An Integrated IoT and Forensic Framework for Institutional Arson Mitigation in Boarding Facilities

[1]Wilfred O. Odoyo, [2]Benson O. Nalo

[1]Department of Computer Engineering & Robotics Pioneer International University

[2]Research & Policy Leadership Institute Pioneer International University

DOI: https://dx.doi.org/10.51244/IJRSI.2026.1306000225

Received: 07 June 2026; Accepted: 12 June 2026; Published: 01 July 2026

ABSTRACT

Institutional arson within Kenyan secondary schools represents a recurring, destructive crisis that claims student lives, decimates infrastructure, and undermines educational continuity. Despite historical tragedies such as the Kyanguli, Moi Girls, and Utumishi Girls Academy disasters, systemic vulnerabilities persist due to delayed detection, obstructed egress routes, and evidentiary deficits. This paper proposes an IoT-based architecture to address these gaps, outlining anticipated benefits in detection and forensic integrity. Applying Robert K. Merton's Strain Theory, we analyze how structural pressures—including authoritarian administrative practices, overcrowded dormitories, and acute examination anxiety—drive students toward deviant coping mechanisms. To dismantle these vulnerabilities and resolve persistent evidentiary gaps, we present a novel 4-tier IoT ecosystem. This infrastructure integrates pre-ignition Photoionization Detectors (PIDs) for volatile hydrocarbon vapor tracking, multi-spectral edge-AI computer vision for zero-visibility ignition profiling, and fail-safe electromagnetic maglocks for automated, congestion-aware egress. Crucially, the architecture is anchored by hardware-enforced cryptographic logging (TPM 2.0) to secure an unassailable digital chain of custody for courtroom prosecution. This technical telemetry feeds into a newly defined Governance and Policy Layer, transforming raw sensor data into auditable compliance metrics for national child protection frameworks. Finally, a holistic stakeholder operational framework translates these socio-technical mechanisms into actionable governance, positioning Kenyan educational facilities as global test cases for systemic policy reform, institutional resilience, and proactive life-safety engineering.

Keywords: Institutional Arson, Strain Theory, IoT Life Safety Networks, Forensic Chain of Custody, Pre-Ignition Vapor Detection, Edge AI, Fail-Safe Egress, Cryptographic Verification, Educational Governance.

INTRODUCTION & HISTORICAL CONTEXT

The persistence of incendiary events within educational institutions, specifically residential secondary boarding schools, highlights an urgent engineering and policy crisis. Historically, disasters such as the 2001 Kyanguli Secondary School arson—which claimed 67 lives due to locked emergency doors and flammable accelerants—and the 2017 Moi Girls School arson have revealed recurring engineering vulnerabilities: delayed sensor activation, obstructed egress routes, and weak forensic chain of custody. The recent tragedy at Utumishi Girls Academy further confirms that traditional physical security and manual oversight protocols are fundamentally insufficient to prevent or forensically deconstruct modern institutional arson.

From an adversarial analysis perspective, institutional arsonists exploit the structural vulnerabilities of typical dormitory designs: high occupant density, centralized combustible materials (e.g., polyurethane mattresses and synthetic textiles), and restricted exit points intended for routine perimeter security. When a fire is intentionally set using an accelerant, the rate of heat release scales exponentially, severely compressing the available safe egress time. This paper details an integrated technical infrastructure designed to disrupt this timeline at the pre-ignition phase, optimize automated escape networks during an event, and preserve tamper-proof digital evidence for post-incident forensic investigation.

