**ENHANCING PRISON SECURITY THROUGH AN IOT BASED POWERED SYSTEM MONITORING AND ALERTING DURING JAIL BREAK AND ATTEMPTS**

**Abstract**

Prison security remains a critical challenge, especially preventing escape attempts and unauthorized movements within facilities. With the rapid advancement of Internet of Things (IoT) technology, intelligent security systems can now offer real-time monitoring and alerts. This paper proposed an IoT-based prison security system powered with backup support to monitor and alert during jailbreak attempts. Three major methods are suggested to improve system performance: The system integrates Multi-Sensor Fusion for Precise Intrusion Detection System (MS-PIDS), including PIR motion detectors, vibration sensors, ultrasonic sensors, and door magnetic sensors, to detect unusual activities in and around the prison. These sensors are connected to a central Microcontroller Unit (MCU), which processes the Time-Based alert logic to Reduce False Alarms (TB-RFA), sensor inputs, checks for intrusion conditions during restricted hours, and triggers appropriate alerts. Then GSM-Based Priority Notification for Timely Response (NTR). A buzzer is activated if a critical threat is detected, and the GSM module sends SMS notifications to security personnel. To ensure reliability, the system includes a power backup unit that activates during power failure and a health check module that continuously monitors the operational status of each component. The Workflow of the system employs mathematical models to quantify response time, logging rate, and memory usage. Results from simulation and implementation confirm that the proposed system can provide fast alerts, accurate threat detection, and robust monitoring, even during power outages or system faults, significantly improving prison safety and response readiness.

**Keywords:** IoT, Prison Security, Intrusion Detection, GSM Alert, Sensor Monitoring, Power Backup, Real-Time System.

**1. Introduction**

The rise of IoT technology offers a transformative solution by enabling automated, real-time monitoring systems that can improve situational awareness and response time in such environments. IoT-based systems integrate smart sensors with microcontroller platforms to continuously monitor physical conditions and detect anomalies [1].

Ensuring prison security is a critical concern for public safety and law enforcement, particularly in high-risk correctional facilities where the possibility of jailbreak attempts remains a constant threat [2]. Traditional security measures, such as manual patrolling and CCTV surveillance, often fall short in providing real-time detection and response, especially during power outages or when unauthorized activities occur in blind spots [3]. Additionally, many traditional systems are highly dependent on continuous power supply and do not offer automated real-time notifications, creating vulnerabilities during power outages or in quick escape attempts [4].

There is also a lack of integrated monitoring and centralized decision-making, which can delay response time and coordination during critical incidents. Early detection and fast communication to the appropriate authorities can make the difference between a failed and a successful escape attempt [5].

The system presented here tackles such issues by implementing three main mechanisms: Multi-Sensor Intrusion Detection, Time-Based Alert Filtering, and Priority-Based GSM Notification Logic. These mechanisms reduce false alarms, enhance detection accuracy, and facilitate responsive action. With this innovative and fault-resistant architecture, the system seeks to significantly improve correctional institutions' security and operational effectiveness.

**2. Related Work**

The author suggests that scholars focus their attention on Research initiatives that affect participants and researchers alike may benefit from unintended consequences. They offer insights on how art workshops foster a sense of community and connection between the participants and the researcher [6]. The "Prison Break Monitoring and Alert System" paper is a prime example of how wireless communication and the Internet of Things may be used to improve the security of correctional facilities. By offering it greatly lowers the dangers of prison escapes with real-time surveillance and immediate alarms, protecting both staff and convicts [7]. In order to maintain the growth of smart prisons (PB-WC), the study highlights the significance of ongoing assessment, international cooperation, and adherence to ethical norms. The outcome demonstrated the significance of smart prisons in the realm of corrections [8]. It is advised that the minimal standards for inmate care set out by the UN Congress on crime prevention and offender treatment be followed [9]. The chapter examines how a student club brought together parents, educators, and students to challenge the conventional aims of public education and provide a place for liberator learning using counter stories gleaned from kitchen table conversations. Multiracial resistance, the value of community and connections, and building resilience and strength are some of the emerging themes [10]. These scenarios' unique narrative patterns demonstrate Sequential Break's adaptability PBMAS to different prompt forms outside of those covered. Numerous tests show that Sequential Break only requires one query to produce a significant increase in attack success rate above current benchmarks for both closed-source and open-source models [11]. It is a drastic change from Norwegian prisons, where officers' primary responsibilities are to communicate with inmates and establish connections with them that this incarceration resulted in such stringent security measures, such as the jail guard speaking to Breivik as little as possible [12].

