International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 5, Issue 10, 2026
DOI: https://doi.org/10.38124/ijsrmt.v5i10.1753

GSM-Based Intrusion Detection and OTP Authentication Using PIR Sensing: An LED Prototype

Obiora Emeka Okoye[1]; Onyedikachi Fortune Nwandieze[2]; Chinaza Desmond Nwajiobi[3]; Ernest Chidi Okoroafor[4]; Chika Chibuzor Okwuma[5]; Chinyere Perpetual Ezeuzo[6]

[1]Department of Physics with Electronics Technology, School of Science and Technology, Federal Polytechnic Oko, Nigeria
[2]Department of Physics with Electronics Technology, School of Science Laboratory Technology, University of Port Harcourt River, Nigeria
[3,4,5,6]Department of Physics with Electronics Technology, School of Science and Technology, Federal Polytechnic Oko, Nigeria

Publication Date: 2026/11/14

Abstract

In this study we describe the design and experimental evaluation of a GSM based intrusion detection and one time password (OTP) authentication prototype. An Arduino Uno controls an HC-SR501 passive infrared sensor, a SIM800L GSM module, a 4 x 4 keypad, a 16 x 2 I2C liquid-crystal display, a green indication LED and a buzzer. When motion is detected, the controller creates a 4-digit pseudo code and sends it to the predefined cellphone number via GSM module. The user enters the code on the keypad and presses the hash key to confirm. Correct and wrong answers have different visual and sound effects. Prototype tests revealed reliable sensing of motion within a range of 3–5 m, correct processing of all documented OTP test cases, and transmission of brief messages reliant on the network with an approximate 70% success rate among four Nigerian providers evaluated. These results demonstrate the viability of combining local sensing, GSM notification, and temporary code-based authentication in a low-cost LED prototype, and point to power stability, network coverage, and message latency as significant implementation obstacles.

Keywords: *Intrusion Detection; Passive Infrared Sensor; GSM Communication; One-Time Password; Arduino; LED Prototype*.

I. INTRODUCTION

It is still a major problem for people, organisations, and governments to provide security, as the rate of burglary, unauthorised access, and intrusion is increasing (Adeyeye et al., 2024). Traditional security methods like mechanical locks, guard patrols and simple alarm systems are sometimes insufficient to combat today's threats as they can be readily circumvented or fail to offer real-time notifications (Sabit, 2025).

Electronic security systems have implemented groundbreaking solutions that integrate sensors, communication technologies, and authentication methods (Lucas & Ibrahim, 2025). The passive infrared (PIR) sensor identifies motion by assessing variations in infrared radiation, providing affordability, energy efficiency, and dependability in recognising human activity (Mahajan, 2023; Yongchareon et al., 2025). The Global System for Mobile Communication (GSM) facilitates the transmission of data over mobile networks (Arinde & Idowu, 2024; Kabilan et al., 2023). Incorporating GSM technology facilitates the transmission of notifications directly to the owner's mobile device, enhancing the speed of responding to any dangers (Nigade, 2024).

Okoye, O. E., Nwandieze, O. F., Nwajiobi, C. D., Okoroafor, E. C., Okwuma, C. C., & Ezeuzo, C. P. (2026). GSM-Based Intrusion Detection and OTP Authentication Using PIR Sensing: An LED Prototype. *International Journal of Scientific Research and Modern Technology*, *5*(10), 139–147. https://doi.org/10.38124/ijsrmt.v5i10.1753

A reliable technique for confirming identity is one-time password (OTP) authentication (Mashta, 2023). OTPs are more resilient to replay attacks and password theft than static passwords since they are dynamic codes created for a single session (Al-Zubaidie et al., 2022). Users can be alerted to intrusions and asked to provide a temporary code before access is approved by integrating OTP authentication with GSM-based communication (Mashta, 2023).

Intrusion detection systems (IDS) monitor the environment and detect unauthorised entry (Lawrence, 2025). The traditional IDS used basic alarm devices activated by motion or forceful access (Tripathy & Behera, 2025). With recent developments, smart IDS may now include sensors, microcontrollers, and communication modules for real-time monitoring (Alashjaee & Alqahtani, 2025; Miracle et al., 2025). The combination of PIR sensors with GSM modules enhances security by delivering immediate alerts (Arinde & Idowu, 2024; Okafor et al., 2024). Integration of RFID readers, NodeMCU microcontrollers, and GSM modules for full security solutions in identity verification and access control (Bhat et al., 2023).

