Power System Technology
ISSN:1000-3673

Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

Secure Offline Surveillance and Data Logging System for Detecting Unauthorized Alien Movement in Remote U.S.A Entry Zones

Isabirye Edward Kezron
Independent Researcher

Abstract:- The security of remote United States entry zones, particularly those bordering sparsely populated and infrastructure-deficient areas**,** has become a mounting concern for national security agencies. These locations are increasingly exploited for unauthorized crossings, surveillance blind spots, and logistical loopholes. Traditional surveillance technologies such as drone patrols, satellite imagery, and wireless camera networks rely heavily on constant connectivity and centralized data transmission. In many remote regions, however, these dependencies render such systems ineffective, unreliable, or economically unsustainable due to terrain, signal interference, and high maintenance requirements.

To address this critical gap, this study proposes the design and development of a secure, offline surveillance and data logging device intended to detect unauthorized human movement across border regions without relying on real-time internet access or external control infrastructure. The system combines passive infrared (PIR) motion sensors, a low-energy microcontroller unit (MCU), and local encrypted data storage housed in a weather-resistant, tamper-resistant casing. Its purpose is to autonomously monitor entry points, detect human presence, and securely log these events with time stamps and sensor-triggered metadata, all while operating on limited power resources such as long-life batteries or compact solar panels.

This research presents both the hardware and software architecture of the device, including its modular component design, logic control sequences, data encryption methods, and power optimization strategies. The device was field-tested in simulated remote environments to assess its detection accuracy, false positive rate, storage reliability, and battery efficiency under different weather and terrain conditions. The results indicate that the prototype can maintain continuous operation for multiple weeks without manual intervention, while maintaining data integrity and reliable motion capture over various environmental stressors.

One of the most critical features of this system is its entirely offline capability. By eliminating real-time data transmission, the device reduces exposure to hacking, jamming, and signal-based interference issues common to networked systems. Furthermore, the cost of deployment is significantly lower, making it feasible for large-scale installations along low-priority or

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

difficult-to-access borders. Its low visibility and passive operation also help reduce detection and tampering by intruders.

In addition to performance results, this paper discusses the broader implications of integrating such devices into national border security frameworks. Topics include deployment logistics, system limitations, ethical considerations related to surveillance, and potential future enhancements. These enhancements may include the integration of lightweight machine learning algorithms for behavioral analysis, as well as hybrid offline-online synchronization protocols for batch data uploads where periodic connectivity is possible.

Ultimately, the proposed device fills a niche that is currently underserved by high-tech but connectivity-reliant systems. It offers a low-cost, resilient, and scalable solution for border surveillance, rural facility monitoring, and other national security scenarios where real-time systems are either impractical or vulnerable. The findings of this research could inform future defense procurement strategies and influence how physical security infrastructure is developed for decentralized environments in the modern era of digital surveillance.

Keywords: Offline surveillance, Motion detection system, Border security, Data logging device, Unauthorized entry monitoring, Remote sensor technology, National security infrastructure

1. Introduction

The security of national borders has long been a matter of strategic importance, particularly in nations with expansive geographic territories and varied terrain. In the United States, the southern and northern borders present unique challenges to policymakers, border patrol agents, and national defense strategists. While urban ports of entry and border cities are typically monitored with advanced surveillance systems, the vast, sparsely populated, and infrastructure-limited areas between official entry points remain particularly vulnerable. These regions, often spanning rugged desert, forest, or mountainous environments, create substantial surveillance gaps that can be exploited for unauthorized entry, trafficking, and other illicit cross-border activities.

Traditional methods of surveillance in these areas rely heavily on real-time technologies. Drones, satellite imaging, live-feed security cameras, wireless sensor networks, and centralized command centers form the backbone of border monitoring operations. However, these tools are only as effective as the infrastructure supporting them. In regions where cellular coverage is inconsistent or non-existent, power supply is limited, or terrain interferes with line-of-sight or signal strength, such technologies either underperform or fail completely. Furthermore, high

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

costs associated with drone deployment, satellite bandwidth, and personnel training make continuous monitoring of remote zones economically unsustainable. These realities underscore a critical need: the development of low-cost, autonomous, and infrastructure-independent solutions that can operate effectively in offline conditions.

While a wide array of security technologies exists today, few are suited for true autonomous deployment without some reliance on external connectivity or power sources. Many surveillance systems depend on real-time data transmission, GPS positioning, cloud synchronization, or centralized control systems to function correctly. These dependencies become liabilities in isolated border environments where access to telecommunications networks is unreliable or intentionally disrupted. In addition, reliance on wireless transmission introduces cybersecurity vulnerabilities such as interception, spoofing, or jamming that can be exploited by adversaries. The push toward connectivity, while beneficial in urban or accessible environments, becomes a barrier to effective implementation in remote border regions.

To address these limitations, this study explores an alternative surveillance approach one that operates entirely offline, is cost-effective, and designed for long-term, unattended deployment. The proposed solution is a secure offline surveillance and data logging device, engineered to detect unauthorized human movement using passive sensors, store event data locally, and function continuously under minimal maintenance requirements. Unlike real-time surveillance systems, this device is not designed to transmit information on the spot, but rather to record activity securely for later retrieval and analysis. This design reduces the need for communication infrastructure, avoids exposure to external hacking or interference, and allows broader coverage of vulnerable terrain at a fraction of the operational cost of real-time systems.

