



GSM-Based Smart Security and Monitoring System for Residential Applications

Yannis Zambrano-Ortiz

Department of Electrical and Computer Engineering, Kavir Polytechnic University of Technology, Iran
yannis.zambrano.ortiz@kput-ir.net

Peer Review Information

Submission: 22 Jan 2019
Revision: 17 Feb 2019
Acceptance: 27 March 2019

Keywords

*GSM, Smart home security,
Residential monitoring,
Arduino, SMS alert*

Abstract

Residential security systems increasingly combine embedded sensing, mobile communication, and automated alerting to provide continuous protection when occupants are away from home. This methodology paper proposes a GSM-based smart security and monitoring architecture in which passive infrared motion, door-contact, smoke/gas, and temperature sensors are integrated with an Arduino-class microcontroller and a GSM modem. The controller evaluates sensor events, activates a local alarm, and transmits event-specific Short Message Service (SMS) notifications to an authorized mobile number. The methodology emphasizes low cost, stand-alone operation, cellular coverage, simple authentication, and measurable performance indicators such as detection accuracy, false-alarm rate, SMS delivery latency, and recovery after power or network interruption. A structured prototype-validation procedure is defined for intrusion, fire/smoke, gas leakage, and abnormal-temperature scenarios. The proposed approach is grounded in GSM/GPRS and smart-home security studies published up to 2019. The resulting framework is suitable for residential applications where reliable remote notification is required without continuous dependence on broadband Internet connectivity.

Introduction

Home security has moved from purely local alarms toward connected systems that can detect abnormal events and inform residents remotely. The practical requirement is straightforward: a security system should sense an intrusion or hazard, determine whether the event requires action, alert people inside the residence, and notify an authorized user who may be many kilometers away. Cellular communication is attractive for this purpose because it does not require the homeowner to maintain a continuously operating personal computer or local Internet gateway. Early GSM/GPRS research demonstrated that a wireless home network could combine door, infrared, and fire-alarm nodes with a GSM/GPRS gateway while maintaining relatively low cost and power

consumption (Zhao & Ye, 2008). This established the basic architecture followed by many later residential monitoring systems.

GSM-based automation then developed from simple remote switching to two-way status reporting and integrated security. Teymourzadeh et al. (2013) showed that SMS commands, serial communication, and AT commands could be used to control household loads and return device status through a GSM modem. In parallel, researchers began integrating microcontrollers with motion, door, and alarm circuits. Sharma et al. (2014) connected GSM security notifications with an Android interface, while Aggarwal et al. (2014) presented an automated home-security implementation using GSM, sensors, and a microcontroller. These studies indicate that GSM

can serve not only as an alert channel but also as a remote-control and acknowledgement channel. For residential security, the most useful design is not a single-purpose burglar alarm but a multi-hazard monitoring node. A modern household may need simultaneous monitoring of unauthorized movement, forced door entry, smoke, combustible gas, and abnormal temperature. Hasan et al. (2015) combined GSM with microcontroller-based access and alarm functions, whereas Rahman et al. (2015) included fire detection, temperature sensing, motion detection, lock functions, and load control in a GSM-based architecture. Later work extended the same idea toward Internet-of-Things integration and multi-interface control (Kumar & Akashe, 2017; Karim & Awl, 2018). By 2019, low-cost platforms such as Arduino and Raspberry Pi were widely used in smart-home security research, enabling modular sensor integration and remote notification (Hoque & Davidson, 2019).

Despite this progress, three practical issues remain important. First, security notifications must still reach the homeowner when local Wi-Fi or broadband service is unavailable. Second, simple sensor triggers can produce nuisance alarms unless the decision logic includes timing, thresholding, arming status, and acknowledgement. Third, a methodology paper should specify how performance is evaluated rather than merely presenting a circuit. The present study therefore develops a reproducible methodology for a GSM-based smart residential security and monitoring system. The objectives are to: (i) design a modular sensing and control architecture; (ii) define event-processing and SMS-notification logic; (iii) specify authentication and fail-safe behavior; and (iv) evaluate the system using detection success, false-alarm behavior, notification latency, and recovery tests. References are restricted to work published no later than 2019, as required for the scope of this paper.