PIR sensor pick up changes in the infrared radiation that things, especially people, give off (Yang et al., 2019). As Kumari et al. (2023) and Sonowal et al. (2025) say, they can tell the difference between human movement and background sounds, but not between authorised and unauthorised people. This means that they need to be integrated with access control systems. This limitation underscores the value of supplementary authentication methods (Arinde & Idowu, 2024).

GSM modules facilitate security systems in transmitting immediate notifications through SMS or phone calls (Kumar et al., 2025). GSM-based systems offer an economical and dependable solution for remote surveillance, particularly in areas with restricted internet access (Okafor et al., 2024; Omede et al., 2024). GSM integration facilitates remote control capabilities, permitting users to activate or deactivate equipment by SMS commands (Ikpenyi et al., 2022).

While security systems are available, many of them have limitations. Traditional alarm systems usually use a local sound alert; thus they will not be useful when the property owner is not physically at the location (Zhang et al., 2025). Mechanical locks and static passwords can be copied, stolen or brute-forced (Thopate et al., 2023). The absence of real-time communication between security systems and property owners is another important barrier (Sudha et al., 2024). Response time is delayed without timely notification, allowing intruders to escape or cause harm.

This research examines the gaps of traditional security systems in delivering: (i) dependable intrusion detection using effective sensors, (ii) immediate communication and notifications through GSM technology, and (iii) secure access management utilising dynamic OTP authentication.

The main goal of this work is to design, implement and experimentally assess a GSM based intrusion detection and one-time password (OTP) authentication prototype that blends passive infrared (PIR) sensor with short-message-service (SMS) notification and local code verification. The prototype is implemented as an LED indicator system to illustrate the viability of combining motion detection, GSM connectivity and temporary code-based authentication in a low-cost embedded platform. The specific objectives are: (i) design and build a PIR-based motion-detection subsystem for detecting unauthorised movement within a predefined range; (ii) incorporate a SIM800L GSM module for transmitting OTP notification messages to a registered mobile number; (iii) develop a four-digit OTP generation and verification protocol with specified validity and failed attempt limits; (iv) devise a user interaction interface employing a 4 4 keypad and a 16 2 I2C liquid-crystal display for system.

II. METHODOLOGY

- *Materials*

The following components set up the system: a microcontroller called Arduino Uno (ATmega328P), a motion detector called PIR Sensor (HC-SR501), a communication module called GSM 800L, an input matrix keypad called 4×4, an LCD display with an I2C interface, a green LED that indicates access, a buzzer that makes noise, and a regulated power supply with at least 2A for the GSM and 1A for the Arduino and peripherals.

The embedded software was created using the Embedded C/C++ programming language within the Arduino Integrated Development Environment (IDE). The Serial Communication Library, LiquidCrystal I2C Library, and GSM AT Command Library are all libraries.

- *System Architecture*

Following a modular design approach, the system's peripheral components are coordinated in data flow by the central processing unit, the Arduino Uno. The block diagram of the system is shown in Figure 1.