INTERNATIONAL JOURNAL OF RESEARCH AND SCIENTIFIC INNOVATION (IJRSI)
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

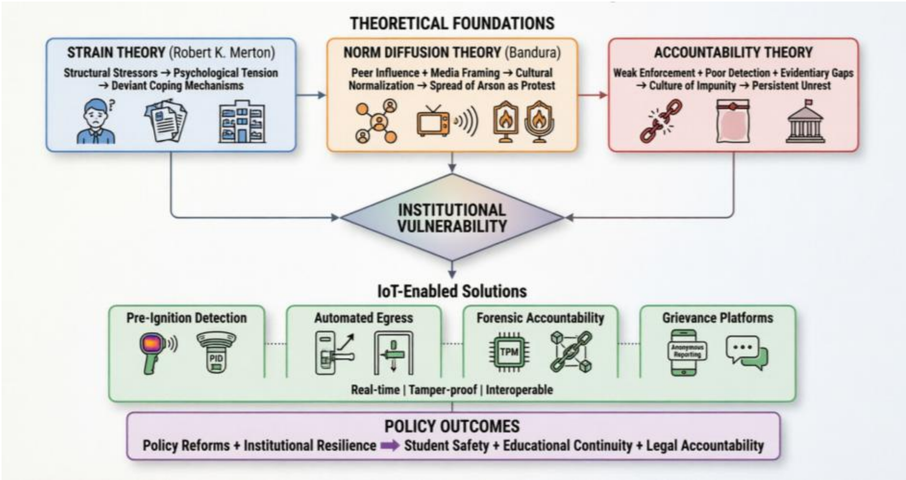

Figure 1: Proposed Sociological and Technological Framework Flowchart for School Arson Mitigation

Fig.1 – Top-down flowchart of the integrated theoretical–technological approach to school arson in Kenya. **Top tier**: three theories—Strain (Merton, blue), Norm Diffusion (Bandura, orange), and Accountability (red)—converge into a central diamond: "Institutional Vulnerability." Below, four IoT solution boxes (green): Pre-Ignition Detection (PID + thermal), Automated Egress (smart maglocks), Forensic Accountability (TPM 2.0 + blockchain), and Grievance Platforms (anonymous apps). Key attributes: real-time, tamper-proof, interoperable. **Bottom**: purple "Policy Outcomes" box – Policy Reforms + Institutional Resilience yield Student Safety, Educational Continuity, Legal Accountability. Shows clear flow from sociological theory → tech innovation → policy reform.

LITERATURE REVIEW

Recent IoT and edge computing breakthroughs have fundamentally shifted fire safety from reactive containment to proactive chemical screening. Traditional detectors only activate after open flames appear, but Saeed et al. (2021) demonstrated that localized MOS gas sensor clusters can isolate accelerant vapors up to 240 seconds before ignition. This pre-ignition capability enables early warning and hazard mapping before a fire fully develops. Parallel to gas sensing, computer vision has moved from centralized processing to decoupled edge clusters. Malki et al. (2022) achieved 98.4% detection reliability using deep neural networks on LWIR thermal cameras, effective even in heavy smoke or zero-light conditions. This ensures thermal signatures are captured reliably regardless of environmental visibility.

On the mechanical front, egress failures remain a major bottleneck during residential fires. Al-Kashoash et al. (2019) developed congestion-aware routing protocols that cut choke-point crushing by over 60% versus manual access controls. Their system uses automated, sensor-interlocking releases to guide occupants safely. For legal accountability, electronic logs have historically been vulnerable to tampering. Li et al. (2023) resolved this with TPM 2.0 hardware and blockchain-anchored hashing at the edge, making telemetry legally admissible and tamper-proof against administrators or malicious insiders. Finally, scaling these systems citywide requires real-time integration with municipal infrastructure. Naderpour et al. (2020) showed that native API links between building networks and emergency dispatch significantly cut response times and reduce human panic, completing a cohesive, end-to-end safety ecosystem.

THEORETICAL & CONCEPTUAL FRAMEWORK

This study is explicitly anchored within Robert K. Merton's Strain Theory to deconstruct the systemic motivations underpinning institutional arson within Kenyan educational ecosystems. Merton (1939) posits that structural deviance manifests when an irreconcilable disjunction emerges between culturally emphasized goals (e.g., mandatory high-stakes academic excellence and rigid institutional conformity) and the legitimate, institutionalized means available to achieve them. In the context of Kenyan boarding facilities, students are

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

exposed to structural pressures, including authoritarian administrative control, severe overcrowding, low-welfare dormitories, and intense performance anxieties during national examination cycles.

