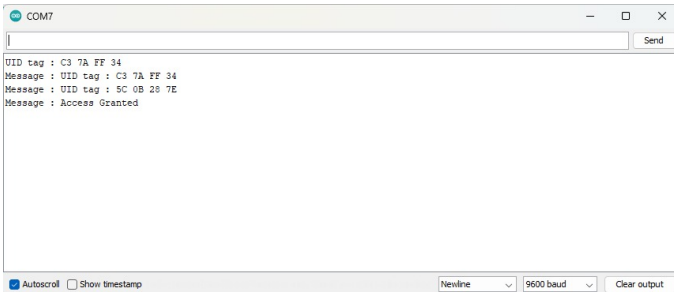

Fig. 5. Serial Monitor readings of smart door lock system for ATMs

IV. RESULTS

In two different cases, the performance and security of the RFID-based smart door lock system were tested - the first case when an RFID card that is registered has been scanned while the door was in the closed position and the second case where an unregistered RFID card has been scanned with the door not closed. This test is necessary to verify whether the user authentication occurs or not and to provide security access control by the system.

The system was tested thoroughly and the observed results are presented in this section as the two scenarios:

Case 1: *Registered Card Scan with Door Closed*

In this case, if the door is closed and when a valid RFID card has been read, the door unlocks. The access time logged and door opened and upon entry into the ATM room, that is to say it has worked as expected if the card is validated and the door is closed position as shown in Fig. 6.

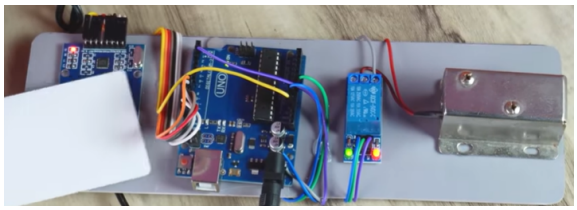

Fig. 6. Door Closed

Case 2: *Registered Card Scan with Door Open*

In this case, if any door is not closed with a scanned unregistered RFID card, then access shall be denied. The system will note the failed attempted access and keep the door locked. This outcome confirms the fact that the system correctly identifies the unregistered cards and thus denies illegal people from opening the door but allows only the legal registered users to open the door as shown in Fig. 7.

V. CONCLUSION

One of the most successful implementations in integrating RFID technology and IoT-based automation for improved ATM security and convenience is the Smart Door Lock System for ATMs. The use of RFID cards for user authentication makes sure that the unauthorized accesses are denied and the

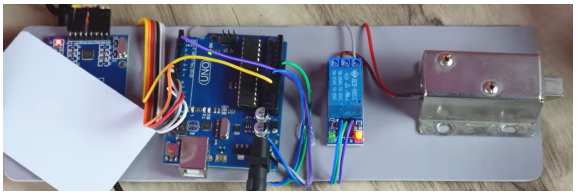

Fig. 7. Door not Closed

fraud activities are prevented. It makes use of an MFRC522 RFID Reader, LEDs, and an electronic lock all controlled through a microcontroller and makes use of very wonderful components. This makes it a reliable, scalable, and energy-efficient solution that offers a very seamless experience for the users. More so, the instant denial of access by the system to cards that have not been registered is a good indication of the security level that has been offered by the solution. Overall, the proposed system achieves both major issues of securing ATMs and user accessibility, thus further improving the systems in the safe access control area for different industries.

VI. FUTURE SCOPE

This might include a smart door lock system for ATMs with biometric authentication settings, such as fingerprint and facial recognition authentication, coupled with RFID technology. Its connection with a real-time monitoring platform or a mobile application would also enable the system to provide remote access control, alerts, and activity logs. Additional features could include IoT-based cloud storage for storing user access logs and machine-learning algorithms for anomalous activity detection, which would intensify security and increase usability. This would entail making the system more polished for use beyond ATMs.

REFERENCES

[1] Shanthini, M., G. Vidya, and R. Arun. "IoT enhanced smart door locking system." In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 92-96. IEEE, 2020.

[2] Venkatasamy, Ramkumar, Joshuva Arockia Dhanraj, S. Aravinth, and K. Balachandar. "Design and Development of IOT based Smart Door Lock System." In 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), pp. 1525-1528. IEEE, 2022.

[3] Ahmed, Abdullahi, Said Abdulkadir, Jama Mohamed, Suleiman Abdullahi Ali, Mowlid Abdi, and Sharmake Ali Kahie. "Design and Implementation of an IoT based Smart Door Lock System." In 2023 2nd International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS), vol. 1, pp. 1-6. IEEE, 2023.

[4] Kolluru, Chaitanya, G. V. Akhil, Krishna Reddy, and Aruru Sai Kumar. "Development of Face Recognition-Based Smart Door Lock System with Remote Servo Control Authentication." In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-6. IEEE, 2023.

[5] Mathew, Meera, and R. S. Divya. "Super secure door lock system for critical zones." In 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), pp. 242-245. IEEE, 2017.

[6] Sivaprasad, R., C. Yazhini, G. S. Harini, J. Jayashree, and K. Prathibanandhi. "Automatic Door Locking System in Households Using IoT." In 2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS), pp. 1-4. IEEE, 2023.