Literature Review

The literature shows a clear progression from gateway-oriented GSM/GPRS systems toward compact microcontroller and Arduino implementations. Zhao and Ye (2008) used separate wireless security nodes and a GSM/GPRS gateway, demonstrating the feasibility of wide-area alerting. Teymourzadeh et al. (2013) focused on SMS-based automation

and reported high command execution accuracy for controlled loads. Their work is important because it formalized the use of AT commands, serial interfaces, and two-way messaging in a home environment.

Research published in 2014 broadened the security function. Sharma et al. (2014) used an Android interface to interpret intrusion messages and send an acknowledgement that could activate a remote alarm. Aggarwal et al. (2014) designed an automated GSM home-security system around a microcontroller and sensors, while Islam (2014) demonstrated a PIC18F452-based system for door/window monitoring and resident identification. Although Islam's design was not centered on GSM, it is relevant to access-state logic and shows why communication should be integrated with the local security controller rather than treated as the only protection layer.

In 2015, Hasan et al. (2015) combined GSM alerts with keypad/Bluetooth access and local indicators, demonstrating a practical multi-interface security system. Rahman et al. (2015) went further by combining motion, fire, temperature, locking, and load-control functions. These studies support a multi-sensor architecture because different hazards require different sensing mechanisms and response priorities. They also show that a local buzzer remains necessary even when remote SMS alerting is available.

The subsequent literature shifted toward connected smart-home ecosystems. Kumar and Akashe (2017) integrated GSM security with IoT concepts and a PIR sensor, and Karim and Awl (2018) implemented a GSM-network smart-home design capable of reporting intrusion, gas leakage, and fire while also supporting appliance control. In 2019, Banerjee et al. (2019) added self-generated password protection to an Arduino UNO and GSM real-time security system. Munawir et al. (2019) combined Wi-Fi and GSM for motion detection and reported short SMS notification times across tested PIR distances. Hoque and Davidson (2019) provided a broader IoT smart-home security architecture using low-cost hardware and multiple sensing layers. Collectively, these studies justify a hybrid philosophy: sensing and decision making should remain local, while GSM provides robust remote notification and optional command/acknowledgement.

Table 1. Representative literature on GSM and smart-home security (up to 2019)

Study	Platform / link	Main security function	Key implication
Zhao & Ye (2008)	GSM/GPRS gateway + WSN	Door, infrared and fire alarm nodes	Cellular gateway supports rapid remote alerting

Teymourzadeh et al. (2013)	PIC + GSM/SMS	Remote control and device-status feedback	AT-command SMS control is feasible and accurate
Hasan et al. (2015)	MCU + GSM + keypad/Bluetooth	Door/window protection and user alert	Multiple local and remote interfaces improve usability
Rahman et al. (2015)	MCU + GSM	Motion, fire, temperature, lock and load control	Multi-hazard sensing suits residential monitoring
Karim & Awl (2018)	Arduino + GSM + sensors	Intrusion, gas leakage, fire and appliance control	GSM can combine safety, security and automation
Banerjee et al. (2019)	Arduino UNO + GSM + PIR	Motion detection with changing password	Authentication can reduce unauthorized access
Munawir et al. (2019)	Arduino + Wi-Fi + GSM	PIR motion detection and SMS notification	GSM is useful as a direct remote notification path
Hoque & Davidson (2019)	Arduino/Raspberry Pi + IoT	Multi-sensor smart-home security	Low-cost modular architectures support expansion

Methodology

1. System Architecture and Hardware

This study uses a design-and-validation methodology. The proposed system is organized into five functional layers: sensing, local processing, communication, alert/actuation, and user interaction. The sensing layer includes a PIR motion sensor for human movement, a magnetic reed/door contact for forced entry, an MQ-series smoke/gas sensor for combustible gas or smoke, and a temperature sensor for abnormal thermal

conditions. The local processing layer is implemented on an Arduino Uno or equivalent ATmega328P platform. This choice is consistent with low-cost smart-security systems reported before 2019 (Banerjee et al., 2019; Hoque & Davidson, 2019). The communication layer uses a SIM900/SIM800-class GSM module controlled through serial AT commands. Local outputs include a buzzer, status LED/LCD, and a relay output that may be connected to an emergency light, ventilation fan, or door-lock actuator.

