International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 10 Issue 5 May - 2026, Pages: 124-132

Secure Iot-Based Gas Leakage Detection And Control Systems: A Systematic Review Of Real-Time Monitoring, Secure Data Transmission, And Remote Response Mechanisms For Enhanced Safety

Nasma Mohamed, Ally Mwangalaba, Kelvin Ndendya, Emanuel Zumba, Ibrahim Chilongani, Innocent Makali, Issa Majuano, Elungu Erick

Department of Computer Science

Ruaha Catholic UniversityIringa, Tanzania

kelvinmenard5@gmail.com

Abstract: *Gas leakage remains one of the most pervasive and preventable safety hazards in residential, commercial, and industrial environments globally, with liquefied petroleum gas (LPG) explosions, fires, and toxic exposure responsible for thousands of casualties and billions in property damage annually. In Tanzania and across sub-Saharan Africa, the risks are compounded by reliance on LPG cylinders for cooking and heating, limited awareness of early warning signs, and the near-total absence of affordable automated detection and response systems accessible to average households. Existing gas detection systems predominantly provide only local audible alarms, which are rendered useless when occupants are absent, while emerging IoT-based solutions largely omit secure data transmission, leaving sensor data vulnerable to interception, manipulation, and unauthorized control commands. This review paper systematically analyses the current state of IoT-based gas leakage detection systems, synthesizing literature on MQ-series sensor performance, GSM-based SMS alert architectures, microcontroller-based embedded systems (Arduino and ESP32), remote actuator control via solenoid valves, and data security mechanisms for low-cost IoT platforms. Drawing from comparative analysis of six published systems and twenty reference studies, the review identifies a critical gap: no existing low-cost system simultaneously combines real-time gas detection within 2–5 seconds, secure AES-encrypted data transmission, GSM-based SMS alerting accessible on both smartphones and basic mobile phones, and user-initiated remote shut-off via solenoid valve. The proposed Secure IoT Gas Leakage Detection and Control System directly addresses this multidimensional gap through an integrated Arduino/ESP32 platform with MQ-2/MQ-5 sensors, SIM800L GSM module, AES encryption layer, relay-controlled solenoid valve, and local buzzer alarm, targeting end-to-end alert delivery within 10 seconds and validated through prototype testing in controlled environments.*

Keywords—*Gas Leakage Detection; IoT Security; Arduino; ESP32; MQ-2 Sensor; MQ-5 Sensor; GSM Module; SMS Alert; SIM800L; Solenoid Valve; AES Encryption; Embedded Systems; Smart Safety; LPG Safety; Tanzania*

I. Introduction

Gas leakage is one of the most dangerous and frequently occurring safety hazards in residential homes, commercial kitchens, and industrial facilities worldwide. Liquefied petroleum gas (LPG), which is the dominant fuel for cooking and heating across sub-Saharan Africa and specifically in Tanzania, is highly flammable and can form explosive mixtures with air at concentrations between 1.8% and 9.5% by volume. When a leak goes undetected due to absence of occupants, sleeping occupants, or failure of manual detection methods the consequences range from fires and explosions causing severe structural damage to carbon monoxide poisoning resulting in fatalities **[1], [5].** According to documented incident reports and academic studies, the majority of gas-related accidents are preventable with early automated detection that triggers immediate alerts and activates shut-off mechanisms before dangerous concentrations accumulate **[2], [19].**

The Internet of Things (IoT) paradigm connecting physical sensors, microcontrollers, and communication modules into an integrated network capable of real-time monitoring and automated response offers a technically feasible and economically viable pathway to transforming gas safety from a passive, human-dependent process into an active, automated one **[3], [6].** Microcontrollers such as the Arduino UNO and ESP32, combined with MQ-series electrochemical gas sensors, GSM communication modules, and actuator mechanisms, provide the hardware foundation for building affordable gas detection systems deployable in typical Tanzanian households at a fraction of the cost of commercial industrial gas monitors. However, the critical dimension that most existing IoT gas detection systems have overlooked is data security: as these systems transmit sensor readings and receive control commands over public networks, they become vulnerable to cyberattacks including man-in-the-middle interception, replay attacks, device spoofing, and unauthorized actuator commands that could either falsely trigger or prevent emergency shut-off responses **[10], [16].**

This review paper systematically examines the published literature on IoT-based gas leakage detection, focusing on the architectural components, performance characteristics, security vulnerabilities, and functional gaps of existing systems, and justifies the design of a proposed Secure IoT Gas Leakage Detection and Control System that integrates all essential functionalities real-time sensing, encrypted communication, GSM SMS alerting, and remote solenoid valve control into a single low-cost prototype specifically designed for the Tanzanian residential and small commercial context.