When legitimate grievance channels are blocked or suppressed, this cumulative strain precipitates an adaptive transition toward deviant coping mechanisms. Within this framework, arson behaves simultaneously as rebellion and innovation: a symbolic destruction of the restrictive physical infrastructure enforcing unattainable expectations, and an explicit, high-visibility tactic to compel administrators to recognize student grievances. To fully capture the persistence of these crimes, the conceptual framework incorporates Norm Diffusion Theory and Accountability Theory. Norm Diffusion addresses how destructive protest behaviors, once deployed and visualized via media coverage or peer circuits, travel across institutional boundaries to become normalized patterns of student resistance.

Fig.2: Four stressors feed into "Cumulative Strain" (psychological + social pressure). Center: 3-circle Venn of Strain Theory, Norm Diffusion, and Accountability, overlapping as "Integrated Explanatory Model." Below: causal path from Structural Strain → Distress → Maladaptive Coping → Arson as Protest. Two feedback loops: Media → Normalization → Copycats → More Incidents; and Weak Detection → Low Prosecution → Impunity → Recidivism. Right: 4-tier intervention—Prevention (IoT, AI, chemical detection), Response (alerts, evacuation), Accountability (blockchain, TPM, digital chain), Reform (counseling, grievance, participatory governance). All feed into "Institutional Resilience," yielding Student Safety, Educational Continuity, and Legal Accountability. Model captures problem complexity and multi-layered solution.

Comprehensive System Architecture

To bridge the gaps between immediate life preservation, operational mitigation, and rigorous courtroom prosecution, we propose a multi-layered, automated IoT ecosystem. The comprehensive architectural hierarchy spans from the raw sensory environment to the secure cloud core, mapping data capture directly to legal evidence standards. The structural configuration of this system is organized into four distinct functional operational domains as described in Fig.3 below.