The purpose of this study is to elucidate the factors that led to the paradigm change. It accomplished this by first describing the jail security management tactics that Italy has been promoting for the past few decades. Second, by examining both the "inside" and "outside" of prisons, it explores the current shift away from dynamic security [13]. This research explains and addresses the dehumanizing and (de) socializing practices used in prison schooling. We examine efforts to challenge jail school teaching and its effects using a socioracial literacy course that incorporates abolitionist action [14]. The analysis of the uniformed staff's experiences and views of the new regime focuses on the impact of the prison's complex environment and the symbolic order created throughout rehabilitation [15]. The "digital vulnerability" of inmates, that is, the relationship between the vulnerabilities of inmates using remote communication tools like videoconferencing or video links and the potential for digital inequality to be exacerbated or resolved, will be the main topic of this article [16]. They discovered that while inmates and staff generally held similar values, their relative priorities differed significantly, indicating the different roles that each play in the prison's operation [17]. The results broaden the knowledge of judicial consciousness of jail life and shift the scholarly focus of judicial decision-making from the amount to the quality of punishment [18]. According to the study, even though cyberspace offers opportunities for social interaction, idea sharing, information sharing, business dealings, and other activities, it is still vulnerable to cyber threats like ransom ware, fraud, terrorism, war, trafficking, and privacy violations [19]. Since it examines the growing potential of activists' engagement in intersectional and transnational narratives, the relationship between resistance practices inside Israeli colonial prisons and the various degrees of solidarity created outside of prisons is a difficult new area of study to address in Palestine Studies [20].

**3. proposed method**

The purpose of the proposed method is to develop a real-time prison security system using IOT-based monitoring and warning mechanisms to effectively detect, report and react to Prison security efforts. This method integrates a network of smart sensors with microcontroller, real -time communication module and centralized data logging during potential security violations.

**Architecture Diagram**

Motion

Sensors

Door

Contact

Sensors

Vibration

Sensors

Ultrasonic

Sensors

**loT-Based Sensor Deployment using** **MS-PIDS**

Real-Time Alerting using NTR and TB-RFA

Alert

GSM

Module

Buzzer/

Siren

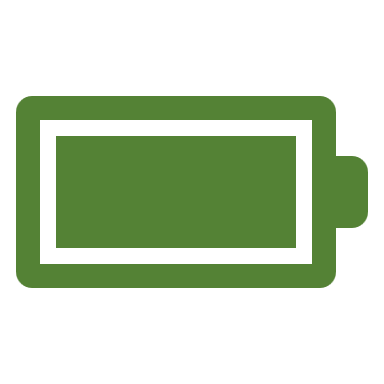
Mobile/

WebApp

Microcontroller

Power

Backup



Battery

**Figure 1. Architecture Diagram for Proposed Method**

The proposed prison security system uses IoT devices to monitor and alert authorities during jailbreak attempts. The system starts with different sensors, such as motion sensors, vibration sensors, ultrasonic sensors, and door sensors, placed in key areas of the prison. These sensors constantly watch for unusual activity, such as forced doors, movement during lockdown, or wall tampering. All the data from these sensors is sent to a MCU such as an Arduino or Raspberry Pi. The MCU checks the inputs to detect any suspicious behavior. If something unusual is found—especially during restricted hours, like nighttime—the system treats it as a potential security breach. Once a breach is detected, the system does two things: triggers a local alert—sounds a buzzer or siren inside the prison. It also sends a remote alert—uses a GSM module to send an SMS alert to the jail authorities. A priority system decides whether the situation is critical. If it is, the message is sent immediately. If it’s less serious, it’s just recorded for later review. All events—both normal and abnormal—are stored in a Monitoring and Logging System. This helps with future analysis or investigations. To ensure the system always works, a power backup (like a battery or UPS) is included. If the main power goes off, the backup takes over automatically. Lastly, a Health Check Module monitors whether all parts of the system are working properly. If something stops working, the system sends a maintenance alert.