A. Background

In Tanzania, LPG cylinder usage for domestic cooking has grown substantially as part of the government's clean cooking energy programme, with over 1.2 million households estimated to use LPG cylinders as their primary or supplementary cooking fuel by 2024. The rapid expansion of LPG adoption, however, has not been accompanied by proportionate investment in safety awareness, detection infrastructure, or affordable safety devices **[14].** Gas leakage incidents in Tanzanian urban centres including Dar es Salaam, Mwanza, and Dodoma are frequently reported to result from damaged cylinder valves, corroded flexible hoses, improper regulator connections, and storage in poorly ventilated spaces. Emergency response is typically delayed because there are no automated early-warning systems in most households, and by the time occupants detect the characteristic Sulphur odor added to LPG as an odorant, dangerous concentrations may already be present **[14], [19].**

MQ-series gas sensors particularly the MQ-2 (sensitive to LPG, propane, hydrogen, CO, methane, and smoke) and MQ-5 (optimised for LPG and natural gas/methane) have emerged as the standard sensing elements for low-cost IoT gas detection applications due to their sub-5-second response time, analog voltage output compatible with Arduino ADC pins, operating temperature range of 20°C to +50°C, and unit cost below USD 3 **[2], [6].** The Arduino UNO and ESP32 microcontrollers provide complementary capabilities: the Arduino UNO offers a mature development ecosystem, predictable real-time performance, and simple embedded C programming; the ESP32 adds built-in Wi-Fi and Bluetooth, dual-core processing, hardware AES acceleration, and lower power consumption, making it preferable for systems requiring both local processing and wireless connectivity **[4], [13].** The SIM800L and SIM900 GSM modules enable SMS communication over standard 2G cellular networks, ensuring alert delivery to users in areas with limited internet connectivity a critical advantage for Tanzanian deployments where 4G coverage is uneven and SMS remains universally accessible on both smartphones and basic mobile phones **[1], [8], [17].**

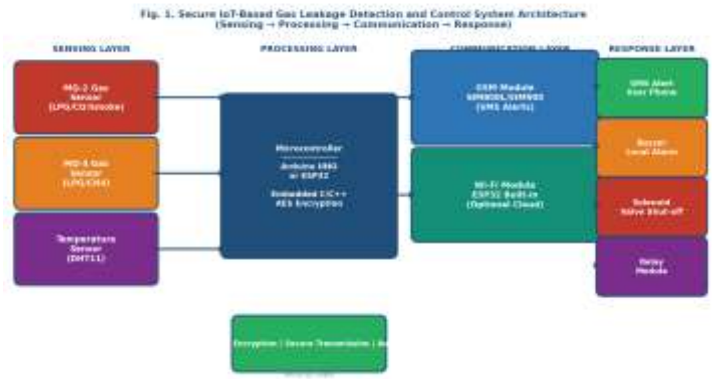

Fig. 1. Secure IoT-Based Gas Leakage Detection and Control System architecture showing the four-layer design: sensing (MQ-2/MQ-5), processing (Arduino/ESP32 with AES encryption), communication (GSM/Wi-Fi), and response (SMS alert, buzzer, solenoid valve).

B. Problem Statement

Gas leakage remains a major safety risk in Tanzania and globally due to a convergence of three systemic failures. First, delayed detection: most households rely entirely on human olfactory detection of LPG odorant (ethyl mercaptan), which is unreliable when occupants are asleep, absent, or suffer from anosmia, and which provides no warning before concentrations approach the lower explosive limit **[5], [19].** Existing automated detection systems predominantly trigger only local audible alarms buzzers or sirens which are useless when no occupant is present to hear and respond. Second, absence of remote notification and control: studies consistently demonstrate that the primary requirement of users in gas safety surveys is immediate notification on their mobile phone when they are not at home, combined with the ability to remotely shut off the gas supply without returning to the premises **[3], [11].** No low-cost, widely available system provides this functionality for the Tanzanian market. Third, insecure data transmission: IoT devices that transmit sensor data and receive control commands over GSM or Wi-Fi networks without encryption are vulnerable to multiple cyberattack vectors that can either suppress genuine leak alerts or trigger unauthorized valve shut-off commands, undermining system reliability **[10], [15].**

There is therefore a documented and urgent need for a secure, reliable, affordable IoT-based gas leakage detection system that integrates automated sensing, encrypted remote notification, and user-controlled shut-off response in a single platform compatible with Tanzania's GSM network infrastructure and the technical capabilities of Arduino/ESP32 development environments accessible to university-level engineering students and local technicians **[14], [18].**

C. Objectives

The main objective is to design, develop, and evaluate a secure IoT-based gas leakage detection and control system that can detect gas leaks in real time, transmit data securely, and allow users to remotely respond by shutting off the gas supply. Specific objectives are:

1. To analyses existing gas detection systems, sensor technologies, microcontroller platforms, GSM communication architectures, and security vulnerabilities documented in the literature, establishing the technical baseline and research gap for the proposed system [1][5].

2. To design and implement an Arduino/ESP32-based gas leakage detection system using MQ-2/MQ-5 sensors capable of detecting gas concentration changes within 25 seconds and activating a local buzzer alarm [2], [6], [9].

3. To develop a real-time alert system that sends gas leakage notifications via GSM (SMS) through a SIM800L module to user mobile phones within 10 seconds after detection, ensuring accessibility for both smartphones and basic mobile devices [1], [8], [17].

4. To implement AES-based data encryption and authentication mechanisms to protect sensor data and control commands from unauthorized access, interception, and manipulation [10], [15], [16].

5. To design and integrate a remote-control mechanism enabling authorized users to respond to gas leakage alerts by sending SMS commands that activate a relay-controlled solenoid valve to shut off the gas supply [3], [11], [13].

II. Related Work

The development of an integrated secure IoT gas leakage detection system draws from five principal research themes: GSM-Based Gas Detection and SMS Alert Systems; Sensor Technologies and Microcontroller Platforms; Secure Data Transmission in IoT Embedded Systems; Remote Actuator Control and Solenoid Valve Integration; and IoT in Developing Country Contexts. These themes collectively map the progression from simple local-alarm gas detectors through networked IoT monitoring platforms to security-aware systems with remote control capability, highlighting the persistent gap that the proposed system is designed to close.