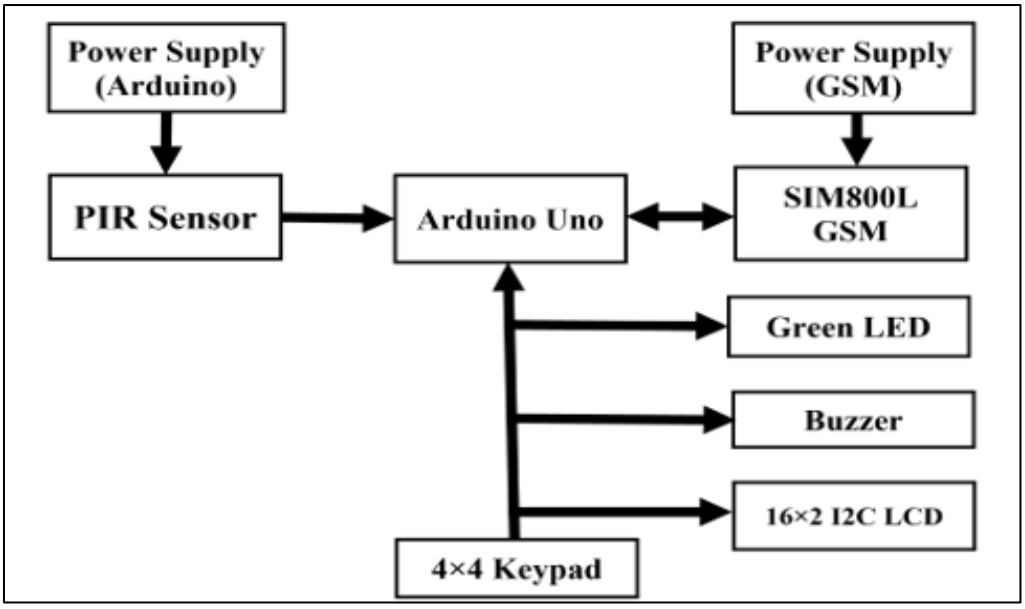


Fig 1 Block Diagram of the GSM-Based Intrusion Detection and OTP Authentication System

The modular approach enabled individual testing and validation of components before integration, minimizing potential conflicts and ensuring optimal performance.

- *Circuit Implementation*

Figure 2 is a circuit diagram showing the connections between the power source, buzzer, LCD, keypad, GSM module, PIR sensor, and Arduino Uno. Table 1 details the pin configurations for each component and how they connect.

Connected to digital pin D2, the HC-SR501 PIR sensor draws power from the 5V supply and GND. In order to respond instantly to motion detection, this pin is set up as an input with interrupt capabilities.

Through UART serial communication, the GSM module (SIM800L) exchanges data. The TX pin of the GSM module is connected to digital pin D3 (RX) on the Arduino, and digital pin D4 (RX) is also connected to the GSM module. This allows for two-way communication, which is necessary for delivering AT commands and SMS warnings. During gearbox bursts, the GSM module needs a steady supply of 3.7V to 4.2V that can produce 2A at least.

Eight digital pins set up as a row-column scanning matrix power the 4×4 matrix keypad. Configured as inputs with internal pull-up resistors are four column pins (D5-D8) and four row pins (A0-A3) that are set up as outputs. By reading the states of each column and scanning each row, this setup can determine which key is pushed.

Using pins A4 (SDA) and A5 (SCL), the 16×2 LCD display can be connected over the I2C interface. The I2C interface simplifies the circuit and frees up digital pins for additional operations by reducing the number of pins from six to two. Status messages, one-time password requests, and access notifications are all handled by the LiquidCrystal_I2C library's communication protocol.

Digital pin D10 controls the green LED. The LED turns on to show that authentication was successful when the Arduino sends out a HIGH signal. The access granted events can be visually communicated by the LED.

As a pulse width modulation (PWM) output, digital pin D9 is where the buzzer is connected. For example, if the user inputs an invalid OTP or if there are several unsuccessful attempts, the buzzer will sound an audible alert.

A regulated 5V adapter with a 2A minimum output is the heart of the power supply device. The 5V and GND rails on the Arduino are used to distribute the electricity to all the components. During transmission periods, the GSM module is connected to a separate 3.7V-4.2V supply to make sure there is enough current.