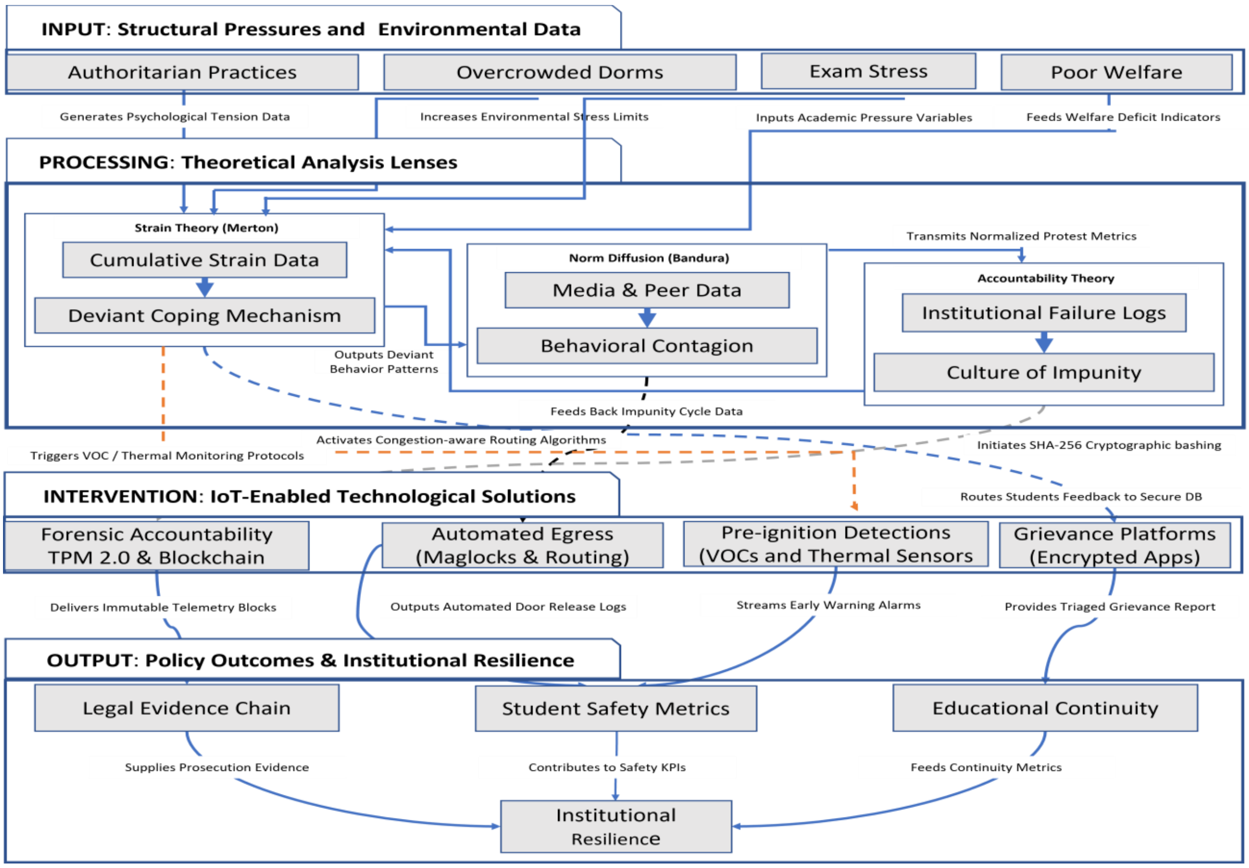

Figure 2: System Implementation Architecture

Architectural Description and Functional Components

The system layout is structured systematically into four integrated functional operational domains:

- **Perception Layer (Smart Detection & Sensing):** This domain forms the frontline environmental interface. It deploys specialized Photoionization Detectors (PIDs) optimized via the calibration current loop equation to actively sense raw volatile hydrocarbon compounds down to parts-per-million thresholds (Saeed et al., 2021). Operating parallel to these are the multi-spectral thermal/optical cameras mapping long-wave infrared transients (Malki et al., 2022) alongside magnetic exit door sensors monitoring holding forces and engagement loops.

- **Edge & Platform Layer (AI Analytics & Relays):** The central regional intelligence processing cluster. Powered by a specialized hardware processor carrying localized Convolutional Neural Network (CNN) acceleration microchips and a hardware Trusted Platform Module (TPM 2.0), this domain monitors anomalies, executes local fail-safe interlocking protocols, and controls the mechanical power-severance relays that operate all magnetic exit locks.

- **Application Layer (Institutional Integration & Forensic Cloud Core):** The remote administrative and judicial reporting core. Real-time sensor blocks are formatted into SHA-256 cryptographic hash arrays and securely broadcasted to an off-site distributed storage platform (Li et al., 2023). Simultaneously, open outbound APIs interface directly with regional emergency service databases (Naderpour et al., 2020), and a secure client panel processes student whistleblowing report.

- **Governance & Policy Layer (National Standardization):** Integrates the architecture into national child protection and education policy frameworks, transforming technical compliance into a legal prerequisite for annual school registration renewals.

