European Journal of Electrical Engineering and Computer Science
Vol 9 | Issue 6 | December 2025
ISSN 2736-5751

CrossMark

RESEARCH ARTICLE

Development and Analysis of an IoT Security Alarm System Leveraging GSM Communication Networks

Md Babul Akhter[1,*] and Md Mohsin[2]

ABSTRACT

In this paper, a versatile safety and security system is introduced that brings together intrusion, fire, water and gas leakage, environmental, and emergency monitoring in one platform. The setup uses a range of detectors, including Passive Infrared (PIR) motion sensors, magnetic door/window contacts, smoke and heat sensors, gas and water detectors, glass break sensors, and even an SOS emergency feature. Unlike typical systems, it maintains 4G/3G networks and automatically switches to 2G for SMS and call alerts when network signals are weak. The system also allows real-time location tracking and cloud-based control through mobile apps like Blynk or web dashboards that making remote monitoring possible. When any abnormality is detected, SMS alerts are send to three pre-set numbers. If they go unacknowledged, the system places sequential calls until the alert is confirmed and resolved. Integration with fire alarm control panels, electrical fences, and CCTV systems is implemented, extending the system's functionality. The system is supported by a dual backup of solar power and the electrical grid. This dual system remains reliable and operates effectively in both urban and rural areas.

Keywords: GSM-based security system, multi-sensor integration, SMS and call alert mechanism, solar-powered alarm.

Submitted: October 22, 2025
Published: December 05, 2025

10.24018/ejece.2025.9.6.765

[1] *Master's Student, Department of Telecommunications Engineering, World University of Bangladesh, Bangladesh.*
[2] *Assistant Professor, Faculty of Electrical and Electronics, World University of Bangladesh, Bangladesh.*

* ***Corresponding Author:***
e-mail: babul.a.zim@gmail.com

1. Introduction

Safety and security are basic needs in our lives extending from the home to commercial or industrial sectors. With increasing urbanization, environmental hazards, and rising concerns about intrusion and fire incidents, traditional solutions are no longer able to meet the demand. Even so, there is a growing demand for intelligent, integrated and reliable systems capable of simultaneously providing comprehensive protection against multiple threats [1], [2].

Wireless technology has made it easier to remotely monitor and control systems. Among these options, a Global System for Mobile Communication (GSM) is truly dependable. It works worldwide and does not require constant internet access [3]. Studies have shown that the GSM can be used for intrusion detection, fire alarms, and appliance control [4], [5]. However, numerous systems have concentrated on only one type of hazard. They frequently depend only on SMS alerts and have no escalation systems. To solve these problems, the proposed system uses SMS based remote control operation and notification system over the GSM. Real-time location tracking is also performed. It also connects to the cloud using mobile apps and web dashboards, which are presently executed using Blynk. This system uses redundant communication. However, it automatically switches to 2G, if 3G or 4G fails. This keeps alerts and remote controls running all the time.

Recent advancements in the Internet of Things [IoT] and cloud-based services have expanded the possibilities of smart security results. IoT platforms such as Blynk enable real-time monitoring and control through mobile apps and web dashboards [6]. Although IoT-based systems offer flexibility, their reliance on stable 4G or broadband connections restricts their use in rural or low-signal areas [7]. This limitation highlights the need for results that combine IoT capability with GSM redundancy, assuring uninterrupted communication under varying conditions.

Former work on GSM-based home safety and security systems has shown the effectiveness of integrating mobile communication with detector networks [5]. However, these systems lack multi-sensor integration, redundant communication and escalation protocols under weak network conditions, which our study addresses. While previous studies have explored WSNs and IoT for security monitoring [8], [9], comparable approaches generally provide minimum features. In contrast, our design integrates multiple functionalities, offering a more comprehensive and practical result that is suitable for real-world deployment.

Building on an Autonomous and Collaborative Smart Home Security System [10], our design extends its functionality by transferring SMS alerts, calls and notifications via mobile or web apps indeed when the internet is unavailable. In 3G/4G each notification also includes a Google Maps link to indicate the device's current location, providing enhanced real-time monitoring.

The proposed system introduces multifunctional safety and security platform that integrates Passive Infrared (PIR) motion sensors, magnetic door/window sensors, smoke detectors, heat detectors, LPG and refrigerant gas sensors, water leakage sensors, and glass break sensors. An SOS emergency button is also included to allow manual activation of alerts. Unlike earlier designs, our system ensures redundant communication, operating on 4G/3G networks and automatically switches to 2G when internet services are unavailable.

A distinct point of this design is its alert escalation protocol. In the event of an abnormal incident, the system sends SMS cautions to three designated numbers and, if unacknowledged, automatically initiates back-to-back phone calls until the alarm is confirmed and deactivated. This operation ensures that critical alerts can not be ignored, making the system largely dependable compared to conventional designs.

Integration with Fire Alarm Control Panel (FACP), electrical fences, and CCTV enables real-time monitoring and coordinated responses, thereby enhancing overall security and protection. Another important advancement is real-time position tracking, which enables users to cover system activity and positioning remotely. Combined with cloud-based IoT integration, users can view system status, receive event logs, and control operations through mobile applications and web dashboards, regardless of location.