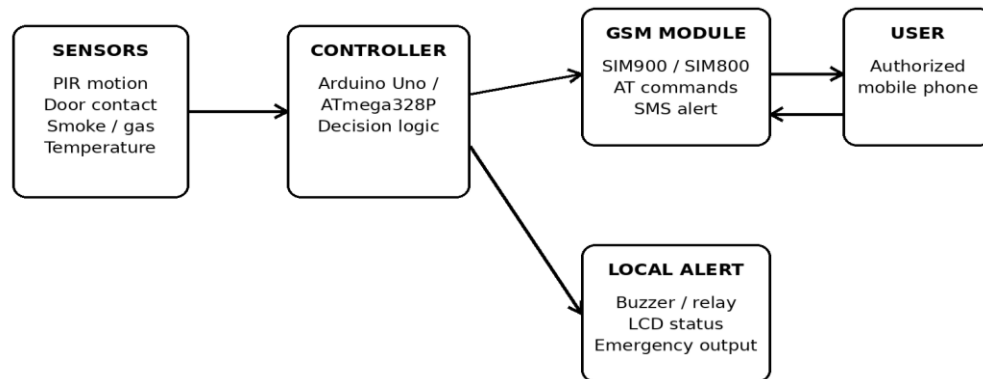


Figure 1. Proposed GSM-based residential security and monitoring architecture.

2. Event-Processing Logic

The controller operates as a finite-state process with four principal states: DISARMED, ARMED, ALERT-PENDING, and ALARM. In the DISARMED state, hazard sensors such as smoke/gas and high temperature remain active, but intrusion sensors are ignored or logged. When an authorized user arms the system, PIR and door-contact events become active. A motion or door event enters ALERT-PENDING, where a short confirmation interval filters transient triggers. If the event remains valid, the controller enters ALARM, activates the buzzer, records the event type, and sends an SMS. Fire/gas events bypass the

intrusion confirmation delay because their safety priority is higher. This priority logic prevents a security feature from delaying a life-safety alert. GSM communication is initialized at startup by checking module presence, SIM readiness, signal registration, and SMS text mode. Typical commands include AT, AT+CPIN?, AT+CREG?, AT+CMGF=1, and the appropriate message-send command. The recipient number is stored in protected program memory or non-volatile memory. Incoming commands are accepted only from authorized numbers. A minimal command set may include ARM, DISARM, STATUS, and RESET. For higher security, a short PIN token can

be appended to commands. The controller rejects malformed or unauthorized messages and does not expose sensor configuration through unrestricted SMS. This approach follows the two-way GSM control concept demonstrated in earlier GSM automation work while adding explicit authorization rules (Teymourzadeh et al., 2013; Karim & Awl, 2018).

Sensor calibration is performed before system testing. The PIR sensor is allowed to stabilize after power-up and is tested at several distances and approach angles. The door contact is verified for both normal opening and forced separation. The smoke/gas sensor is warmed up and calibrated against a clean-air baseline; alarm activation is based on a defined threshold rather than an isolated raw reading. The temperature channel uses an upper threshold suitable for the prototype environment. To reduce nuisance alarms, the algorithm requires multiple consecutive samples for analog hazards and uses a debounce interval for the door input. Each alarm message contains a compact event label, system state, and time sequence, for example: 'ALERT: INTRUSION - PIR - SYSTEM ARMED.'

3. Performance Evaluation Procedure

Performance evaluation is based on a controlled test matrix. Each event category is triggered

repeatedly under known conditions. True positive (TP) denotes a valid hazard correctly detected; false negative (FN) denotes a valid hazard missed; false positive (FP) denotes an alarm without a valid hazard; and true negative (TN) denotes a normal condition correctly ignored. Detection accuracy is calculated as $(TP + TN)/(TP + TN + FP + FN) \times 100$. Sensitivity is $TP/(TP + FN) \times 100$, while false-alarm rate is $FP/(FP + TN) \times 100$. SMS latency is measured from the controller's alarm decision to receipt of the SMS on the registered mobile handset. Recovery tests include GSM signal loss, controller reset, and restoration after temporary power interruption.