**3.1 Multi-Sensor Based Precise Intrusion Detection System (MS-PIDS)**

The system's first component involves deploying various IoT sensors across the prison facility. These sensors monitor key areas such as cell doors, fences, walls, and high-security zones. The following types of sensors are used: Motion Sensors Detect unauthorized movement near restricted areas or cell doors. Vibration Sensors: Detect any tampering with walls, fences, or other structural components. Door Contact Sensors: Determine whether a door has been forcibly opened. Ultrasonic Distance Sensors: Detect any unexpected distance changes, such as a breached wall.

Where: equation 1, = Intrusion Detected, = Motion Detected, = Vibration Detected, = Door Forced Open, = Unexpected Ultrasonic Distance Change. If any sensor is triggered, the system will treat it as an intrusion and move to the next stage.

I=M ∨ V ∨ D ∨ UI (1)

These sensors send real-time data to a microcontroller (e.g., Arduino or Raspberry Pi), where the data is analyzed to check for abnormal readings. If any sensor value exceeds a predefined threshold (indicating a potential breach), the system triggers an alert, indicating possible security threats.

**3.2 GSM-Based Priority Notification for Timely Response (GSM-NTR):**

The real-time warning mechanism becomes active once the system detects a violation or suspicious activity. This mechanism is designed to inform security personnel immediately, which allows for a sharp response. The system sends alerts through various channels, such as SMS notification using GSM modules and sending a text message to the safety team or relevant officers. Mobile/Web Notification: Alert is sent to a centralized dashboard or mobile app for real-time monitoring.

The Equation 2, N = Notification Signal (1 = Send SMS), A = Alert Triggered, P = Priority Level (1 = Critical, 0 = Low-Priority) in equation 2.

(2)

To ensure that important events are given immediate attention, a priority system is used to classify the alert based on the event's severity. Important events trigger immediate notifications, while low-primary alerts are logged in to analyzed.

A power backup system is integrated into the system to provide continuity for the monitoring and alerting system in case of power failure or sabotage. The component provides continuity for the sensors, controllers, and notification modules even in case of power failure.

Power backup is done using a rechargeable battery or an Uninterruptible Power Supply (UPS), so that the system stays up. The system will automatically switch to backup power in the event of a power supply failure.

(3)

Where: equation 3, = b. = Availability of backup battery power. The system will remain active and functional as long as either the main power or backup battery is available.

The proposed system combines advanced IoT technology with real-time alerting and power backup integration to create a robust, responsive security solution for prison environments. By detecting intrusions early and responding quickly, the system helps prevent jailbreak attempts and enhances overall security management.

**4. Result and Discussion**

This section introduced real-world testing results and intensive evaluation of the suggested IoT-based jail monitoring and alert system. The assessment was based on some major performance indicators, such as reaction time, accuracy of alert, system reliability in terms of power loss, and lowering false alarms. The suggested approach, including multi-sensor infiltration detection, time-based alert logic and GSM-based notification, exhibits notable improvements compared to traditional jail security methods in terms of accuracy and efficiency.

**Table 1. Hardware and System Setup**

|  |  |
| --- | --- |
| Parameter | Value |
| Microcontroller | Arduino Uno (ATmega328P) |
| Sensors Used | PIR, Vibration, Ultrasonic, Magnetic Door Sensor |
| Communication Module | GSM SIM800L |
| Power Backup | 12V Rechargeable Battery |
| Total Response Time | 5.2 seconds |
| Test Environment | Simulated Jail Setup (Room Scale) |
| Intrusion Types Tested | Motion, Vibration, Door Breach |
| Power Failure Simulation | Yes (UPS Simulation Active) |

As shown in Table 1, the system was deployed in a scaled-down prison environment where multiple intrusion scenarios were simulated. The results confirmed that the multi-sensor-based intrusion detection logic reduced false positives by validating each suspicious activity using data from multiple sources. For example, during the day a standalone PIR sensor trigger did not result in an alert unless it coincides with limited hours and other sensor inputs, verifying the innovative filtering feature of the system.

**Figure 2: Detection Accuracy**

Figure 2 displays a comparative study of detection precision for three implemented models: PB-WC, PBMAS, and MS-PIDS. Detection precision was analyzed in three different scenarios, with 30, 60, and 100 sensor sample sizes. As sensor inputs increased, detection performance improved across all models. PB-WC showed a gradual increase in accuracy from approximately 15% at 30 samples to 50% at 100 samples. PBMAS performed better, reaching around 60% detection accuracy at the highest sensor input level. The outcomes demonstrate the effectiveness of the MS-PIDS methodology in accurately identifying intrusion or breach attempts in the prison setting.