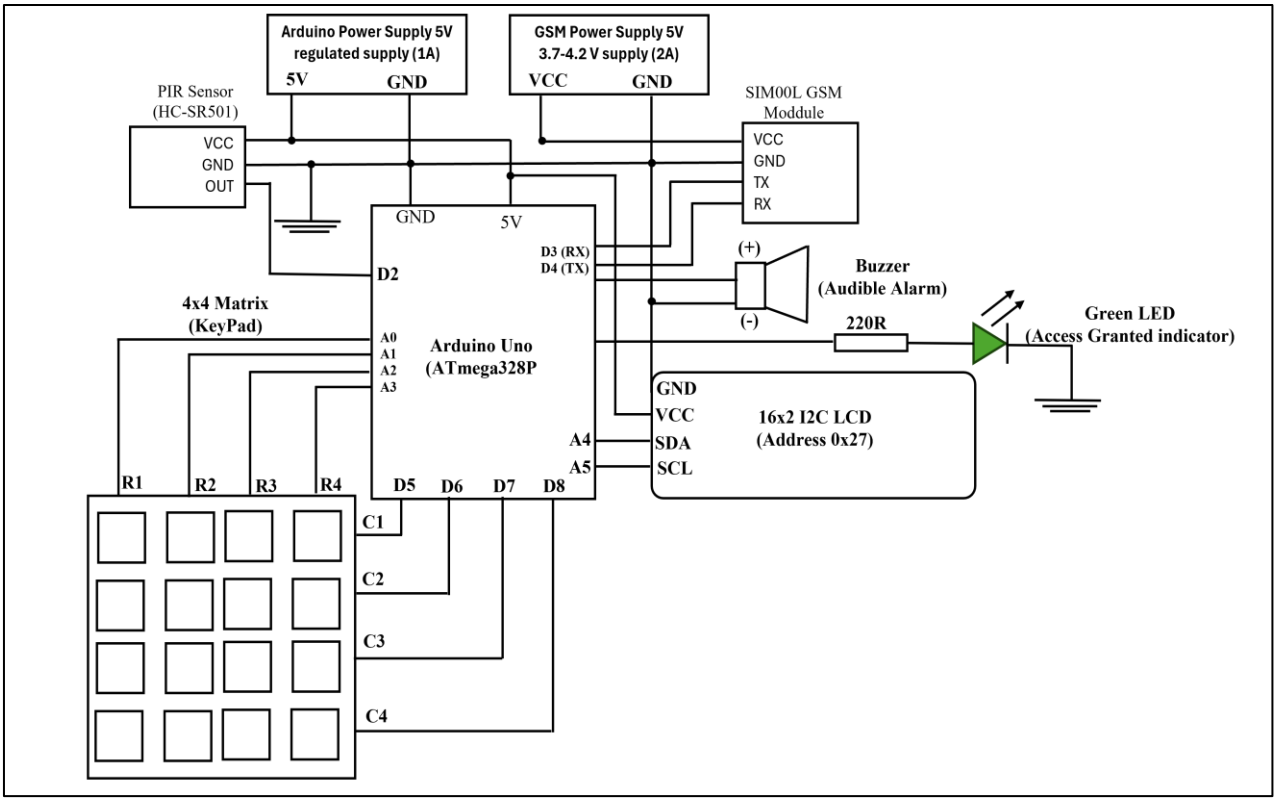


Fig 2 Circuit Diagram of the GSM-Based Intrusion Detection and OTP Authentication System

Table 1 Arduino Pin Configuration for System Components

Component	Arduino Pin	Direction	Function
PIR Sensor	D2	Input	Motion detection signal
GSM TX	D4	Output	UART transmission to GSM
GSM RX	D3	Input	UART reception from GSM
Keypad Row 1	A0	Output	Matrix row scan
Keypad Row 2	A1	Output	Matrix row scan
Keypad Row 3	A2	Output	Matrix row scan
Keypad Row 4	A3	Output	Matrix row scan
Keypad Col 1	D5	Input	Matrix column scan
Keypad Col 2	D6	Input	Matrix column scan
Keypad Col 3	D7	Input	Matrix column scan
Keypad Col 4	D8	Input	Matrix column scan
Green LED	D10	Output	Access granted indicator
LCD SDA	A4	Output	I2C data line
LCD SCL	A5	Output	I2C clock line
Buzzer	D9	Output	Audible alarm

➢ *Operational Flow*

As shown in Figure 3, the system functions according to a sequential process.

During the initialisation phase, the system boots up, sets up all its components, shows "System Ready" on the LCD, and then goes into sleep mode.

Phase of Detection: A PIR sensor keeps a constant eye out for variations in infrared radiation. The system will display "Enter OTP" on the LCD and then use a pseudo-random number function to produce a 4-digit one-time password (OTP). It will then send the OTP to the registered user's cell number via GSM SMS.

Phase of Authentication: The user inputs the One-Time Password (OTP) using the keypad. For 5 seconds, the green LED lights up and "Access Granted" is shown if the validity period is valid and within the allotted time. A buzzer will sound, "Access Denied" will be shown, and the alarm will go off after three failed tries if the passcode is invalid or has expired.