[7] Jayaram, B., D. Abdus Subhahan, B. Sakthivel, T. A. Mohanaprakash, Sunita Joshi, and M. Jogendra Kumar. "IoT and Image Processing based Smart Door Locking System." In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), pp. 291-295. IEEE, 2022.

[8] Hou, Dongkun, Shiyuan Cheng, Jie Zhang, Yuji Dong, Jieming Ma, Xiaohui Zhu, and Ka Lok Man. "A highly secure authentication module for smart door lock with temporary key function." In 2022 International Conference on Cyberworlds (CW), pp. 228-235. IEEE, 2022.

[9] Saroha, Aditya, Anant Gupta, Aditya Bhargava, Anup Kumar Mandpura, and Himanshu Singh. "Biometric authentication based automated, secure, and smart IOT door lock system." In 2022 IEEE India Council International Subsections Conference (INDISCON), pp. 1-5. IEEE, 2022.

[10] Keerthi, Koney Sai, Anushree A. Yadwad, Katikala Sai Kumar, and M. Ananda. "Independent, Integrated, Reconfigurable IOT based Home Security System." In 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 27-34. IEEE, 2022.

[11] Hindusree, M., and R. Sasikumar. "Preventing shoulder surfing in secure transactions." In 2015 International Conference on Computing and Communications Technologies (ICCCT), pp. 160-163. IEEE, 2015.

[12] Doshi, Om B., Hitesh N. Bendale, Aarti M. Chavan, and Shraddha S. More. "A Smart Door Lock Security System using Internet of Things." In 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1457-1463. IEEE, 2022.

[13] Balbin, Jessie R., Ramon G. Garcia, Mary Anne E. Latina, Ma Anthonette S. Allanigue, Jan Kenneth D. Ammen, Anthony Vil B. Bague, and Jack Miller Jimenez. "Vehicle door latch with tracking and alert system using global positioning system technology and IoT based hardware control for visibility and security of assets." In 2017IEEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), pp. 1-5. IEEE, 2017.

[14] Do, Tri-Nhut, Cong-Lap Le, and Minh-Son Nguyen. "IoT-based security with facial recognition smart lock system." In 2021 15th international conference on advanced computing and applications (ACOMP), pp. 181-185. IEEE, 2021.

[15] Prabakaran, Pavithra, I. Sumedha, Lathesh Umashankar, Manvitha M. Rai, and Mitai Swathi. "Smart Door Lock System For The Elderly And Disabled." In 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), pp. 229-233. IEEE, 2021.

[16] Kavde, Siddhi, Riddhi Kavde, Sonali Bodare, and Gauri Bhagat. "Smart digital door lock system using Bluetooth technology." In 2017 International Conference on Information Communication and Embedded Systems (ICICES), pp. 1-4. IEEE, 2017.

[17] Masykuroh, Kholidiyah, Fikra Titan Syifa, Gatot Rizky Setiyanto, Afifah Dwi Ramadhani, Danny Kurnianto, and Nanda Iryani. "Prototype smart door lock by using wireless network based on arduino uno." In 2021 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), pp. 342-347. IEEE, 2021.

[18] Ahtsham, Muhammad, Huang Yan Yan, and Usman Ali. "IoT based door lock surveillance system using cryptographic algorithms." In 2019 IEEE 16th International Conference on Networking, Sensing and Control (ICNSC), pp. 448-453. IEEE, 2019.

[19] Baikerikar, Janhavi, Vaishali Kavathekar, Nilesh Ghavate, Ronit Sawant, and Kharanshu Madan. "Smart door locking mechanism." In 2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), pp. 1-4. IEEE, 2021.

[20] Khan, M. Adil, Kashif Nisar, Ehtisham Lodhi, Jawad Khan, Muhammad Imran Khan, Tariq Rahim Soomro, and Sana Nisar. "Prototype model of an IoT-based digital and smart door locking system with enhanced security." In 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), pp. 1-7. IEEE, 2022.

[21] Abhijith, S., K. N. Sreehari, and Anu Chalil. "An IOT based system for securing ATM machine." In 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1, pp. 1764-1768. IEEE, 2022.

[22] Telluri, Pavan, Saradeep Manam, and Jayashree M. Oli. "Automated bus ticketing system using RFID." In 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), vol. 1, pp. 445-450. IEEE, 2019.

[23] Malla, Hemanth, Preethish Purushothaman, Shivnesh V. Rajan, and Vidhya Balasubramanian. "Object level mapping of an indoor environment using RFID." In 2014 Ubiquitous Positioning Indoor Navigation and Location Based Service (UPINLBS), pp. 203-212. IEEE, 2014.

[24] Gokul, S., S. Kukan, K. Meenakshi, SS Vishnu Priyan, J. Rolant Gini, and M. E. Harikumar. "Biometric based smart atm using rfid." In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 406-411. IEEE, 2020.

[25] Rathina Raj, Vishnu Kanthan, and Meena Belwal. "Design of CoAP Based Model for Monitoring and Controlling Physical Parameters." In Ubiquitous Communications and Network Computing: 4th EAI International Conference, UBICNET 2021, Virtual Event, March 2021, Proceedings, pp. 105-115. Springer International Publishing, 2021.