**Figure 3: False Positive Rate**

Figure 3 presents a comparative evaluation of the false positive rate for three intrusion detection models—PB-WC, PBMAS, and the proposed MS-PIDS —across varying node quantities (10, 30, 80, and 100). In contrast, the MS-PIDS system always had the lowest false favorable rate, never more than 30%, even at 100 nodes. The ability to differentiate between real threats and environmental noise makes MS-PIDS more reliable for jail settings, where accuracy in alerting is paramount to avoid unnecessary nervousness or misuse of resources.

**Figure 4: Memory Usage per Event**

Figure 4 compares the memory usage per event across three systems— MS-PIDS, PBMAS, and PB-WC—at different event volumes (20, 50, and 100). The MS-BIDS model consistently demonstrated the most efficient memory handling. At 100 events, it used approximately 45 KB, while PBMAS and PB-WC consumed about 65 KB and 80 KB, respectively. MS-BIDS' lower memory requirement stems from its highly optimized event processing, which logs only meaningful multi-sensor information. PB-WC and PBMAS are more likely to log redundant or raw data, resulting in higher memory requirements. This efficiency is important in large-scale prison environments where hundreds of events can be logged daily.

**Figure 5: Notification Time**

Figure 4 compares notification time for three models— MS-PIDS, PBMAS, and PB-WC—based on the number of events recorded. The MS-PIDS system consistently delivered the fastest notification time, averaging around 30 seconds for 100 events. PBMAS followed closely behind, while PB-WC showed a significant delay, reaching nearly 70 seconds at the highest event count. This minimized response time in MS-PIDS proves its capability of swift processing and forwarding of alerts, which is critical for real-time intervention in security during breach attempts. The lag in PB-WC reflects inefficiencies in fundamental detection and the forwarding of alerts; thus, it is less dependable in critical situations.

**5. Conclusion**

This paper offered an IOT-based system to increase prison security by accurately monitoring and warning officers during jailbreaks or suspicious movements. The system integrates three major modules: PB-WC, PBMAS, and proposed MS-PIDS. MS-PIDS combines data from several sensor types to achieve high accuracy and reliability. Performance evaluation through simulation showed that MS-PIDS detects accuracy, false favorable rates, notification time and other models have been improved in detecting memory efficiency. It achieved accuracy to detect more than 85% in high node deployment and maintained less than 30% false positive rate on 100 nodes. In addition, it reduces the consumption of notification time and memory, which facilitates quick transmission of alerts and effective use of resources. Such results prove that the fusion of multi-sensor data and creative decision mechanisms especially enhances the system's ability to detect real threats, limiting false alarms. The advocated system in this letter improves the monitoring and monitoring of the jail and timely interferes during the operation of potential migration, thus improving institutional safety and operational efficiency.