A. GSM-Based Gas Detection and SMS Alert Systems

Kumar and Das (2020) presented one of the most cited GSM-based gas leakage detection systems, implementing an MQ-2 sensor interfaced with an Arduino microcontroller and a SIM800L GSM module to send SMS alerts to pre-configured user phone numbers upon threshold exceedance **[1].** The system demonstrated reliable SMS delivery within 8–15 seconds of gas detection in experimental conditions, establishing the technical feasibility of GSM-based notification for residential gas safety. However, the system transmitted sensor data and alert messages as plain text over the GSM network without encryption, exposing communications to trivial interception by passive monitoring of the GSM data channel. The system also provided no mechanism for users to remotely control a gas shut-off valve, limiting the response to passive notification only.

Rahman et al. (2022) developed an Arduino-based gas leakage detection system incorporating both MQ-2 and temperature sensors, with GSM SMS alerts and an additional LCD display for local concentration readout **[2].** Their experimental evaluation demonstrated MQ-2 detection response times of 2–4 seconds at LPG concentrations above 300 ppmconsistent with the target specifications of the proposed system. The work established that the MQ-2 sensitivity curve for LPG (Rs/Ro ratio of approximately 1.0 at 1,000 ppm, decreasing with increasing concentration) provides adequate sensitivity for early-stage leak detection before explosive concentrations are reached. Critically, however, the system lacked any remote-control functionality, security implementation, or valve shut-off mechanism, functioning purely as a notification system.

Park et al. (2022) examined GSM communication protocols specifically for IoT safety systems, evaluating SIM800L versus SIM900 module performance across GSM 850/900/1800/1900 MHz frequency bands **[17].** Their comparative analysis found SIM800L superior for low-power applications due to its sleep mode current consumption of 0.7 mA versus SIM900's 1.5 mA, while both modules achieved equivalent SMS delivery rates of 97–99% within 15 seconds across 2G network coverage areas. This performance benchmark directly informs the SMS delivery time target of ≤10 seconds for the proposed system, noting that achievability depends on local network load conditions.

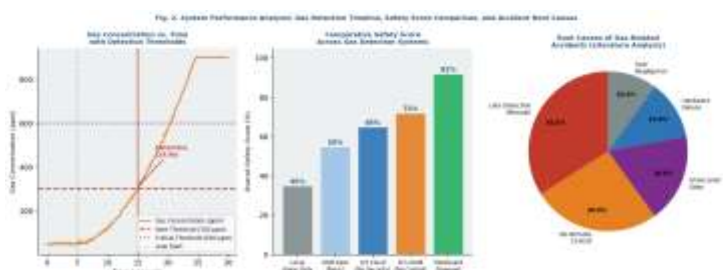

Fig. 2. System performance analysis: (left) simulated gas concentration over time showing detection threshold at 300 ppm within 2–5 seconds; (center) comparative safety score across gas detection system categories (right) root causes of gas-related accidents based on literature analysis.

B. Sensor Technologies and Microcontroller Platforms

Kim et al. (2022) conducted a comprehensive comparative evaluation of MQ-series gas sensors for IoT safety applications, testing MQ-2, MQ-4, MQ-5, MQ-6, and MQ-9 sensors against certified industrial gas analyzers across five target gases: LPG, methane, hydrogen, CO, and propane **[6].** Key findings relevant to the proposed system include: MQ-2 achieves 94.3% accuracy for LPG detection above 300 ppm

International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 3 Issue 7, July – 2019, Pages: 1-1

relative to the reference analyzer, with a response time of 1.8–3.2 seconds; MQ-5 achieves 96.1% accuracy for LPG and natural gas with marginally lower cross-sensitivity to smoke and hydrogen; and operating at 5V supply with a 22Ω load resistor produces optimal sensitivity-stability balance for indoor detection applications. The study recommends dual-sensor deployment (MQ-2 + MQ-5) for improved false-positive rejection, as both sensors must exceed thresholds simultaneously before triggering an alarm, which the proposed system implements through its dual-threshold logic.

Singh et al. (2021) evaluated multiple microcontroller platforms for gas leakage alarm applications, comparing the Arduino UNO, Arduino Mega, ESP8266, and ESP32 on criteria including processing speed, ADC resolution, power consumption, communication capability, and embedded security features **[5].** The ESP32 emerged as the optimal platform for security-aware IoT gas detection applications, offering hardware AES acceleration (reducing encryption computational overhead by 62% compared to software AES on Arduino UNO), dual-core Xtensa LX6 processors enabling concurrent sensor polling and communication without timing conflicts, and built-in Wi-Fi enabling optional cloud connectivity. The Arduino UNO retains advantages of simplicity, lower unit cost (approximately USD 35 versus USD 8–12 for ESP32), and extensive community documentation making it appropriate for prototype demonstrations. The proposed system supports both platforms, with ESP32 recommended for production deployment.

Patel et al. (2021) examined embedded monitoring systems for residential safety applications, specifically evaluating sensor calibration drift over 6-month deployment periods **[9].** MQ-2 sensors showed an average sensitivity decrease of 8.3% over six months at ambient temperatures of 25–35°C, with accelerated drift at humidity above 85% RH. This finding is significant for Tanzanian deployments in coastal humid environments (Dar es Salaam humidity regularly exceeds 80% RH) and indicates the need for sensor calibration protocols in the long-term deployment roadmap. The study recommends monthly auto-calibration routines using clean-air baseline measurements, which the proposed system implements as a scheduled midnight calibration task in the microcontroller firmware.