Power Reliability is ensured with a solar-rechargeable battery alongside the grid connection, delivering uninterrupted operation during blackouts. This dual charging system enhances both adaptability and sustainability. The purpose of this study is to design and apply a cost-effective, scalable, and largely dependable safety and security system that bridges the gap between IoT and GSM-based results. The ambition is not only to integrate multiple hazard detection features but also to assure reliability under weak signal conditions and give advanced escalation mechanisms. The significance of this research offering a security result suitable for both urban areas with advanced internet connectivity and rural regions dependent on GSM networks.

In summary, this work advances existing literature by combining multi-sensor integration, GSM redundancy, IoT-based remote monitoring, real-time tracking, and solar-backed operation into a unified platform. The scope of the system extends beyond domestic use to commercial and industrial applications, positioning it as a practical and innovative approach to modern safety and security challenges.

1.1. Literature Review

Research on safety and security systems has extensively explored GSM-based and IoT-based approaches. GSM offers reliable communication in areas with low network signals, whereas IoT enables cloud-based monitoring and control. However, most prior studies focus on single hazards, exhibit limited scalability, or depend on stable internet connections, indicating a need for enhanced multi-sensor integration and communication redundancy.

Vasavi and Akashe [1] implemented a GSM-based security system with IoT applications, demonstrating mobile-based alerts and appliance control. Aditi *et al.* [2] designed an Arduino-based GSM alarm using a PIR sensor, which generated motion alerts but was limited to intrusion detection. Al Rakib *et al.* [5] advanced this field by integrating GSM for home safety against fire and intrusion; however, their system lacked escalation protocols, location tracking or IoT dashboards. Similarly, Recy and Chelsea [9] developed a cost-effective, SMS-based intrusion alarm, yet it addressed only a single hazard.

IoT-driven studies emphasize cloud connectivity and mobile monitoring. Oladunjoye and Okwori [3] introduced an Arduino-based IoT home security system with smartphone access, while K. Vishvakumar [4] proposed a hybrid IoT–GSM model for real-time alerts. Chen and Gupta [8] and Hassan and Khaleeq [10] explored advanced IoT and AI-enabled smart homes, offering intelligent control but requiring robust internet connectivity, which reduces their practicality in rural or low-signal regions.

Other contributions address specific technical concerns. Halak [6] examined secure GSM interfaces for IoT, focusing on communication security. Sahu and Mehta [7] introduced a solar-powered IoT system that ensured backup power but did not resolve redundancy issues in weak network areas.

From this review, it is evident that GSM-based designs ensure reliability without internet dependency, while IoT approaches deliver flexibility and scalability. Nevertheless, existing works do not combine multi-sensor detection, GSM redundancy with SMS and call escalation, IoT/cloud integration, real-time tracking, and renewable energy backup into a single unified system. This gap motivates the proposed work, which aims to deliver a resilient, adaptable, and comprehensive safety and security solution suitable for both urban and rural environments.

2. Method and Design

Our proposed system is a comprehensive multi-sensor platform designed to monitor diverse hazards—including intrusion, fire, gas leaks, water leakage, glass breakage, and SOS emergencies—with commercial-grade compatibility. It offers real-time location tracking and cloud-based IoT integration via mobile apps and a web dashboard. A key advantage is its redundant communication: if internet or 3G/4G fails, it seamlessly switches to 2G GSM to ensure critical SMS and call alerts are always transmitted.

2.1. System Architecture

The overall architecture of the system is based on several subsystems. A block diagram of the system architecture is

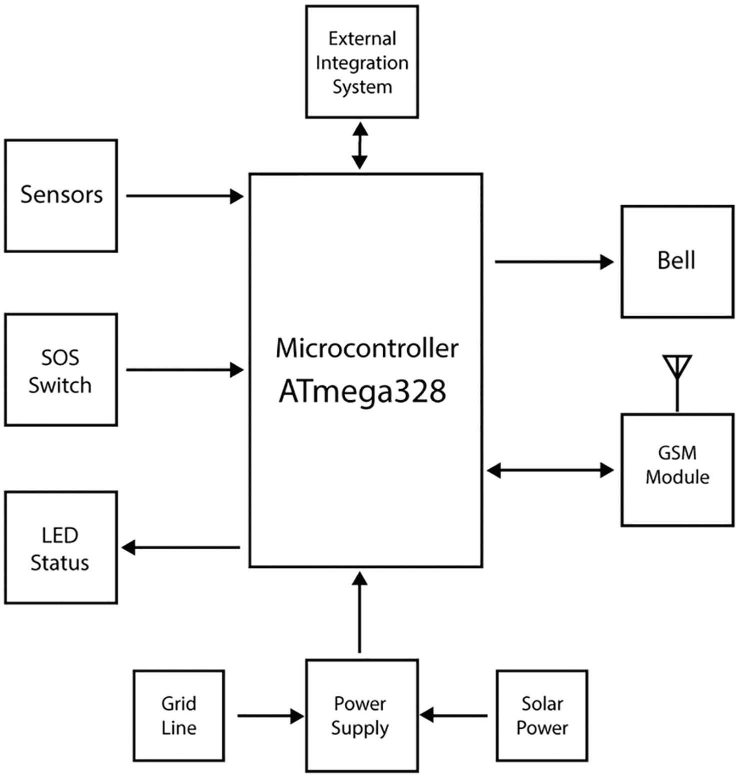

Fig. 1. Block diagram of the system architecture.