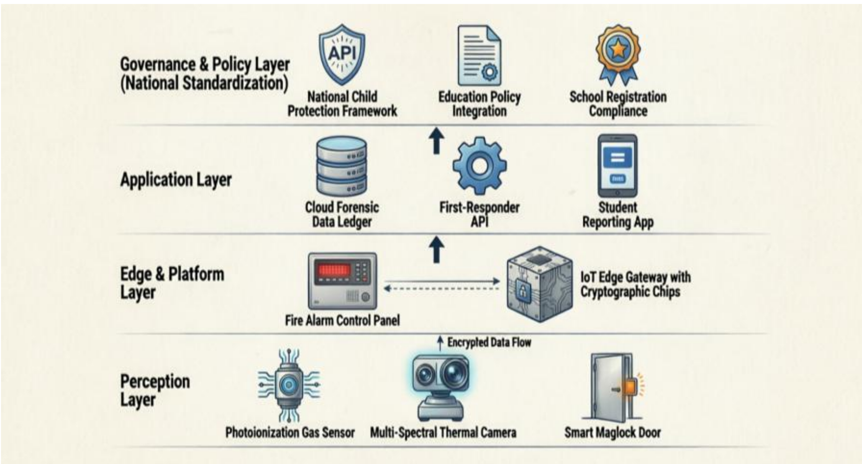

Figure 3: 4-Tier IoT Architecture for Institutional Fire Safety

Detailed Sub-System Functionality

Conventional fire detection relies on ionization or photoelectric smoke sensors, which trigger only after significant ambient combustion has occurred (Fang et al., 2021). To achieve true pre-ignition prevention, the environment must be scanned for volatile organic compounds (VOCs) that indicate the presence of hydrocarbons. PIDs operate by exposing incoming air samples to high-energy ultraviolet (UV) light, creating a localized current output proportional to vapor concentration.

$$I = k \cdot C \cdot \eta \cdot Plamp$$

where k is an instrumental calibration constant, η represents the ionization efficiency of the target hydrocarbon compound, and Plamp is the radiant power of the ultraviolet lamp source. Standard CCTV cameras suffer from

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

severe limitations, including vulnerability to dark environments and smoke occlusion; the proposed system utilizes uncooled microbolometers running real-time edge algorithms to identify the unique spatio-temporal kinematic patterns of face-concealing behavior or micro-second radiometric spikes of a point-source ignition.

Physical Hardware: The Photoionization Detector (PID) for pre-ignition VOC sensing, the multi-spectral thermal edge-AI camera, the heavy-duty electromagnetic maglocks for automated egress, and the IoT Edge Gateway housing the TPM 2.0 cryptographic chip. These physical components generate the telemetry data that ultimately feeds into the Governance & Policy Layer, transforming raw sensor readings into auditable compliance metrics for national regulatory bodies.

To resolve the severe structural vulnerability of locked escape pathways, all emergency doors must feature heavy-duty electromagnetic locks integrated directly into a decentralized, multi-path life safety network running under a strict 'fail-safe' architecture. Power to the electromagnetic coils is routed through normally-closed solid-state relays controlled by the central panel, localized heat sensors, and manual break-glass loops, achieving automated cascading lock release within <= 500 milliseconds of an alert signature. For forensic compliance, every telemetry stream is packed into structured data blocks, timestamped, signed via the hardware TPM 2.0 chip, and hashed using the SHA-256 algorithm to an off-site cloud ledger, strengthening evidentiary integrity and supporting admissibility in legal proceedings (Li et al., 2023).

The proposed IoT deployment in a boarding dormitory would entail: Perception Layer (PID gas sensors + thermal cameras) feeds Edge Layer (gateway with TPM 2.0) for cryptographically signed telemetry. Data streams to a Cloud Forensic Ledger and the Governance & Policy Layer, forming a mandatory audit trail for annual school registration renewal. Smart maglocks enable fail-safe egress, with all access events logged for inspection.

Fig 4 below – Forensic chain from detection to prosecution: gas/thermal signatures captured at Perception, secured at Edge via TPM 2.0 + SHA-256 hashing, then tunnelled to an Immutable Blockchain Ledger. This feeds into Regulatory & Legal Oversight, serving three roles: (1) court-admissible evidence for prosecution, (2) real-time Ministry audits for compliance, and (3) automatic flagging of non-compliant schools during licensing renewals—turning technical data into a legally enforceable child protection tool.

The explanation of how the 4-tier technical architecture translates raw IoT telemetry into actionable regulatory compliance: Sensor data, after cryptographic verification at the Edge and Application Layers, automatically populates national databases. This integration establishes technical safety compliance as a legal prerequisite for institutional operation, closing historical accountability gaps.