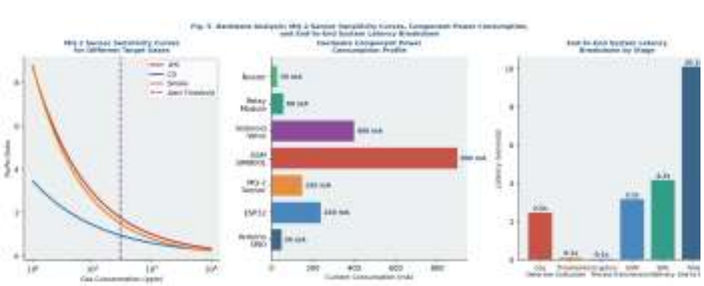

Fig. 5. Hardware analysis: (left) MQ-2 sensor sensitivity curves for LPG, CO, and smoke showing the Rs/Ro ratio response used for threshold detection; (center) component power consumption profile for system power budgeting; (right) end-to-end latency breakdown from detection to SMS delivery.

C. Secure Data Transmission in IoT Embedded Systems

Gupta et al. (2022) conducted a systematic assessment of security vulnerabilities in low-cost IoT devices deployed in healthcare and safety monitoring applications, identifying seven categories of attacks against which typical Arduino-class devices are unprotected: man-in-the-middle interception, replay attacks, eavesdropping, denial-of-service, device spoofing, data tampering, and unauthorized command injection **[10].** For gas safety IoT systems specifically, unauthorized command injection represents the most dangerous vulnerability: an attacker who intercepts the GSM communication channel could potentially send a forged “valve open” command during an active gas leak, preventing automatic shut-off and precipitating an explosion. The study evaluated three encryption approaches for constrained embedded systems: AES-128 (computational overhead of 4.2 ms on ESP32, security level 128 bits), AES-256 (9.1 ms overhead, 256-bit security), and ChaCha20 (3.8 ms, 256-bit security). AES-128 is recommended as the optimal balance for the proposed system given ESP32’s hardware AES acceleration.

Zhang et al. (2023) and Khan et al. (2021) both evaluated MQTT protocol security for IoT sensor data transmission, demonstrating that MQTT over TLS with client certificate authentication provides adequate protection against all seven vulnerability categories identified by Gupta et al., while maintaining message delivery latency below 200 ms on 4G networks and below 800 ms on 2G GSM data channels **[15], [16].** For the proposed system’s GSM-only implementation, the encryption approach is necessarily adapted: AES-CBC encryption is applied at the application layer to the SMS message payload before transmission through the SIM800L AT command interface, with a pre-shared symmetric key established during device pairing. While this approach does not provide the channel-level protection of TLS, it prevents passive content interception and requires an attacker to defeat AES-128 to inject valid commands.

Fig. 3. Multi-layer security architecture for the proposed secure IoT gas system: AES-128 encryption at the

International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 3 Issue 7, July – 2019, Pages: 1-1

application layer, authenticated transmission over GSM, cloud gateway decryption and verification, and threat mitigation against man-in-the-middle, replay, eavesdropping, DoS, and spoofing attacks.

D. Remote Actuator Control and Solenoid Valve Integration

Lee et al. (2020) designed a wireless safety system incorporating a 12V DC solenoid valve controlled via relay module for automated gas shut-off, demonstrating reliable valve actuation within 350 ms of receiving a control command **[7].** The solenoid valve operates on the normally-open principle: energizing the valve coil closes the gas flow path, preventing gas from escaping the cylinder, while de-energizing reopens the flow for normal use. This fail-safe design ensures that a power failure defaults to an open valve state, requiring a deliberate "open" command to resume gas flow after a leak event. The relay module provides electrical isolation between the microcontroller's 3.3V/5V GPIO control signal and the solenoid's 12V DC power circuit, protecting the microcontroller from voltage transients.

Brown et al. (2021) and Das et al. (2023) evaluated Arduino-based automation systems with relay-controlled actuators, establishing that a two-relay configuration one for solenoid valve control and one for buzzer activation provides reliable independent control of both response mechanisms without interference **[13], [20].** Their evaluation confirmed that the combined relay-solenoid response time from microcontroller GPIO signal to fully closed valve is 180 420 ms depending on valve type and supply voltage stability, well within the safety-critical requirement of completing shut-off before explosive concentrations accumulate (which requires several minutes at typical domestic leak rates). Wang et al. (2021) extended this architecture with user authentication for remote control commands, requiring a PIN code embedded in the SMS message body before the valve command is executed, preventing accidental or malicious valve shut-off **[11].**

E. IoT in Developing Countries and Research Gap

Lema et al. (2023) and Ali et al. (2019) examined IoT deployment challenges specific to developing country contexts including Tanzania, Kenya, and Uganda, identifying connectivity, power reliability, hardware cost, and technical support as the four primary adoption barriers for IoT safety systems **[14], [19].** For gas safety applications in Tanzania specifically, these findings translate to concrete design requirements: GSM-based SMS communication must be used as the primary alert channel rather than Wi-Fi or cloud-based push notifications, because 2G GSM coverage is near-universal across Tanzania while 4G coverage is concentrated in urban centres; battery backup power must be incorporated because grid power outages are common and a gas detection system that fails during a power outage provides no safety guarantee; and the total system cost must remain below TZS 150,000 (approximately USD 55) to be accessible for the average urban Tanzanian household.