shown in Fig. 1. A few subsystems of system architecture are as follows:

1. **Sensing Subsystem—**Responsible for detecting abnormal conditions through multiple types of sensors, like Passive Infrared (PIR) sensors for motion detection, magnetic door/window sensors for intrusion, smoke detectors, heat detectors and multi-detectors for fire hazards, gas leakage sensors (LPG and AC refrigerant), water leakage sensors, glass break sensors for forced entry attempts, an SOS button for manual emergency activation.
2. **Processing and Control Subsystem—**Here, ATMEGA 328 microcontroller that processes signals from the sensors and makes logical decisions. It manages event prioritization, determines escalation steps and activates the communication module.
3. **Communication and Alert Subsystem—**A GSM module that transmits SMS alerts and initiates phone calls. The system first sends SMS notifications to three pre-configured numbers. If no response is received, it automatically calls each number sequentially until the alarm is acknowledged. This escalation protocol ensures that critical events are not overlooked, even under weak network conditions.

2.2. *GSM Communication Flow*

The system is designed to work effectively even under low signal strength and 2G network conditions, where conventional IoT platforms often fail. Its SMS-based command and alert mechanism enables remote activation or deactivation of specific functions and ensures immediate reporting of hazards through text notifications. If these alerts remain unacknowledged, the GSM module automatically escalates the event by initiating sequential phone calls to registered contacts until the alarm is confirmed and deactivated. This dual-alert strategy forms the core novelty of the system, providing reliability beyond typical GSM-based designs [5]. In addition, the system incorporates real-time location tracking for enhanced situational awareness and integrates with cloud-based IoT platforms such as Blynk and web dashboards, enabling users to monitor and control the system from anywhere. Most importantly, it introduces redundant communication, seamlessly switching between 3G/4G internet-based IoT functions and 2G SMS/call services under weak signal conditions. These combined innovations make the system highly resilient, scalable, and distinct from conventional solutions.

2.3. *Integration with Commercial Systems*

To enhance scalability, the system integrates with Fire Alarm Control Panels (FACP), electrical fences, and CCTV surveillance. This interoperability enables fire detection, intrusion alerts from fence tampering, and notifications from camera activity, extending its use beyond households to commercial and industrial environments.

2.4. *Power Backup and Reliability*

Trustability in nonstop operation is achieved by integrating a rechargeable backup battery system. The battery can be charged from either the grid force or solar panels, ensuring continued service during power outages. This point is especially useful in regions with unreliable electricity force, making the system tone- sufficient and sustainable.

2.5. *System Uniqueness*

The proposed system incorporates several innovations that distinguish it from conventional safety and security designs. It integrates multiple sensors—including intrusion, fire, gas, water, and glass-break detectors—into a unified platform, eliminating the need for separate systems. Its dual escalation protocol, combining SMS alerts with sequential phone calls, ensures that critical events are promptly acknowledged. The system's redundant communication allows reliable operation under varying network conditions, functioning via 3G/4G IoT monitoring and automatically switching to 2G SMS and call alerts during internet failure. Cloud connectivity through Blynk and web dashboards enables real-time monitoring, remote control, and location tracking. Compatibility with Fire Alarm Control Panels (FACP), electrical fences, and CCTV extends its application beyond households to industrial settings. Additionally, the solar-powered backup enhances reliability during power interruptions. These combined features make the system intelligent, self-sustaining, and dependable across both urban and rural environments.

3. Hardware Implementation

The hardware implementation of the proposed system combines detectors, a microcontroller platform, a GSM module and a power backup unit to achieve dependable monitoring and communication. Each element was precisely named to insure comity, continuity and ease of integration.

In the Fig. 2 schematic of the main control circuit for the proposed system, showing a microcontroller ATmega328P, which processes detector signals and executes control logic. The ATmega328P microcontroller (U1) acts as the central controller. It communicates with the SIM7600E GSM module through its TX and RX lines for sending and receiving messages or control commands. A crystal oscillator (Y2) and capacitors C1, C2 ensure accurate clock timing for the microcontroller's operation. The sensor input section (J3 and K2) allows the system to monitor external sensors. The microcontroller reads the signal through the Sens pin. The output control section (J2 and K1) uses a relay controlled by transistor Q1 and diode D2 for switching external loads or alarms. BZ1 is a buzzer, activated through BUZ_CTRL, for audible alerts. Resistors R1–R5 provide current limiting and biasing where necessary, and C5 helps filter noise in the control signal. The power supply section uses U2 (voltage regulator) with capacitors C3 and C4 to provide stable DC voltage to the microcontroller and other components. D1 and D3 protect against reverse polarity and voltage surges.

To describe the system in more detail, it is divided into the following functional units:

3.1. *Sensor Units*

Intrusion Sensors: Passive Infrared (PIR) Sensors detect human movement by measuring infrared radiation changes. Magnetic Door/Window Sensors monitor entry points. When the magnetic contact is broken, the sensor triggers an intrusion event.

Fire Detection Commercial Sensors: Smoke Detectors detect the presence of smoke particles. Heat Detectors sense rapid temperature increases. Multi-Detectors combine smoke and heat sensing for higher accuracy.

Environmental Hazard Sensors: LPG Gas Detectors detect flammable gas leaks in kitchens and storage areas. Air Conditioner Gas Leakage Sensors monitor refrigerant leaks that may pose safety risks. Water Leakage Sensors detect flooding or pipeline failures. Glass Break Sensors detect vibrations or sharp frequency changes caused by breaking glass.