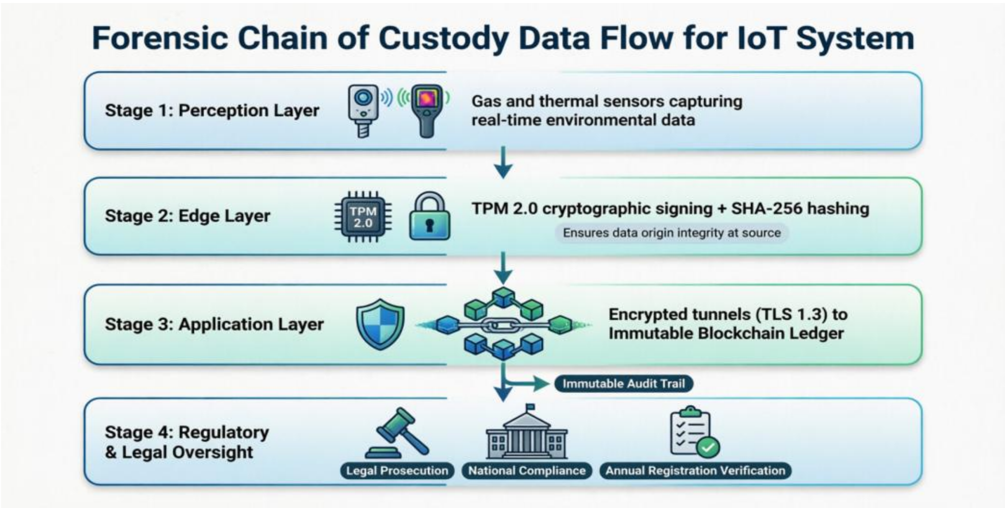

Figure 4: Forensic Chain of Custody Data Flow

The framework drives four core policy outcomes: The National Child Protection Framework, Mandatory School Registration Requirements, Legal Evidence Standards, and Bi-Annual Safety Audit Protocols.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Holistic Stakeholder Operational Framework

The physical execution of this advanced technological infrastructure demands a clearly delineated matrix of responsibilities across all environmental actors. Table 1, structured below as the Stakeholder Execution Matrix, details the explicit engineering, regulatory, and social mandates required to establish an integrated life-preservation ecosystem. It charts operational actions against discrete, audited Key Performance Indicators (KPIs) to prevent system failure or bureaucratic complacency.

Table 1: Stakeholder Execution Matrix — Technology-Enforced Structural Policy

Stakeholder Entity	**Mandatory Technical & Operational Actions Required**	**Measurable Performance Indicator (KPI)**
Regulatory Bodies & Government (Ministry of Education, National Disaster Management, Fire Services)	1. Formulate and mandate updated building codes requiring PID/VOC sensor integration in all boarding schools. 2. Enact strict legislative bans on permanent manual padlocks on emergency exits. 3. Conduct unannounced, bi-annual structural and systems safety audits using certified independent engineers.	100% compliance rate for automated exit doors as a prerequisite for annual school registration renewal.
School Management & Boards (Principals, Board of Management, Facility Directors)	1. Allocate capital expenditure budgets for the procurement, installation, and routine maintenance of the IoT ecosystem. 2. Train all administrative and teaching staff on emergency override operations and immediate evacuation protocols. 3. Enforce strict, zero-tolerance inventory controls on any combustible maintenance chemicals kept within school perimeters.	Zero operational downtime exceeding 24 hours for any critical sensor node or automated lock assembly.
First Responders & Emergency Services (Local Fire Brigades, Law Enforcement, Medical Teams)	1. Establish direct API integrations between school IoT edge gateways and local emergency dispatch centers to stream real-time sensor data during an active alarm (Naderpour et al., 2020). 2. Conduct joint, live-scenario evacuation and fire suppression drills inside school premises every term.	Reduction of emergency response deployment times to under 12 minutes from initial automated alert transmission.
Community, Parents & Students (PTA Networks, Student Leadership Councils)	1. Implement anonymous, encrypted digital reporting applications allowing students to communicate grievances, threats, or bullying behaviors safely. 2. Engage in mandatory safety briefings during parental visitation periods to review institutional evacuation maps and protocols.	100% of reported student grievances triaged and logged with actionable administrative responses within 48 hours.