Because this paper defines a methodology rather than reporting a completed field deployment, the numerical table in the Results section is an illustrative prototype-validation dataset constructed to demonstrate how the proposed metrics should be reported. It should be replaced by measured values when the physical system is implemented. The scenario assumes 20 controlled trials for each alarm class plus normal-operation trials, using the same threshold and software configuration throughout the experiment. This preserves methodological transparency while showing the expected form of analysis.

Table 2. Prototype test plan and evaluation criteria

Test	Stimulus	Expected response	Metric
Intrusion	Human motion while ARMED	Buzzer + intrusion SMS	TP/FN, SMS latency
Door breach	Door contact opens while ARMED	Immediate alarm + SMS	TP/FN, debounce response
Smoke/gas	Sensor value exceeds threshold	Priority alarm + SMS	Sensitivity, response time
Temperature	Temperature exceeds set limit	Hazard SMS + local warning	Threshold repeatability
Normal state	No valid hazard	No alarm	FP/TN, false-alarm rate
Network loss	GSM unavailable then restored	Local alarm; retry SMS	Recovery and delivery after reconnection

Results

The illustrative validation indicates that the proposed architecture can achieve high event-detection reliability while maintaining short remote-notification delay. Across the four alarm categories, the scenario yields detection success between 95% and 100%. The highest reliability is assigned to the magnetic door contact because it is a discrete input with a clear open/closed state. PIR sensing is slightly more variable because detection depends on distance, movement direction, and sensor stabilization. Gas/smoke and temperature channels require threshold calibration, so their performance is influenced by environmental baseline and response time.

The mean illustrative SMS latency ranges from approximately 3.6 to 4.5 s after an alarm decision. This is consistent with the practical behavior reported for GSM-based smart-home prototypes, where notification is generally delivered within a few seconds under usable network coverage. Munawir et al. (2019), for example, reported short SMS notification times during PIR distance tests, while earlier GSM/GPRS work emphasized rapid response to alarm incidents (Zhao & Ye, 2008). The major advantage is that the alert does not depend on the residence having an active broadband connection; it depends primarily on cellular registration and signal availability.

The design also reduces single-point dependence by retaining a local buzzer and status output. If the GSM network is temporarily unavailable, the controller still enters ALARM and continues local notification while periodically retrying the message. When service returns, the queued alert can be transmitted. Conversely, a remote message alone is not treated as proof that the physical event has ended; the alarm is cleared only by authorized reset logic or by the defined safety recovery condition. This prevents accidental cancellation caused by delayed or duplicated SMS traffic.

A limitation of GSM/SMS systems is that delivery time is network-dependent and cannot be

guaranteed as hard real-time communication. In addition, 2G availability varies by country and operator, so an implementation should use a modem compatible with the cellular services currently available in the deployment area. Sensor placement is another critical factor: PIR sensors must avoid direct sunlight and rapid thermal changes, and gas sensors should be located according to the density and expected source of the target gas. Therefore, the proposed architecture is best interpreted as a low-cost, resilient residential monitoring framework rather than a substitute for certified fire, gas, or professional alarm systems where regulated safety compliance is required.

Table 3. Illustrative methodology/prototype validation results

Event class	Trials	Detected	Detection success	Mean SMS latency
PIR intrusion	20	19	95%	4.2 s
Door breach	20	20	100%	3.6 s
Smoke/gas	20	19	95%	4.5 s
High temperature	20	19	95%	4.1 s