**References**

1. Chandra, P. Satish, K. Indu, J. Sheshank, J. Prashanth, and K. Vamshi. "Iot Based Prison Break Monitoring And Alert System Using Wireless Communication." International Journal of Engineering Research and Science & Technology 20, No. 2 (2024): 229-235.
2. Imandeka, Ejo, Panca Oktavia Hadi Putra, Achmad Nizar Hidayanto, and Mufti Mahmud. "Exploring the World of Smart Prisons: Barriers, Trends, and Sustainable Solutions." Human Behavior and Emerging Technologies 2024, no. 1 (2024): 6158154.
3. Saiem, Bijoy Ahmed, M. D. Shanto, and Rakib Ahsan. "SequentialBreak: Large Language Models Can be Fooled by Embedding Jailbreak Prompts into Sequential Prompt Chains." arXiv preprint arXiv: 2411.06426 (2024).
4. Murray, Conor, Brendan Coyle, Haydyn Morgan, Ian Marder, David Woods, Tandy Haughey, Matthew Maycock et al. "International consensus statement on the design, delivery and evaluation of sport-based interventions aimed at promoting social, psychological and physical well-being in prison." BMJ open 14, no. 1 (2024): e075792.
5. Omel’chenko, Elena L., Albina R. Garifzyanova, and Judith Pallot. "‘Humiliation, shame and torment’: Continuity and change in the statuses and power hierarchies in the post-Soviet prison system." Incarceration 5 (2024): 26326663241257360.
6. Power, Erin, Maria Adams, Vicki Harman, Jon Garland, and Daniel McCarthy. "‘Connection Rather Than Output’: Reflections on the Role of Art Workshops in Qualitative Research with Women in Prison." International Journal of Qualitative Methods 23 (2024): 16094069241273593.
7. Chandra, P. Satish, K. Indu, J. Sheshank, J. Prashanth, and K. Vamshi. "Iot Based Prison Break Monitoring and Alert System Using Wireless Communication." International Journal of Engineering Research and Science & Technology 20, No. 2 (2024): 229-235.
8. Imandeka, Ejo, Panca Oktavia Hadi Putra, Achmad Nizar Hidayanto, and Mufti Mahmud. "Exploring the World of Smart Prisons: Barriers, Trends, and Sustainable Solutions." Human Behavior and Emerging Technologies 2024, no. 1 (2024): 6158154.
9. Amali, Sadiq Ewaoda, Tinyiku D. Ngoveni, and Muzukhona Wilfred Buthelezi. "Prison-Based Factors and Deviant Behaviors amongst Inmate in Selected Correctional Centers in IIorin, Kwara State, Nigeria." African Journal of Criminology and Justice Studies 14, no. 2 (2025): 1.
10. Ramirez, Guadalupe, Steven Flores, Kyndall Jackson, Breanna Lopez, Dulce Gonzalez, and Aayla Holiday. "Jailbreak! Students, Parents, and Teachers Practicing Fugitivity and Freedom Dreaming." In Youth Resistance for Educational Justice, pp. 139-152. Routledge.
11. Saiem, Bijoy Ahmed, M. D. Shanto, and Rakib Ahsan. "SequentialBreak: Large Language Models Can be Fooled by Embedding Jailbreak Prompts into Sequential Prompt Chains." arXiv preprint arXiv: 2411.06426 (2024).
12. Sørensen, Knut Mellingsæter. "Do Risk-Reducing Measures Only Reduce Risk? Prison Officer Work with Risk-Reducing Measures in the Imprisonment of a High-Risk Prisoner." In Prison Officers: International Perspectives on Prison Work, pp. 299-323. Cham: Springer International Publishing, 2023.
13. Chisari, Chiara. "Transitioning From Dynamic Security In Italian Prisons: Assessing The Influence Of Perceived Insecurity On Prison Management." Rassegna Italiana Di Criminologia 3 (2023): 240-251.
14. Annamma, Subini A., Brian Cabral, Brianna Harvey, Jennifer M. Wilmot, Annie Le, and Jamelia Morgan. "“When We Come to Your Class… We Feel Not like we’re in Prison”: Resisting Prison-School’s Dehumanizing and (De) Socializing Mechanisms Through Abolitionist Praxis." American Educational Research Journal 61, no. 1 (2024): 3-47.
15. Santorso, Simone. "Rehabilitation and dynamic security in the Italian prison: Challenges in transforming prison officers’ roles." The British Journal of Criminology 61, no. 6 (2021): 1557-1574.
16. McKay, Carolyn, and Kristin Macintosh. "Digital vulnerability: People-in-prison, videoconferencing and the digital criminal justice system." Journal of Criminology 57, no. 3 (2024): 313-333.
17. Seel, Christopher J., Katy Holloway, Ioannis Angelakis, and Jennifer L. Austin. "Finding common ground: Using focus groups to define values among prisoners and staff." Journal of positive behavior interventions 26, no. 2 (2024): 67-78.
18. Dagan, Netanel, and Shmuel Baron. "Taking prison to court: Exploring the judicial review of prison decision-making through Supreme Court judges in Israel." The British Journal of Criminology 64, no. 4 (2024): 913-930.
19. Ezeji, Chiji Longinus. "Cyber policy for monitoring and regulating cyberspace and cyber security measures for combating technologically enhanced crime in South Africa." International Journal of Business Ecosystem & Strategy (2687-2293) 6, no. 5 (2024): 96-109.
20. Daniele, Dr Giulia, and João Pedro Borralho. "Palestinian Hunger Strikers in the Israeli Settler-Colonial and Carceral System: Uniting Inside and Outside Resistance, Local and Transnational Solidarity." Journal of Holy Land and Palestine Studies 24, no. 1 (2025): 73-97.