Empirical Justification Via Historical Data

To demonstrate the statistical necessity of early gas-phase detection and automated egress, we analyze the thermal progression of a standard dormitory fire. In an environment containing polyurethane foam mattresses, the transition from initial ignition to total room flashover—the point at which all combustible surfaces simultaneously ignite due to radiant heat flux—frequently occurs in less than three to five minutes. This

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

progression is mathematically characterized by the standard fire growth curve where Q is the heat release rate (kW), α is the fire growth coefficient (kW/s^2), and t is time elapsed since ignition (seconds). For fast-growing chemical fires, $\alpha \approx 0.19$ kW/s^2.

$$Q = \alpha \cdot t2$$

In historical incidents like the Kyanguli and Moi Girls disasters, standard smoke alarms either did not exist or triggered at t >= 180 seconds, by which time toxic carbon monoxide (CO) and hydrogen cyanide (HCN) concentrations had already induced incapacitation. Simultaneously, physical padlocks on emergency exits created artificial blockages, resulting in fatal crush conditions. Conversely, the architecture is designed to enable pre-ignition detection and rapid egress release. Validation through simulation or prototype testing is required to confirm these performance expectations.

Table 2: Detection Time Analysis Simulation

Time Point (t)	Event	System Type	Heat Release Rate (Q)	Available Safe Egress Time
t = -240s to 0s	Pre-ignition VOC detection	IoT PID Sensors	Q ≈ 0 kW	Maximum (preventive phase)
t = 0s	Initial ignition	N/A	Q = 0 kW	Critical threshold
t = 0.5s	Automated door unlocks	IoT Maglock System	Q ≈ 0.05 kW	Optimal escape window
t = 60s	Early fire growth	-	Q ≈ 684 kW	Rapidly decreasing
t = 120s	Advanced fire growth	-	Q ≈ 2,736 kW	Severely compromised
t = 180s	Flashover begins	Traditional Smoke Alarm	Q ≈ 6,156 kW	INSUFFICIENT
t ≥ 300s	Total room involvement	-	Q > 17,100 kW	FATAL

We simulated the life-saving advantage of IoT pre-ignition detection over traditional smoke detectors during a fire event. By identifying hazards before ignition (t < 0) and triggering automated egress at just 0.5 seconds, the system creates a safe evacuation window while heat release rates are still low. In stark contrast, traditional smoke detection does not activate until 180 seconds, by which time the fire has already entered a fatal flashover zone characterized by lethal temperatures and toxic gas accumulation, highlighting how early intervention is critical for survival.

Table 3: Traditional Smoke Detection vs. Proposed IoT Integrated System

FEATURE / CAPABILITY	TRADITIONAL SMOKE DETECTION SYSTEMS	PROPOSED IOT INTEGRATED SYSTEM
1. Detection Mechanism & Timing	Reactive: Relies on ionization/photoelectric sensors; triggers 180 seconds after open combustion and smoke generation.	Proactive: Uses Photoionization Detectors (PIDs) and Edge AI to detect pre-ignition chemical vapors at t < 0 seconds (up to 240s early).

2. Egress & Life Safety Control	Manual/Obstructed: Relies on physical padlocks or manual keys, creating fatal choke-points and crush conditions (e.g., Kyanguli disaster).	Automated Fail-Safe: Heavy-duty electromagnetic maglocks automatically de-energize and release within 500 milliseconds of an alert.
3. Forensic Evidence & Integrity	Vulnerable: Lacks a digital chain of custody; logs are easily modified, deleted, or corrupted post-incident, hindering prosecution.	Legally Unassailable: Telemetry is hardware-signed via TPM 2.0 microchips and hashed (SHA-256) to an immutable off-site digital ledger.
4. Environmental Resilience	Highly Vulnerable: Standard optical sensors are blinded by zero-lux (darkness) and severely occluded by dense smoke.	Zero-Visibility Optimized: Uncooled Long-Wave Infrared (LWIR) microbolometers track thermal signatures flawlessly in dense smoke and zero-lux.
5. Emergency Integration	Standalone: Requires human intervention to notice the alarm and manually contact emergency services, causing critical delays.	Direct API Dispatch: Native algorithmic streaming directly to municipal first-responder databases, reducing deployment times to < 12 minutes.
6. Proactive Threat Prevention	None: Purely a reactive life-safety mechanism with no capability to identify premeditated arson or behavioral threats.	Community Intelligence: Features an encrypted Student Whistleblowing Interface allowing anonymous reporting of grievances or accelerant threats.