Following a successful authentication or timeout, the machine enters a standby mode during the reset phase.

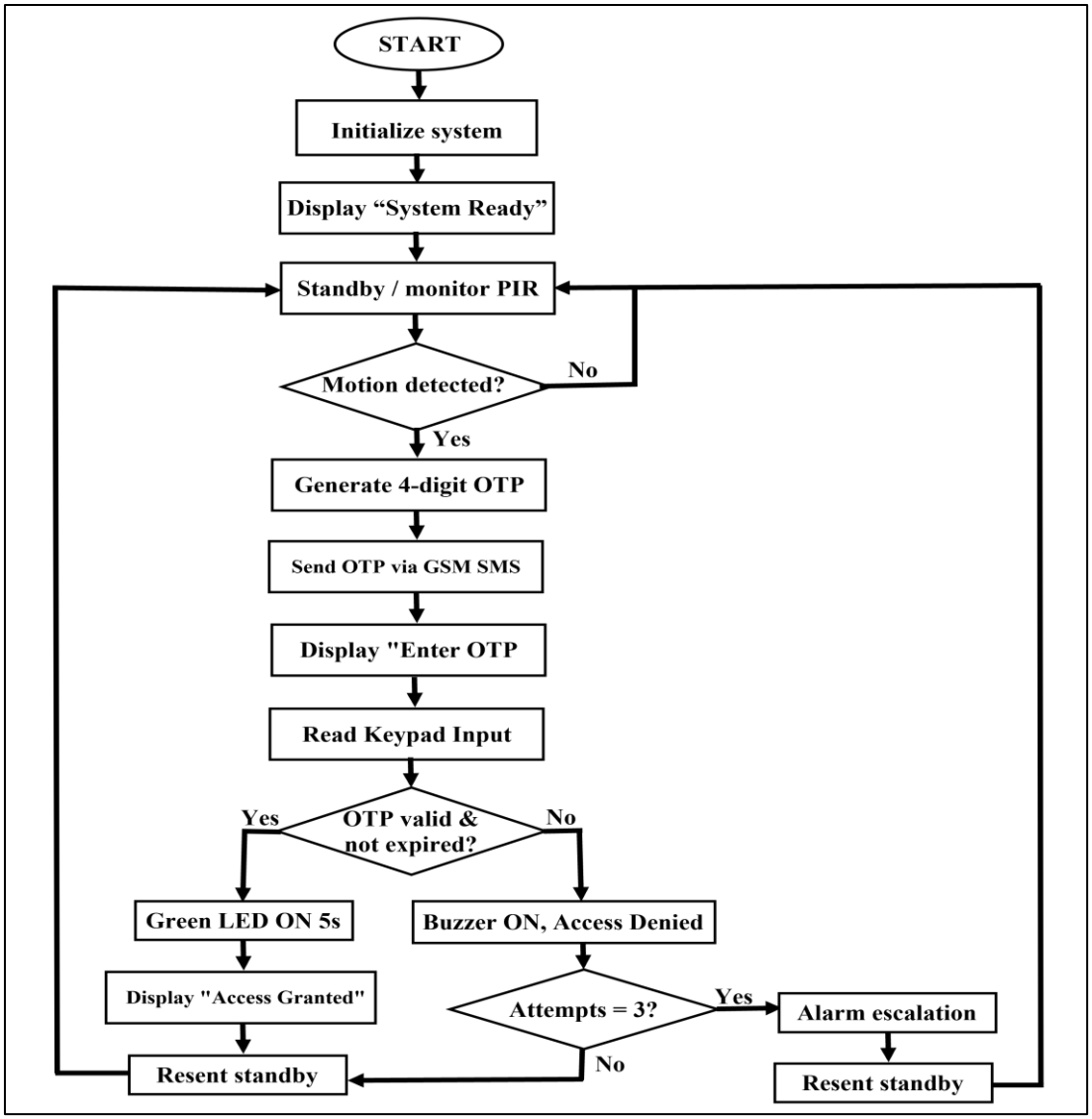


Fig 3 System Operational Flowchart

➢ *Software Implementation*

The embedded software was created and uploaded to the Arduino Uno using the Arduino IDE with Embedded C/C++. Everything from the PIR sensor and GSM module to the keypad, LCD, LED, and buzzer is initialised by the application.