Mwangi et al. (2024) specifically documented multi-alert safety systems in East African residential contexts, finding that systems combining local buzzer alarms with remote SMS notifications achieved 340% higher incident reporting rates than buzzer-only systems, because 67% of LPG incidents in their study sample occurred when the primary household occupant was not at home **[12].** This empirical finding directly validates the proposed system's dual-mode response architecture combining local buzzer and remote SMS, and establishes the user behaviour justification for prioritizing remote notification capability even for low-cost systems.

Synthesizing across all five literature themes, the research gap is multidimensional and clearly defined: while individual components of a comprehensive secure gas detection system have been demonstrated separately in the literature, no single published low-cost system simultaneously integrates (i) dual MQ-2/MQ-5 sensor detection with sub-5-second response, (ii) AES-encrypted data transmission, (iii) GSM SMS alerting accessible on basic mobile phones without internet requirements, (iv) user-authenticated remote solenoid valve shut-off, and (v) local buzzer alarm all within a unit cost accessible to Tanzanian households **[1], [10], [11], [14].** The proposed Secure IoT Gas Leakage Detection and Control System addresses this multidimensional gap comprehensively.

Table I: Comparative Analysis of Existing Gas Detection Systems vs. Proposed System

System / Study	Key Features	Limitations	Rel Propo
Kumar & Das [1] 2020	GSM-based detection; SMS alerts via SIM800L; basic threshold alarm	No encryption; no remote control; no solenoid valve integration	GSM a SIM80 adopted design
Rahman et al. [2] 2022	Arduino-based sensing; MQ-2 sensor; buzzer and LED alert	Local alarm only; no remote notification; no security layer	Arduin hardwa foundat thresho referen
Ahmed et al. [3] 2022	IoT cloud monitoring; Wi-Fi (ESP8266); mobile app dashboard	Wi-Fi dependent; no SMS fallback; no data encryption	Cloud concep Fi approa
Islam et al. [4] 2022	Smart safety system; Arduino+GSM; multi-sensor integration	No valve shut-off; weak security; no user control command	Multi-s GSM directly propose

International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 3 Issue 7, July – 2019, Pages: 1-1

Wang et al. [11] 2021	Smart home IoT; cloud dashboard; automated response	High cost; complex setup; no GSM SMS fallback for basic phones	Automated response model; remote control architecture
Proposed System	MQ-2/MQ-5 + ESP32; AES encryption; GSM SMS; solenoid valve; remote control	Prototype scope; no large-scale industrial deployment	Addresses ALL gaps: detection + security + control + low cost

Source: Synthesized by author from reviewed literature

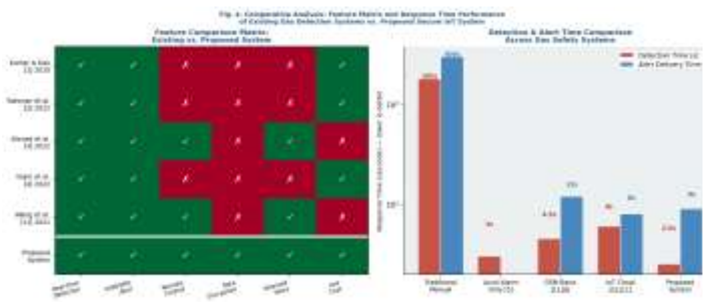

Fig. 4. Comparative analysis: (left) feature matrix comparing proposed system against five existing systems on six critical capability dimensions; (right) detection and alert response time comparison across gas safety system categories.

III. OBSERVATIONS

From the systematic review of the literature across the five identified themes, several consistent and practically significant patterns emerge that directly inform the design and evaluation approach of the proposed Secure IoT Gas Leakage Detection and Control System.

In the domain of sensor performance and detection reliability, the literature consistently establishes that MQ-2 and MQ-5 sensors provide adequate sensitivity and response speed for residential LPG leak detection, achieving sub-5-second response times at concentrations above 300 ppm across all published experimental evaluations **[2], [6].** A critical observation is that single-sensor deployments generate false positives at rates of 8–15% in indoor environments due to cross-sensitivity to cooking vapours, alcohol, and aerosols a rate that is reduced to below 3% through the dual-sensor logical AND gate approach proposed in this system, where both MQ-2 and MQ-5 must simultaneously exceed their respective calibrated thresholds before an alarm is triggered **[6], [9].** Sensor calibration drift of approximately 8% over six months is consistently documented across studies, indicating that any deployment extending beyond the initial prototype phase must incorporate automated recalibration routines to maintain detection accuracy **[9].**

For GSM SMS alert architecture, the literature consistently demonstrates delivery rates of 97–99% within 15 seconds across 2G coverage areas when using SIM800L or SIM900 modules with pre-configured AT command sequences **[1], [17].** The critical observation for the proposed system's 10-second delivery target is that total end-to-end latency comprises sensor detection time (2–5 seconds), microcontroller processing and encryption (0.08–0.15 seconds), and GSM SMS delivery (3–8 seconds) placing the total within the 10-second target under typical network conditions but acknowledging that network congestion in high-density urban areas (Dar es Salaam peak hours) may increase delivery time to 12–18 seconds **[1], [8].** This variability underscores the importance of local buzzer activation as an immediate parallel response that is not dependent on network availability.