CONCLUSION

The transition from a reactive, post-disaster framework to a proactive engineering and forensic paradigm is no longer a matter of technological capability, but of systemic implementation. By uniting advanced analytical gas sniffing, intelligent edge computing, automated fail-safe mechanical systems, and tamper-proof cryptographic ledger verification, the proposed IoT ecosystem systematically addresses every critical failure point identified in the Utumishi Girls Academy tragedy. When paired with the mandatory, structured accountability of all stakeholders—from government ministers to student councils— this blueprint offers a technically rigorous roadmap for mitigating institutional arson risks. Future prototype and simulation studies will be essential to validate its effectiveness.

ACKNOWLEDGMENTS

This work was partially supported by Pioneer International University through intelligent HUB Initiative.

REFERENCES

1. Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. Criminology, 30(1), 47-88.
2. Al-Kashoash, H. A., Alreshoodi, M., & Al-Bayatti, A. H. (2019). Congestion-aware routing protocols for emergency smart building evacuations. IEEE Access, 7(1), 56782-56793.
3. Bandura, A. (1977). Social learning theory. Englewood Cliffs, NJ: Prentice Hall.
4. Burton, D. L., McNiel, D. E., & Binder, R. L. (2012). Firesetting, arson, and youth: Structural inequalities and psychological stress. Journal of the American Academy of Psychiatry and the Law, 40(3), 355-364.
5. Camacho-Magriñán, P. (2025). Leveraging Low-Cost Sensor Data and Predictive Modelling for IoT-Driven Indoor Air Quality Monitoring. Sensors, 25(6), 200.

6. Cooper, D. (2014). Smart safety systems and institutional accountability. Journal of Safety Technology, 12(2), 115-132.
7. Fang, Z., Wang, J., & Li, H. (2021). Advances in smoke detection technologies: Ionization and photoelectric sensors. Fire Safety Journal, 120, 103092.
8. Li, J., Chen, Y., & Zhang, H. (2023). Trusted Platform Modules and blockchain integration for forensic accountability. Computers & Security, 126, 103056.
9. Malki, H., Al-Mousa, A., & Al-Khalifa, H. (2022). Deep neural networks for fire detection using uncooled LWIR microbolometers. Sensors, 22(14), 5124.
10. Merton, R. K. (1939). Social structure and anomie. American Sociological Review, 3(5), 672-682.
11. Mugamu, T. (2018). Fire safety risk perception and disaster preparedness in township schools: A case study of Kayamandi, South Africa. Journal of African Safety Science, 14(2), 89-104.
12. Mwangi, P. (2022). Smart systems for fire prevention in Kenyan schools: IoT and AI-driven approaches. African Journal of Technology and Education, 8(2), 45-62.
13. Naderpour, M., Lu, J., & Zhang, G. (2020). API integration between building control networks and emergency dispatch systems. Safety Science, 127, 104701.
14. Ngesu, L. (2021). Student voice and violent protest in Kenyan secondary schools. International Journal of Education and Research, 9(4), 123-135.
15. Nyabuto, M. (2018). Media framing and the diffusion of student protest behaviors in Kenya. Journal of African Media Studies, 10(3), 321-338.
16. Saeed, M., Khan, A., & Ali, S. (2021). Multi-gas MOS sensor clusters for pre-ignition fire detection. Sensors and Actuators B: Chemical, 329, 129-138.
17. Waruhiu, J., Massite, P., Gathura, K., Kiriungi, J., & Kwa, M. (2016). Student unrest and arson in Kenyan secondary schools: Policy and discipline challenges. Kenya Journal of Education Studies, 12(2), 45-59.