Emergency Sensor: SOS Button enables manual triggering of an alert during emergencies, ensuring human intervention is possible even if automatic sensors fail.

3.2. *Processing Unit*

The control logic of the system is managed by an ATmega328P microcontroller, which receives input signals from various sensors, executes decision-making algorithms for hazard classification, controls relays for alarms and external devices, and communicates with the GSM module to send alerts or receive SMS commands. The microcontroller board supports both digital and analog inputs, enabling seamless integration of multiple sensor types into the system.

3.3. *GSM Communication Module*

The system employs a SIM7600E GSM module for mobile communication, enabling reliable and versatile interaction with users. It provides immediate SMS alerts to up to three registered phone numbers and, if these alerts remain unacknowledged, automatically escalates the event by initiating sequential phone calls until confirmation is received. In addition, users can remotely control or reset the system by sending SMS commands, ensuring continuous functionality even in their absence. Communication is primarily managed through 3G/4G networks for IoT-based monitoring; however, in cases of internet failure, the system automatically switches to 2G SMS and call alerts. This redundancy allows the mechanism to remain operational under weak signal conditions, making it particularly reliable for rural and remote areas where conventional IoT systems often fail [5].

3.4. *Alarm and Notification Units*

- **Buzzer/Siren:** Activated locally during abnormal events to provide immediate onsite alerts.
- **Relay Outputs:** Used to trigger external devices such as electrical fences or fire alarm control panels (FACP).
- **CCTV Linkage:** Integration with cameras allows real-time event correlation with video feeds.

3.5. *Power Supply and Backup*

The system is powered by a 220V AC supply converted through a regulated adapter. To ensure continuous operation, a 12V rechargeable lithium-ion battery pack is integrated. The battery can be charged via direct grid supply or solar panels, providing renewable backup power.

In the circuit shown in Fig. 3 operates using both AC mains and solar power as input sources. The transformer

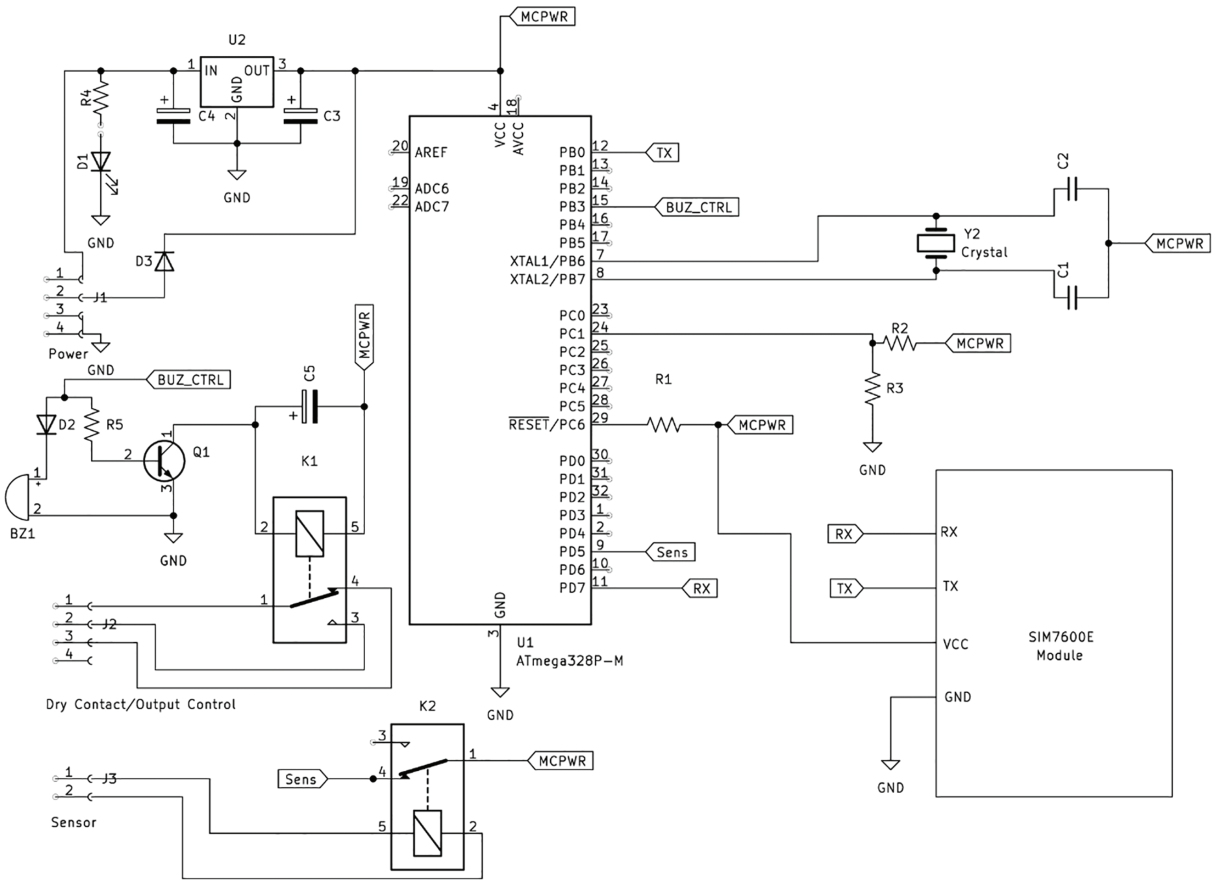

Fig. 2. Schematic circuit diagram of main control system.