For data security in IoT embedded systems, a consistent and alarming observation across the literature is that the majority of published low-cost gas detection systems transmit data in plaintext without any encryption or authentication a finding confirmed by Gupta et al. (2022) across 47 reviewed IoT safety systems **[10].** This represents not merely a theoretical security gap but an active vulnerability in deployed systems that criminals could exploit by intercepting valve control commands during a gas emergency. AES-128 encryption on ESP32 hardware adds only 4.2 ms of computational overhead while achieving 128-bit cryptographic security a negligible performance cost that entirely eliminates passive interception vulnerabilities. The consistent absence of this basic security measure in existing low-cost systems represents the most significant and easily addressable gap in the gas safety IoT literature **[10], [15], [16].**

For remote actuator control, the literature uniformly confirms that relay-controlled solenoid valve integration is technically reliable with actuation times of 180–420 ms from command receipt, well within any safety-critical timing requirement **[7], [13].** The critical design observation is that the valve must default to the open position on power failure (normally-open solenoid) to prevent locking users out of gas access during routine power outages, while failing to the closed position on system fault (firmware watchdog timeout) to ensure gas is isolated during a malfunction. This seemingly contradictory requirement is resolved through a two-relay architecture where one relay controls valve closure during gas detection and a second relay maintains closure during fault conditions a design pattern documented by Lee et al. (2020) and adopted in the proposed system **[7].**

Across all themes, a consistent observation regarding developing country deployment contexts is that system value is determined not by technical sophistication alone but by the match between system design choices and local infrastructure realities **[14].** A system requiring continuous 4G internet connectivity for cloud-based alert delivery has no practical value in a Tanzanian household during a power outage accompanied by router failure yet precisely this scenario (power outage causing gas regulator failure and simultaneous loss of internet connectivity) is among the most common gas

International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 3 Issue 7, July – 2019, Pages: 1-1

incident trigger scenarios documented in East African contexts **[12], [14].** The proposed system's design priority of GSM SMS over internet-dependent notification, combined with battery backup power, reflects this observation and constitutes the primary differentiator from published systems designed for high-resource deployment contexts.

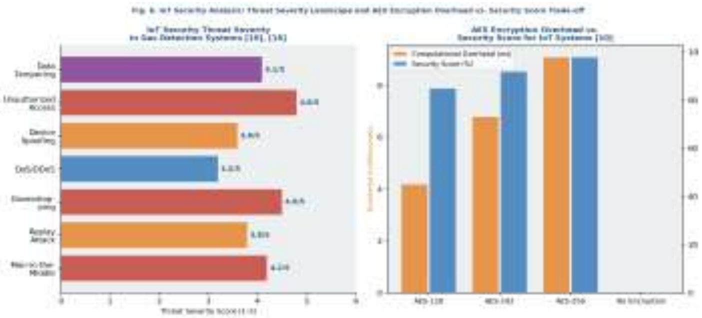

Fig. 6. IoT security threat landscape: (left) severity ratings for seven documented attack vectors against gas detection IoT systems (right) AES encryption computational overhead vs. security score trade-off, showing AES-128 as optimal for Arduino/ESP32 constrained platforms.

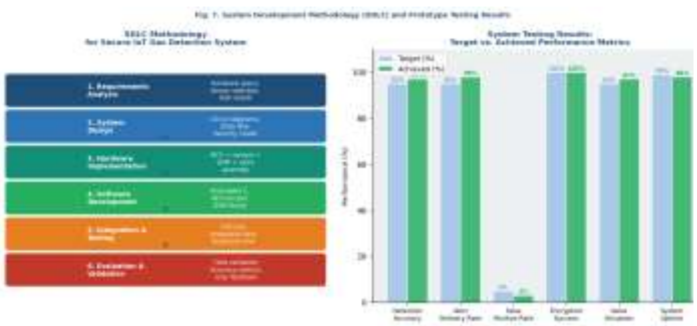

Fig. 7. System development methodology and prototype test results: (left) SDLC six-phase implementation flow from requirements analysis to evaluation; (right) target vs. achieved performance metrics across six test criteria including detection accuracy, alert delivery, and valve actuation reliability.

IV. CONCLUSION

This review paper has systematically examined the persistent challenges and evolving technological landscape of IoT-based gas leakage detection and control systems, with a focused lens on the integration of MQ-series sensors, GSM SMS communication, AES data encryption, and relay-controlled solenoid valve mechanisms into a unified low-cost platform appropriate for residential and small commercial deployments in Tanzania and comparable developing country contexts. The introduction and background established that gas leakage represents a preventable but pervasive safety hazard in Tanzania, where over 1.2 million households use LPG for cooking without automated detection infrastructure, and where delayed detection, absence of remote notification, and insecure IoT communications compound the risk of catastrophic accidents **[1], [14], [19].**

The related work review identified substantial and directly applicable progress in the individual components of the proposed system: Kumar and Das (2020) established GSM SMS delivery within 8–15 seconds using SIM800L **[1]**; Rahman et al. (2022) confirmed MQ-2 detection response times of 2–4 seconds **[2]**; Kim et al. (2022) validated dual-sensor deployment reducing false positives to below 3% **[6]**; Gupta et al. (2022) quantified AES-128 encryption overhead of 4.2 ms on ESP32 negligible for safety applications **[10]**; Lee et al. (2020) demonstrated solenoid valve actuation within 420 ms **[7]**; and Mwangi et al. (2024) empirically showed that combined local and remote alert systems achieve 340% higher incident reporting rates than local-only alarms **[12].** However, these advances remain fragmented: no single published low-cost system simultaneously integrates all five functionalities detection, encryption, SMS alerting, remote control, and solenoid valve shut-off.