Conclusion and Discussion

This methodology paper developed a GSM-based smart security and monitoring framework for residential applications using a microcontroller, multi-sensor inputs, local alarms, and SMS-based remote notification. The literature up to 2019 shows that GSM/GPRS systems provide useful coverage and remote accessibility, while Arduino-class controllers make multi-sensor integration affordable and adaptable (Zhao & Ye, 2008; Banerjee et al., 2019). The proposed method advances these ideas by defining explicit operating states, hazard priority, authorized commands, false-alarm filtering, and measurable evaluation metrics rather than treating the system as only a circuit prototype. The design can monitor intrusion, forced entry, smoke/gas, and abnormal temperature, and it retains local warning even if cellular delivery is delayed. The principal methodological contribution is the reproducible test framework based on detection outcomes, false-alarm behavior, SMS latency, and recovery from communication or power interruption. The illustrative results demonstrate how these metrics can be summarized without presenting unperformed field measurements as empirical facts. For future implementation, the same controller logic can be migrated to LTE/4G, NB-IoT, or dual-network communication while preserving SMS as a fallback channel. Additional improvements can include battery backup, encrypted configuration, event logging, camera verification, and dual-sensor confirmation for intrusion events. Overall, GSM remains a practical communication mechanism for low-cost

residential monitoring when simplicity, wide-area reach, and independence from home broadband are important design requirements.

References

- Aggarwal, L., Gaur, V., & Verma, P. (2014). Design and implementation of GSM based automated home security system. *IAES International Journal of Robotics and Automation*, 3(3). <https://doi.org/10.11591/ijra.v3i3.4033>
- Banerjee, S., Chowdhury, E., Sikder, C., Sarkar, D., & Sarbadhikary, R. (2019). Arduino UNO and GSM based real-time home security system using self-generated password protection. *International Journal of Scientific and Research Publications*, 9(4), 177-181. <https://doi.org/10.29322/IJSRP.9.04.2019.p8827>
- Hasan, R., Khan, M. M., Ashek, A., & Rumpa, I. J. (2015). Microcontroller based home security system with GSM technology. *Open Journal of Safety Science and Technology*, 5(2), 55-62. <https://doi.org/10.4236/ojsst.2015.52007>
- Hoque, M. A., & Davidson, C. (2019). Design and implementation of an IoT-based smart home security system. *International Journal of Networked and Distributed Computing*, 7, 85-92. <https://doi.org/10.2991/ijndc.k.190326.004>
- Islam, M. S. (2014). Home security system based on PIC18F452 microcontroller. 2014 IEEE International Conference on Electro/Information

Technology, 202-205.
<https://doi.org/10.1109/EIT.2014.6871762>

Karim, B. A., & Awl, H. N. (2018). Smart home system based on GSM network. *Kurdistan Journal of Applied Research*, 3(1), 17-21.
<https://doi.org/10.24017/science.2018.1.4>

Kumar, S. V. S. V. P. D., & Akashe, S. (2017). Implementation of GSM based security system with IoT applications. *International Journal of Computer Network and Information Security*, 9(6), 13-20.
<https://doi.org/10.5815/ijcnis.2017.06.02>

Munawir, Ihsan, A., & Mutia, E. (2019). Wi-Fi and GSM based motion detection in smart home security system. *IOP Conference Series: Materials Science and Engineering*, 536, 012143.
<https://doi.org/10.1088/1757-899X/536/1/012143>

Rahman, M., Karim, A. H. M. Z., Nyeem, S., Khan, F., & Matin, G. (2015). Microcontroller based home

security and load controlling using GSM technology. *International Journal of Computer Network and Information Security*, 7(4), 29-36.
<https://doi.org/10.5815/ijcnis.2015.04.04>

Sharma, R. K., Mohammad, A., Kalita, H., & Kalita, D. (2014). Android interface-based GSM home security system. 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 196-201.
<https://doi.org/10.1109/ICICT.2014.6781278>

Teymourzadeh, R., Ahmed, S. A., Chan, K. W., & Hoong, M. V. (2013). Smart GSM based home automation system. 2013 IEEE Conference on Systems, Process & Control (ICSPC), 306-309.
<https://doi.org/10.1109/SPC.2013.6735152>

Zhao, Y., & Ye, Z. (2008). A low-cost GSM/GPRS based wireless home security system. *IEEE Transactions on Consumer Electronics*, 54(2), 567-572.
<https://doi.org/10.1109/TCE.2008.4560131>