and bridge rectifier (D6) convert AC mains into unregulated DC, while the solar panel (J2) provides DC power for charging. The LM317 voltage regulator (U1) ensures controlled charging of the battery, with RV1 allowing adjustment of the charging voltage. To handle higher current, the BD139 transistor (Q1) acts as a current booster, and protection is provided by the Zener diode (D4) for overvoltage and diodes D3 and D7 for preventing reverse current flow. The rechargeable battery (BT1) serves as a backup power source, while the relay (K1) automatically switches the load between solar, battery, and mains depending on availability. The 2N3904 transistor (Q2) controls the relay based on voltage sensing through Zener diode D1, and capacitors C1 and C2 stabilize relay operation. Finally, LEDs D2 and D5 provide visual indication of charging and power status, ensuring easy monitoring of the system's operation.

The seeing subsystem includes intrusion sensors such as PIR motion sensors and magnetic door contacts, environmental hazard sensors including smoke sensors, heat sensors, LPG and AC gas leakage detectors, water leakage sensors, and glass break sensors, along with an emergency SOS push button. Each of these detectors is interfaced with the ATmega328P through digital or analog legs. The microcontroller constantly monitors their outputs and triggers the alarm sequence whenever abnormal exertion is detected. Fig. 4. Internal hardware of the system showing electronic components, battery, buzzer, commercial fire and heat sensors, and SOS button.

This system, built with an ATmega328P and a SIM7600E GSM module, delivers reliable SMS and call alerts. When an abnormality occurs, it immediately notifies three registered numbers and escalates to calls if no response is received. It also offers real-time location tracking and cloud integration via Blynk and web dashboards. Best of all, if 3G/4G connectivity fails, it seamlessly switches to 2G, ensuring notifications continue and remote control remains active via SMS. Relay modules and a siren/ buzzer used for local alerts and external interfacing. Relays allow connection with high-power devices such as Fire Alarm Control Panels (FACP), electrical fence and CCTV systems, extending the system's applications beyond household use to industrial and commercial environments. A 12V rechargeable battery with automatic charging capability from both the grid supply and a solar panel was used. A regulated 5V output powers the ATmega328P and sensors, while the GSM module is supplied through a dedicated regulator to ensure stable operation. This dual charging mechanism provides continued operation during power outages, increasing system resilience.

This hardware design combines multi-sensor integration, GSM communication, relay interfacing, and solar-backed power supply into a compact, cost-effective platform.

3.6. *Hardware Integration*

All modules are interconnected on a control board. The microcontroller receives signals from sensors, processes them, and transmits commands to the GSM module. In