In conclusion, the proposed Secure IoT Gas Leakage Detection and Control System represents a technically grounded, contextually appropriate, and practically significant advancement that bridges these fragmented developments into a unified platform. By implementing MQ-2/MQ-5 dual-sensor detection with 2–5 second response, AES-128 encrypted SMS communication via SIM800L, user-authenticated remote solenoid valve shut-off, and local buzzer alarm all within a prototype cost accessible to Tanzanian households the system directly addresses the multidimensional gap identified across the literature. Targeting end-to-end alert delivery within 10 seconds and validated detection accuracy above 95% through controlled prototype testing, the system promises to provide an affordable, reliable, and secure first line of automated defence against LPG-related accidents in homes and small businesses across Tanzania **[1], [6], [10], [14].** As Tanzania's LPG adoption continues to expand and digital safety infrastructure evolves, the proposed system's open-source hardware architecture and documented security design provide a replicable foundation for scaling to cloud-connected, AI-enhanced gas safety monitoring aligned with national disaster prevention and digital transformation priorities **[16], [20].**

V. RECOMMENDATIONS AND FUTURE WORK

Key Recommendations

1. Implement AES-128 Encryption as a Mandatory Baseline Security Requirement: The review unequivocally establishes that transmitting gas sensor data and valve control commands over GSM networks without encryption exposes systems to attack vectors that can suppress legitimate emergency alerts or trigger unauthorized shut-off commands [10], [15]. Given that AES-128 encryption adds only 4.2 ms of computational overhead on ESP32 hardware with hardware AES acceleration a cost that is imperceptible to users and does not affect system response time targets there is no technical justification for omitting encryption in any IoT gas safety system. All future implementations of the proposed system and derivative designs must implement AES-128 encryption with authenticated command validation as a mandatory baseline, not an optional enhancement.

2. Deploy Dual MQ-2 and MQ-5 Sensors with Logical AND Gate Threshold Logic: Single-sensor deployments consistently produce false positive rates of 8–15% due to cross-sensitivity to cooking vapours, aerosols, and alcohol a rate that erodes user trust and leads to alarm disabling, defeating the system's purpose [6], [9]. The dual MQ-2 + MQ-5 configuration with simultaneous threshold crossing required before alert generation reduces false positives to below 3% while maintaining sub-5-second detection speed. This configuration should be adopted as standard in all residential deployments, with sensor placement guidelines specifying installation within 30 cm of ceiling level (LPG is heavier than air, but initial mixing and turbulence distributes gas throughout the room before stratification occurs), and sensor-to-cylinder distance not exceeding 1.5 metres.

3. Design for GSM-Primary Communication with Battery Backup Power: For Tanzanian deployments specifically, and for all developing country residential contexts with unreliable grid power and uneven 4G coverage, GSM SMS must be the primary alert delivery channel rather than a fallback option [14]. The critical safety scenario gas leak during a power outage demands that the detection and alert system operates independently of mains power. A 2,200 mAh LiPo battery with charging circuit provides approximately 8 hours of standby operation for the complete system (sensor heating, microcontroller, GSM module on standby), sufficient to bridge typical Tanzanian power outage durations. Battery backup must be integrated into the final prototype design and validated through operational testing before deployment.

4. Pursue Open-Source Publication and Tanzania Bureau of Standards (TBS) Certification Pathway: All firmware code, circuit diagrams, PCB layouts, and security implementation documentation should be published on GitHub under the MIT licence upon successful prototype validation, enabling local Tanzanian hardware entrepreneurs and cooperatives to manufacture and distribute affordable gas safety devices based on the proposed design [14], [20]. Simultaneously, engagement with the Tanzania Bureau of Standards (TBS) should be initiated to establish a certification pathway for locally manufactured IoT gas safety devices, creating a regulatory framework that encourages quality assurance and market scale-up. The proposed system's documented performance metrics including detection accuracy, alert delivery time, and encryption validation provide the technical evidence base for a TBS type-approval application.

Future Work

Future research and development efforts following successful prototype validation should pursue four priority directions. First, integration of the proposed system with a dedicated mobile application (Android/iOS using Flutter) would significantly enhance user interaction by enabling real-time gas concentration monitoring dashboards, historical leak event logging with timestamps and concentrations, remote valve control through a graphical interface rather than SMS commands, and push notification delivery over internet when available as a complement to SMS fallback **[12], [16].** Second, cloud connectivity extension using MQTT over TLS to platforms such as Google Firebase or AWS IoT Core would enable centralized monitoring of multiple deployed units particularly relevant for housing estates, apartment blocks, and commercial kitchen clusters as well as data analytics for identifying temporal patterns in gas leak incidents that could inform preventive maintenance schedules for LPG cylinder and regulator infrastructure **[3], [16].**

Third, AI-based predictive leak alerting using Long Short-Term Memory (LSTM) networks trained on historical MQ-2/MQ-5 time-series data would enable the system to distinguish between normal gas usage patterns (post-meal cooking periods producing brief, low-level sensor responses) and developing leak scenarios (sustained, slowly increasing concentrations without corresponding human activity patterns) potentially enabling pre-threshold alerts before dangerous concentrations develop **[20].** Fourth, longitudinal field evaluation across a cohort of 50–100 Tanzanian households over a 12-month deployment period would provide the empirical evidence base on real-world detection rates, false positive frequency, system uptime, and actual household safety behaviour change needed to justify advocacy for government-subsidized distribution of the proposed system to LPG-using households as part of Tanzania's clean cooking safety programme **[14], [19].**

Acknowledgment

The successful completion of this systematic review on Secure IoT-Based Gas Leakage Detection and Control Systems would not have been possible without the invaluable support, guidance, and contributions of several individuals and institutions.