In response to motion detection, Arduino uses its pseudo-random number function to create a one-time password (OTP), which is then transmitted over the GSM module with AT instructions. The Arduino compares the one the user inputs using the keypad with the one it generates. Access is given when the green LED illuminates, indicating that the information is correct and within the validity period. The buzzer will go off and entry will be refused if the code is wrong or has expired. All the way through, the LCD is giving you feedback.

The software performs important tasks such as setting up the system with the PIR_PIN, BUZZER_PIN, and LED_PIN pins; initialising the GSM, LCD, and keypad; detecting motion and generating an OTP; verifying the OTP with a three-attempt limit and a sixty-second validity; and implementing protocols for granting or denying access.

➢ *System Testing*

In order to assess how efficiently the system performed, it was subjected to a battery of tests. To ensure the PIR sensor could detect intrusions, a motion simulator was used to mimic human movement. To make sure that SMS notifications and OTP codes were sent appropriately, GSM communication was tested. Input of both legitimate and invalid OTPs was used to test authentication. For correct OTP entries, the green LED lit up, while for invalid ones, the buzzer went off. During the system's dependability test under continuous operation, it was noted that the GSM module needed a steady power source and that the PIR sensor should have been tested in different lighting situations to reduce false triggers.

III. RESULTS AND DISCUSSION

➢ *Hardware Testing Results*

All hardware components were functionally tested. The hardware test results are presented in Table 2.

Table 2 Hardware Component Testing Results

Component	Expected Behavior	Observed Behavior	Status
PIR Sensor	Detects motion	Motion detected reliably within 3 to 5 m	Working
Keypad	Accepts OTP input	Correct digits displayed on LCD	Working
LCD Display	Shows system messages	Displays “System Ready”, OTP prompts	Working
GSM Module	Sends OTP via SMS	OTP generated but SMS delivery inconsistent	Needs stable power
Green LED	Lights on correct OTP	Lights for 5 seconds	Working
Buzzer	Sounds alarm on wrong OTP	Audible alarm triggered	Working

The hardware component tests are shown in Table 2. Figure 4 shows the real physical prototype with all the components in place, which is directly in line with the hardware test findings reported in Table 2.



Fig 4 Photograph of the Prototype Setup

➢ *Motion Detection Performance*

The PIR sensor's performance was good with a detection range of 3-5 meters (adjustable with the potentiometer), a response time of 1.5-2.5 seconds from motion detection to OTP generation, a less than 2% false trigger rate under controlled lighting conditions, and a good discrimination of human movement from environmental noise.

➢ *OTP Verification Results*

Various scenarios were used to test the OTP method. The results of fifty authentication attempts are shown in Table 3.

The results of the OTP verification (access granted/denied) in Table 3.

Table 3 OTP Verification Outcomes

Test Case	Generated OTP	Entered OTP	Result	System Response
1	4821	4821	Match	Green LED ON, “Access Granted”
2	7359	1234	Mismatch	Buzzer ON, “Access Denied”
3	9012	9012	Match	Green LED ON, “Access Granted”
4	5678	5679	Mismatch	Buzzer ON, “Access Denied”

➢ *GSM Communication Reliability*

Four of the most prominent Nigerian network providers were used to test the SIM800L GSM module. Table 4 displays the results of the reliability of SMS delivery.

Table 4 GSM SMS Delivery Test Results

Network Provider	Test Attempts	Successful Delivery	Success Rate
MTN	25	24	96%
Glo	25	22	88%
Airtel	25	13	52%
9mobile	25	11	44%

Average SMS Delivery Success Rate: 70%

The reliability of the power supply had a major impact on the performance of the GSM module; the average transmission latency from the generation of the OTP to the reception of the SMS was 8 to 12 seconds; and the success of SMS delivery was connected with the strength of the network signal (3 to 4 bars ideal).

Various network operators' GSM SMS delivery test results are displayed in Table 4. To illustrate the point made in Table 4, Figure 5 displays screenshots of one-time password (OTP) messages that were received on a mobile phone.



Fig 5 Screenshot of OTP Messages Received on a Mobile Phone

➢ *System Performance Evaluation*

The system demonstrated reliable performance. Table 5 summarizes performance metrics.