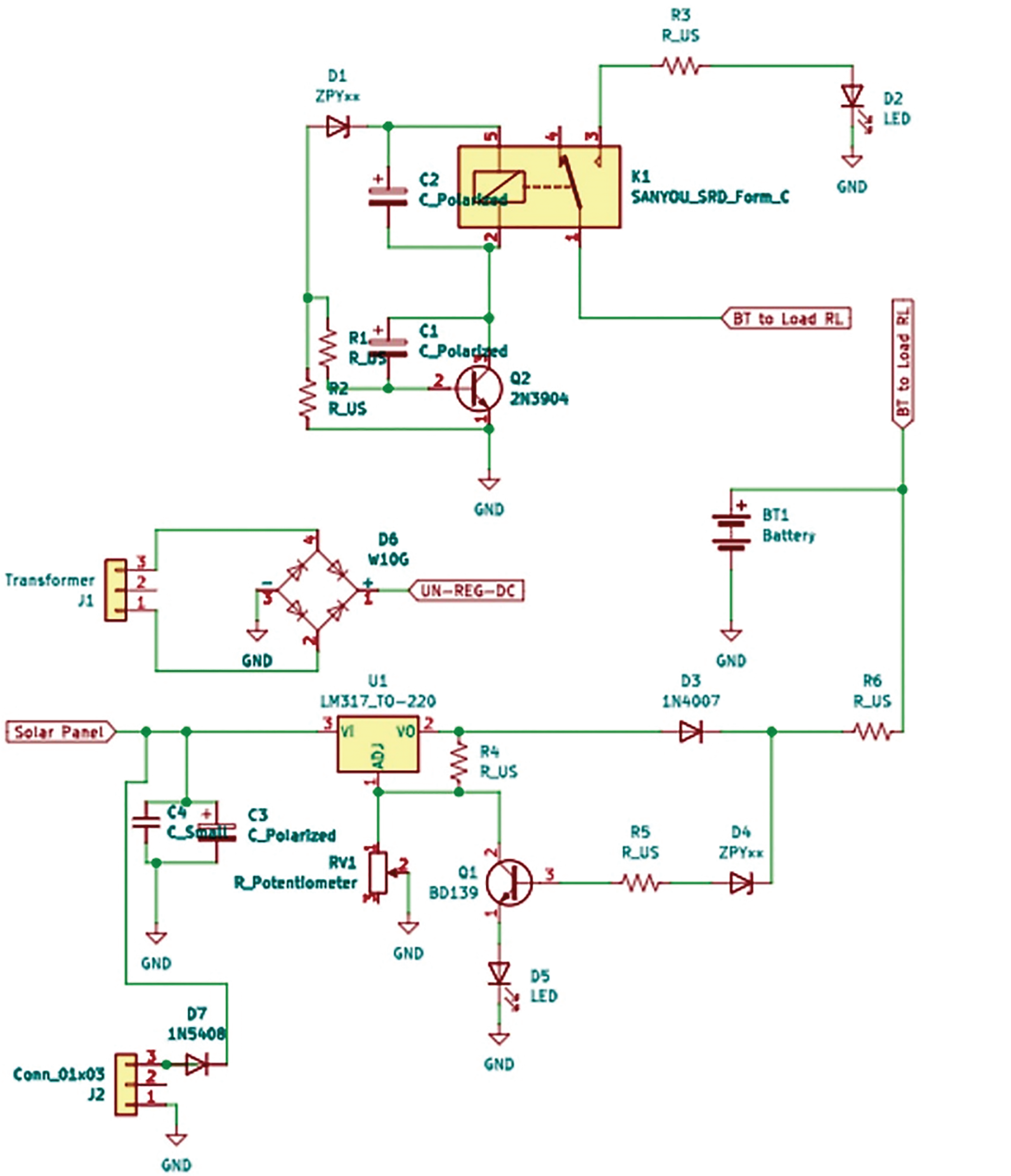

Fig. 3. Schematic circuit diagram of power supply and backup system.

parallel, relays connect external devices such as sirens, FACP and CCTV. Fig. 5 shows the actual hardware setup, where the project module is physically connected to the Fire Alarm Control Panel (FACP) through interface circuits, ensuring proper signal communication and system operation.

4. Results

The prototype system was tested under multiple scenarios to validate its performance. Each test focused on a specific hazard or event, ensuring that the sensors, GSM communication module and backup systems responded as designed.

During testing, a simple button phone was used to verify the alert system. The system automatically generated sequential call alerts and SMS notifications when an anomaly was detected, if they were not acknowledged. This demonstrated that even with low-end mobile devices, the system's communication process is dependable. Fig. 6 Validation of the alert mechanism using a basic button phone shows SMS and sequential call notifications activated by unusual events.

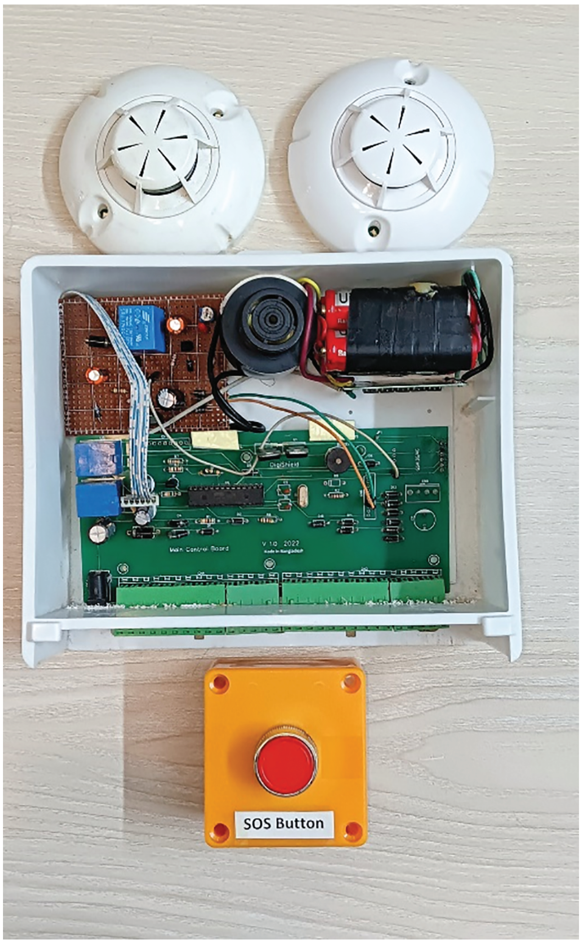

Fig. 4. Internal circuitry of the project.