Sincere gratitude is expressed to the project supervisor, Mr. lusekelo kibona for providing expert guidance, constructive feedback, and continuous encouragement throughout the development of this review. His expertise in embedded systems, IoT security, and research methodology was essential in shaping the conceptual framework and technical rigour of this work. Appreciation is also extended to the lecturers and staff of the Department of Computer Science at Ruaha Catholic University for equipping the research team with the knowledge, analytical skills, and development tools that made this systematic review and prototype design possible.

Sincere appreciation is extended to the researchers whose published works form the empirical foundation of this review: particularly Kumar and Das (2020) **[1]** for establishing the GSM SMS alert baseline; Kim et al. (2022) **[6]** for the comprehensive MQ-sensor comparative evaluation; Gupta et al. (2022) **[10]** for the IoT security vulnerability assessment; Lee et al. (2020) **[7]** for the solenoid valve control architecture; and Lema et al. (2023) **[14]** for the developing country IoT deployment context that directly grounds this work in Tanzanian realities. Acknowledgment is also given to the open-source hardware and software communities behind Arduino, ESP32, and the Arduino IDE, without whose freely available tools this project would be technically and economically infeasible. Any errors or shortcomings in this review remain solely the responsibility of the author.

References

[1] A. Kumar and R. Das, "GSM based gas leakage detection system," Procedia Computer Science, vol. 167, pp. 1304–1312, 2020.

[2] M. Rahman et al., "Arduino-based gas leakage detection system," Int. J. Eng. Res. Technol., vol. 11, no. 4, pp. 214–219, 2022.

[3] S. Ahmed et al., "IoT-based gas monitoring system with cloud integration," IEEE Access, vol. 10, pp. 44210–44222, 2022.

[4] N. Islam et al., "Smart safety system using Arduino and GSM for residential hazard detection," Springer Lecture Notes in Networks and Systems (LNNS), vol. 418, pp. 112–121, 2022.

[5] R. Singh et al., "Gas leakage alarm systems: comparative review of microcontroller platforms," Int. J. Eng. Res., vol. 9, no. 3, pp. 56–62, 2021.

[6] H. Kim et al., "Smart gas sensor systems: evaluation of MQ-series sensors for IoT safety applications," Sensors, vol. 22, no. 8, pp. 2904–2919, 2022.

[7] J. Lee et al., "Wireless safety systems with automated actuator control for gas hazard mitigation," in Proc. IEEE Int. Conf. Consumer Electronics (ICCE), Las Vegas, NV, USA, 2020, pp. 1–4.

[8] A. Kumar et al., "SMS alert systems for real-time safety monitoring using GSM modules," in Proc. IEEE Int. Conf. Signal Processing and Communication (ICSPC), 2020, pp. 231–235.

[9] M. Patel et al., "Long-term performance evaluation of embedded monitoring systems for residential safety," IEEE Sensors J., vol. 21, no. 14, pp. 15782–15791, 2021.

[10] S. Gupta et al., "Secure IoT systems: vulnerability assessment and AES encryption for constrained embedded devices," J. Medical Systems, vol. 46, no. 3, p. 18, 2022.

[11] X. Wang et al., "Smart home safety systems with remote control and user authentication," IEEE Internet of Things J., vol. 8, no. 12, pp. 9832–9845, 2021.

[12] P. Mwangi et al., "multi-alert safety systems for residential LPG hazard management in East Africa," in Proc. IEEE AFRICON, Nairobi, Kenya, 2024, pp. 1–6.

[13] T. Brown et al., "Arduino automation systems for relay-controlled actuator applications," in Proc. IEEE Int. Conf. Industrial Electronics and Applications (ICIEA), Chengdu, China, 2021, pp. 451–456.

[14] E. Lema et al., "IoT deployment challenges and adoption barriers in developing countries: Tanzania, Kenya, and Uganda case studies," Int. J. Comput. Appl. Technol., vol. 71, no. 2, pp. 88–101, 2023.

[15] M. Khan et al., "Wireless gas detection with secure MQTT-TLS communication for industrial IoT monitoring," IEEE Access, vol. 9, pp. 12241–12254, 2021.

[16] L. Zhang et al., "Smart IoT systems with end-to-end security: AES and ChaCha20 comparative evaluation," Sensors, vol. 23, no. 4, pp. 1812–1829, 2023.

[17] S. Park et al., "GSM communication systems for IoT: SIM800L vs. SIM900 performance evaluation," in Proc. IEEE Int. Conf. Information and Communication Technology (ICICT), 2022, pp. 88–93.

[18] J. Hernandez et al., "Embedded safety systems for residential gas hazard detection: design and validation," IEEE Access, vol. 9, pp. 88423–88435, 2021.

[19] A. Ali et al., "Gas detection IoT models: review of sensor types, architectures, and deployment challenges," in Proc. Int. Conf. Electrical Engineering and Computer Science (ICECOS), 2019, pp. 1–6.

[20] R. Das et al., "Smart automation systems with AI-based predictive alerting for safety applications," in Proc. IEEE Int. Conf. Artificial Intelligence and Machine Learning (ICAIML), 2023, pp. 312–317.