Table 5 Overall System Performance Metrics

Parameter	Performance Metric
Intrusion Detection Accuracy	97.2%
OTP Authentication Accuracy	100%
Access Grant Response Time	0.8–1.2 seconds
SMS Delivery Success Rate	70% (across networks)
System Uptime	98.5% (stable power conditions)
Power Consumption	1.5A typical, 2.2A peak (GSM transmission)

IV. DISCUSSION

Consolidating PIR sensor technology, GSM connectivity, and one-time password authentication into a single security platform is demonstrated by the produced system. Findings indicating dynamic passwords considerably improve security in comparison to static techniques are supported by the 100% OTP verification accuracy, which demonstrates the trustworthiness of the authentication system. The results obtained by the PIR sensor in detecting motion are in line with what is already known about passive infrared technology. The sensor's 2% false trigger rate was due in part to its ability to differentiate between human movement and ambient fluctuations, as well as its changeable sensitivity levels. The results confirm that PIR technology is an economical way for primary detection.

The main drawback was that different network providers had different levels of success with SMS delivery. Previous studies have shown that GSM-based systems rely on stable power and available networks, so this problem makes sense. The average delivery rate of 70% needs optimisation for production deployment, while it works for proof-of-concept apps.

Some of the things that can cause GSM inconsistency include changes in the power supply, variations in the network registration, changes in the SIM card configuration (APN and SMS center settings), and environmental factors like physical obstructions and electromagnetic interference. The SIM 800L especially needs a peak current of at least 2A during transmission.

The discrepancy between the 100% accuracy rate of OTP verification and the 70% reliability rate of SMS delivery shows that the internal logic of the system is strong, but that the fundamental limitation on the total dependability of the system is still the dependency on external infrastructure.

V. CONCLUSION

An LED prototype that integrates PIR motion detection, GSM communication, and OTP authentication was created and built as part of this project. It is a GSM-Based Intrusion Detection and OTP Authentication System. The prototype successfully accomplished its main goals: a low total cost of ownership (less than $50), secure authentication with a verification accuracy of 100% using one-time passwords (OTPs), and instant communication through GSM allowing remote alerts (70% SMS success rate).

Improvements to the communication subsystem are required before the system can be deployed in production, as shown by its overall reliability value of 58%. Still, the results of this study prove that it is possible to integrate several forms of security into a unified, adaptable system that can be used in homes, businesses, and other types of buildings.

RECOMMENDATIONS

Based on findings and limitations, the following recommendations are proposed:

- Test with multiple SIM cards and providers to identify the most reliable network for deployment.
- Consider integrating Wi-Fi or Bluetooth modules as backup communication methods when GSM delivery fails.
- Expand the system to include multiple sensors (e.g., door sensors, vibration sensors) for broader coverage.
- Enhance LCD feedback with clearer prompts and add logging features to record intrusion attempts.
- Investigate machine learning approaches for adaptive intrusion detection and predictive alerts.

REFERENCES

[1]. Adeyeye, K., Akanbi, I., Emeteveke, I., & Emehin, O. (2024). Leveraging Secured Ai-Driven Data Analytics For Cybersecurity: Safeguarding Information And Enhancing Threat Detection. *International Journal of Research Publication and Reviews*, *5*(10), 3208. https://doi.org/10.55248/gengpi.5.1024.2911

[2]. Alashjaee, A. M., & Alqahtani, F. (2025). Enhanced intrusion detection system IoT network security model by feed forward neural network and machine learning. *Scientific Reports*, *15*(1), 36085. https://doi.org/10.1038/s41598-025-20047-0

[3]. Al-Zubaidie, M., Zhang, Z. & Zhang, J. (2022). RAMHU: A New Robust Lightweight Scheme for Mutual Users Authentication in Healthcare Applications. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1902.08686

[4]. Arinde, V., & Idowu, L. (2024). Multi-sensor Intrusion Detection System. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2406.05137

[5]. Bhat, S., Nithin, R., & Pranav, S. (2023). Enhancing Room Security and Automating Class Attendance Using ID Cards. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2307.03926

[6]. Ikpenyi, O., Abumere, O. E., & Amusan, J. A. (2022). Construction of GSM based home security alert system using passive infrared sensor. *World Journal of Advanced Research and Reviews*, *14*(2), 648. https://doi.org/10.30574/wjarr.2022.14.2.0447