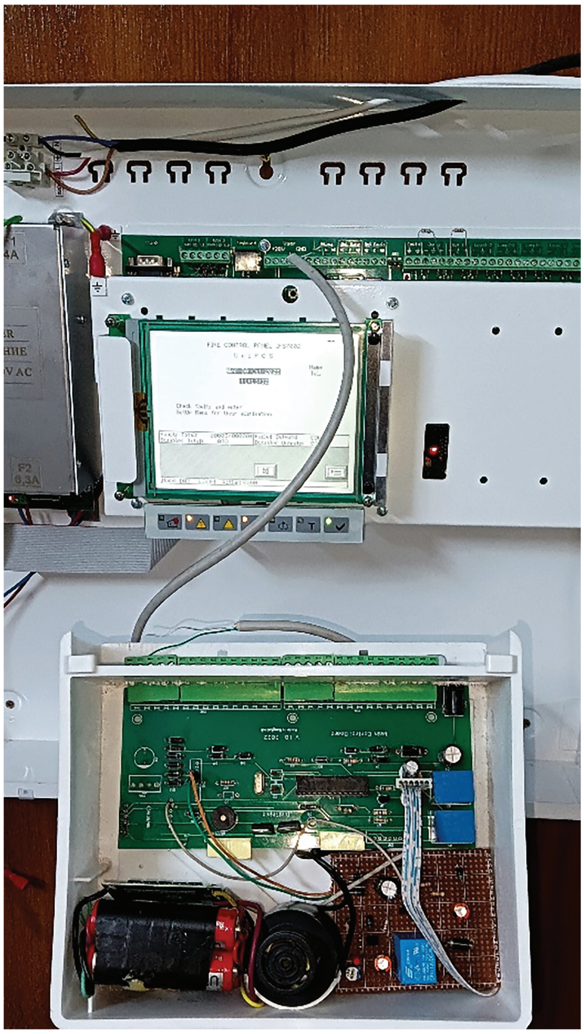

Fig. 5. Hardware integration with Fire Alarm Control Panel (FACP).

4.1. Intrusion Detection Test

The system was configured with a PIR motion detector and magnetic door detector. When motion was detected or the magnetic contact was broken, the microcontroller incontinently actuated the buzzer and touched off the GSM module. An SMS was transferred to three registered numbers within 3–5 seconds of detection. However, the system successfully initiated successional phone calls until the alert was verified, If no acknowledgment was entered. This escalation protocol proved to be a dependable enhancement over traditional single-alert systems.

4.2. Fire Detection Test

Commercial smoke and heat detectors were connected to the system. During simulation with controlled smoke release, the detector output triggered both a local siren and GSM alerts. In case of temperature rise beyond a threshold, the heat detector activated and followed the same SMS and call sequence. The system also successfully relayed signals to a Fire Alarm Control Panel (FACP), confirming its compatibility with commercial fire protection infrastructure.

4.3. Gas and Environmental Hazard Test

To test gas leakage detection, LPG gas was released in a controlled environment near the LPG gas sensor. The sensor output was immediately recognized by the controller, which activated local and remote alerts. Similarly, a water leakage sensor placed at floor level successfully detected minor flooding conditions, triggering alarms and SMS notifications. For air conditioner gas leakage simulation, the refrigerant sensor detected abnormal conditions, showing its potential to prevent long-term health risks and equipment damage.

4.4. Glass Break and SOS Test

The glass break sensor was tested by producing vibration and high-frequency sounds similar to window breaking. The system detected the disturbance within milliseconds and issued alerts. The SOS button was tested under manual operation by pressing the button sent immediate emergency alerts to all registered numbers without delay. This ensures that users have a manual override option in case sensors fail to detect certain situations.

4.5. GSM Communication Reliability

The system's GSM communication was tested under weak network conditions with signal strength equivalent to 2G coverage. Despite low signal, SMS messages were successfully delivered within 5–8 seconds, and sequential calls were initiated without interruption. This validates the system's suitability for rural and low-connectivity areas.

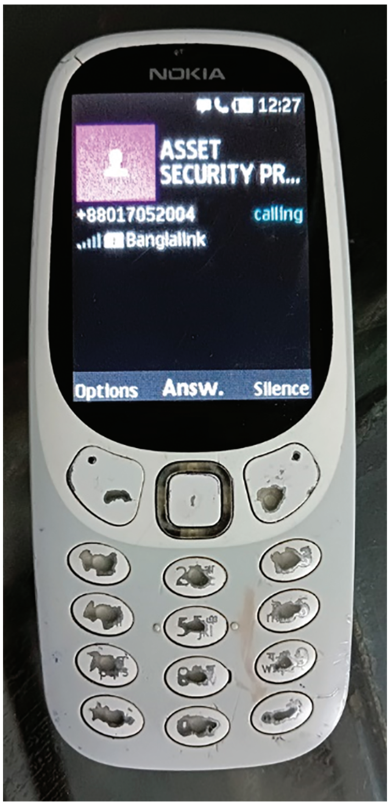

Fig. 6. Alert verification via basic phone using SMS and call notifications.

4.6. *Power Backup Test*

The system was operated on grid supply and later switched to the solar-charged backup battery. During testing, the backup supported continuous operation for more than 8 hours under normal load conditions. Automatic switchover ensured uninterrupted monitoring during simulated power outages, confirming the reliability of the dual power design.

4.7. *Mobile Apps (BLynk) and Mobile Dashboard Test*

The ATmega328P-based system was tested for real-time alert delivery via the Blynk mobile app and web dashboard over 3G/4G networks. Upon detecting any abnormality, sensor data were processed immediately, triggering notifications on the mobile interface. Experimental results showed that alerts appeared within 3–5 seconds, confirming the system's responsiveness and reliability in delivering IoT-based notifications through mobile and web platforms. As shown in Fig. 7, the Blynk app interface allows users to acknowledge and reset alarms and monitor battery voltage in real time, enabling efficient remote monitoring and control.

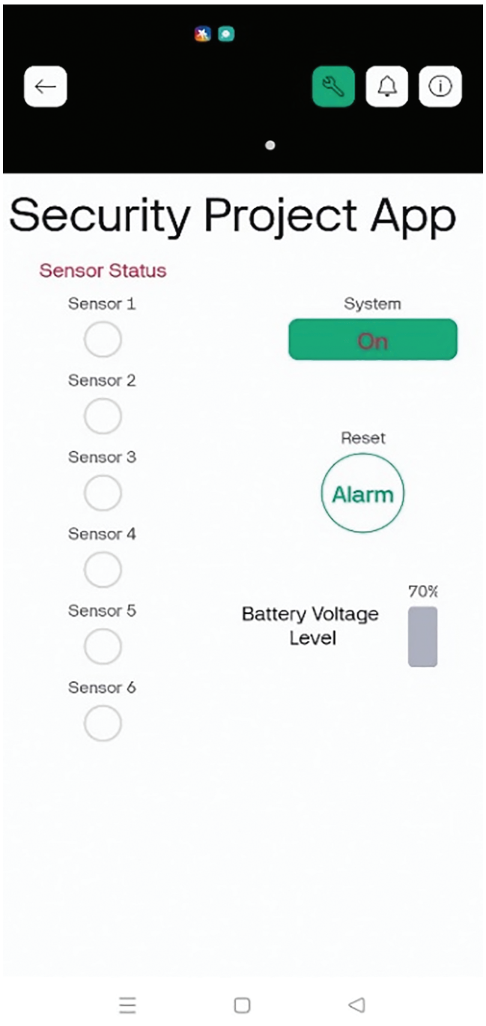

Fig. 7. Blynk app interface showing real-time IoT alerts.

5. Discussion

The experimental results show that the proposed GSM-based safety and security system works effectively by combining multiple sensors and communication methods into a single platform. Unlike traditional systems that focus on a single function, this design can discover fire, gas leakage, water leakage, glass breakage, and intrusion simultaneously, while also handing an SOS emergency option. This integrated approach improves overall safety and reduces the chance of missing critical hazards.

The system's escalation protocol, which sends an SMS first and then repeated phone calls until acknowledgment, ensures alerts are reliably delivered even in areas with weak 2G coverage. Its ability to connect with Fire Alarm Control Panels, electrical fences, and CCTV systems makes it scalable for both homes and businesses.

Additional features such as real-time location tracking, cloud-based dashboards via Blynk, and backup communication switching to 2G when 3G/4G fails enhance the system's adaptability. The solar-powered backup battery ensures continuous operation during power outages, improving reliability and sustainability.

6. Conclusion

This paper presents a reliable and scalable GSM-based safety and security system that can detect multiple hazards and deliver alerts consistently. The experiments confirm that the system is cost-effective, adaptable, and practical for real-life use. Future improvements may include cloud-based data logging, AI-assisted event analysis to make the system smarter and easier to use. Overall, this design offers a practical solution to key safety challenges in modern homes and commercial spaces.

Conflict of Interest

The authors declare that they have no commercial or financial relationships that could be construed as a potential conflict of interest in relation to the work reported in this paper.

References

[1] Vasavi S, Akashe S. Implementation of GSM based security system with IoT applications [Internet]. *ResearchGate*. 2017 Jun [cited 2025 Nov 14]. Available from: https://www.researchgate.net/publication/317413875_Implementation_of_GSM_Based_Security_System_with_IOT_Applications.

[2] Aditi A, Debashis D, Sumendu S. GSM based home security alarm system using Arduino [Internet]. *ResearchGate*. 2023 Aug [cited 2025 Nov 14]. Available from: https://www.researchgate.net/publication/373186416_GSM_Based_Home_Security_Alarm_System_Using_Arduino_Using_Mobile_Call.

[3] Oladunjoye O, Okwori O. Smart home security using Arduino-based Internet of Things [Internet]. *World J Adv Res Rev*. 2024 Jun [cited 2025 Nov 14]. Available from: https://wjarr.com/sites/default/files/WJARR-2023-2000.pdf.

[4] Vishvakumar K. Real-time IoT security alert and monitoring (GSM-based) [Internet]. *Int Res J Moderniz Eng Technol Sci*. 2025 Jun [cited 2025 Nov 14]. Available from: https://www.irjmets.com/upload_newfiles/irjmets70600077829/paper_file/irjmets70600077829.pdf.

[5] Al Rakib MA, Rahman MM, Rana MS, Islam MS, Abbas FI. GSM based home safety and security system. *Eur J Eng Technol Res*. 2021 Sep;6(6):69–73. doi: 10.24018/ejers.2021.6.6.2580.

[6] Halak B. Secure communication interface design for IoT applications using the GSM network [Internet]. *ResearchGate*. 2016 May [cited 2025 Nov 14]. Available from: https://www.researchgate.net/publication/314293661_Secure_communication_interface_design_for_IoT_applications_using_the_GSM_network.

[7] Sahu PK, Mehta R. An IoT-based solar integrated home security system [Internet]. *Int J Adv Eng Res Sci*. 2018 Jan;5(1):28–33.

[8] Rathore Y. S., Kumar S. Advanced IoT-based smart home security system: design, implementation, and future trends [Internet]. *International Journal on Science and Technology (IJSAT)*. 2025 May;16(2):1–14.

[9] Anne R, Chelsea C. Intrusion alarm system for smart home protection and security using SMS. *IEOM Society International Conference Proceedings*, pp. 379–85, Istanbul, 2022 Jul [Internet]. Available from: https://ieomsociety.org/proceedings/2022istanbul/379.pdf.

[10] Hassan H, Khaleeq K. Autonomous and collaborative smart home security system (ACSHSS) [Internet]. arXiv; 2023 Sep [cited 2025 Nov 14]. Available from: https://arxiv.org/abs/2309.02899.