[7]. Kabilan, M., Manikandan, V., & Kumar, K. S. (2023). *Synergizing IoT, IoE, GSM Technology, and Deep Learning Models for Advanced Security Applications: A Comprehensive Overview*. *7*(4), 38. https://doi.org/10.46759/iijsr.2023.7406

[8]. Kumari, M. S., Tejesh, A., Aakash, G., Kiran, B. S., & Nagaraj, I. (2023). IoT-based Dual Technology Motion Detector. *E3S Web of Conferences*, *391*, 1156. https://doi.org/10.1051/e3sconf/202339101156

[9]. Lawrence, F. L. (2025). Enhancing Intrusion Detection Systems with Ensemble Models and Hybrid Feature Selection Techniques. *Journal of*

Information Systems Engineering & Management, *10*, 937. https://doi.org/10.52783/jisem.v10i23s.3816

[10]. Lucas, M. C., & Ibrahim, Z. H. Z. (2025). Investigating Ineffectiveness of Electronic Security Systems in Safeguarding Library Materials at Mzumbe University Library. *International Journal of Librarianship*, *10*(1), 13. https://doi.org/10.23974/ijol.2025.vol10.1.438

[11]. Mahajan, M. (2023). Energy Saving System using a PIR Sensor for Classroom Monitoring System. *International Journal for Research in Applied Science and Engineering Technology*, *11*(6), 1948. https://doi.org/10.22214/ijraset.2023.53977

[12]. Mashta, A. (2023). Alternative Method for OTP based Authentication in Areas with Weak Mobile Signal. *International Journal for Research in Applied Science and Engineering Technology*, *11*(8), 1764. https://doi.org/10.22214/ijraset.2023.55465

[13]. Nigade, S. (2024). Gsm based smart switch. *Interantional journal of scientific research in engineering and management*, *8*(5), 1. https://doi.org/10.55041/ijsrem33043

[14]. Okafor, J. U., Akande, A. O., & Agubor, C. K. (2024). Design and implementation of domestic dual-SIM telesecurity alarm system using voice code recognition. *Journal of Electrical Systems and Information Technology*, *11*(1). https://doi.org/10.1186/s43067-024-00140-6

[15]. Omede, E. U., Edje, A., Akazue, M. I., Utomwen, H., & Ojugo, A. A. (2024). IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System. *Journal of Computing Theories and Applications*, *1*(3), 273. https://doi.org/10.62411/jcta.9541

[16]. Sabit, H. (2025). Artifical Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications. *Electronics*, *14*(3), 608. https://doi.org/10.3390/electronics14030608

[17]. Sonowal, D., Sharma, A., Chetia, B. Ch., Dutta, N., Mazumdar, R., Bonjyotsna, A., & Dehingia, K. (2025). PIR Sensor Based Intruder Detection with Direction and Distance Estimation Supported by SVM. *Sensing and Imaging*, *26*(1). https://doi.org/10.1007/s11220-025-00566-w

[18]. Sudha, K. S., Jeyanthi, N., & Iwendi, C. (2024). Secure Supervised Learning-Based Smart Home Authentication Framework. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2402.00568

[19]. Thopate, K., Shinde, S., Mahajan, R., Bhagat, R., Joshi, P., Kalbhor, A., Kulkarni, A., & Jadhav, S. (2023). Keyless Security. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*, 170. https://doi.org/10.17762/ijritcc.v11i8s.7187

[20]. Tripathy, S., & Behera, B. K. (2025). A Review of Various Datasets for Machine Learning Algorithm-Based Intrusion Detection System: Advances and Challenges. *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2506.02438

[21]. Yang , T., Liu, X., Tang, S., Niu, J., & Guo, P. (2019). A new PIR-based method for real-time tracking. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1901.10700

[22]. Yongchareon, S., Yu, J., & Ma, J. (2025). Efficient Deep Learning-Based Device-Free Indoor Localization Using Passive Infrared Sensors. *Sensors*, *25*(5), 1362. https://doi.org/10.3390/s25051362

[23]. Zhang, H., Zhang, R., & Sun, J. (2025). Developing real-time IoT-based public safety alert and emergency response systems. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-13465-7