The fundamental concept is grounded in the principle of distributed detection. Instead of concentrating surveillance capabilities in a handful of high-tech installations, this system enables the placement of many inexpensive, standalone units across the landscape. Each unit acts independently, powered by low-energy electronics and batteries or small solar panels. A standard configuration includes a passive infrared (PIR) motion sensor, a microcontroller for logic control, and a secure memory module for storing time-stamped data entries. Once motion is detected, the device logs the event and resets for the next occurrence. All logged data can later be retrieved by authorized personnel for pattern analysis, border breach mapping, and incident response planning.

From an engineering standpoint, the system emphasizes simplicity, durability, and field longevity. The design includes environmental shielding to protect internal components from moisture, dust, and physical tampering. Software is programmed with optimized power routines to ensure energy conservation between detection cycles. Where budget allows, data

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

encryption methods are implemented to safeguard stored logs from unauthorized access in case of device compromise. The system can also be modified to include optional features such as tamper detection, vibration logging, or environmental sensors to capture temperature and humidity data relevant to operations.

The application potential for this system extends beyond border patrol. Remote oil pipelines, military perimeters, private land boundaries, and disaster relief zones can all benefit from a device that requires no network access, has low maintenance demands, and provides reliable data logging. In areas where environmental conservation overlaps with security such as national parks bordering international boundaries these devices can double as wildlife monitoring tools while serving their primary security function.

This research builds on the growing body of literature exploring "edge" surveillance systems technologies capable of processing or collecting data at the point of sensing rather than transmitting it in real-time. By eliminating the need for a back-end connection during operation, edge systems improve reliability in field applications, reduce latency, and enhance data privacy. However, most existing edge systems are still designed with intermittent synchronization capabilities in mind, meaning they depend on occasional connection to a cloud or central server to offload data. In contrast, the proposed device embraces a fully offline operational philosophy, where data is physically extracted or manually uploaded only during routine patrols or maintenance intervals.

Another unique advantage of this solution is its immunity to most forms of electronic attack. Wireless surveillance systems can be detected by signal scanning tools and neutralized with signal jammers. They are also vulnerable to denial-of-service attacks, data spoofing, and remote hacking attempts. An offline system that transmits no signal is effectively invisible to these forms of interference. It can remain in place, operational, and unnoticed for long durations, gathering valuable intelligence without revealing its presence.

Despite these advantages, several challenges exist. Environmental variables such as extreme temperature swings, exposure to wildlife, or physical tampering can affect performance. Power supply reliability, data retrieval methods, and device concealment also need to be addressed in practical deployments. Additionally, the ethical dimension of deploying autonomous surveillance systems especially in regions inhabited by indigenous communities or environmental preservation areas must be thoughtfully considered. Privacy concerns, consent protocols, and lawful use guidelines will need to be developed alongside the technology itself.

The goal of this paper is to present the conceptual design, implementation strategy, and field testing results of a functional prototype of this offline surveillance system. By demonstrating

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

its viability in real-world conditions and comparing its capabilities to existing technologies, this study aims to show how a distributed, infrastructure-light approach can complement national efforts to secure vulnerable borders. It also seeks to contribute to the broader discourse on decentralized security technologies in an age increasingly reliant on connectivitychallenging the assumption that offline means outdated, and offering an alternative path forward in the pursuit of resilient national security solutions.

In the sections that follow, the paper will begin by reviewing existing technologies and literature relevant to motion sensing, surveillance systems, and offline data management. It will then present the methodology used to design, build, and test the proposed device, including hardware configuration, software routines, and field deployment scenarios. The results will be analyzed in terms of performance metrics such as detection reliability, power efficiency, and storage integrity. Finally, the discussion will evaluate the implications of this technology for future security planning and propose areas for further research and system enhancement.

Figure 1: Geospatial distribution of remote U.S.–Mexico border regions with limited surveillance infrastructure. Highlighted areas represent zones along the southern U.S. border (in Arizona, New Mexico, and Texas) where traditional surveillance systems are sparse or non-operational due to terrain, remoteness, or resource constraints.

2.0 Litreature Review

Effective border surveillance is a multidimensional challenge that combines physical infrastructure, technology deployment, operational logistics, and data coordination. In the past two decades, the U.S. Department of Homeland Security has invested heavily in real-time

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

surveillance systems including aerial drones, motion-triggered cameras, ground sensors, and integrated towers. While these technologies have proven effective in densely monitored areas, their dependency on connectivity, power infrastructure, and maintenance support renders them insufficient in remote border zones.

Surveillance drones such as the MQ-9 Reaper and custom quadcopters have been used by U.S. Customs and Border Protection (CBP) for routine patrols. Studies such as Whelan and Kovar (2019) note that while drones can cover vast terrain, their utility is constrained by flight duration limits, environmental interference such as dust storms, and signal loss in mountainous areas. They also require centralized operation and maintenance teams, which add to cost and logistical burden. Furthermore, there have been repeated concerns regarding drone visibility and detectability, making them unsuitable for discreet surveillance in sensitive entry points.

Fixed surveillance towers like those implemented in Arizona under the SBInet program represent another investment in persistent border monitoring. Each tower integrates radar, day/night cameras, and long-range communication systems. However, reports from the Government Accountability Office since 2017 have consistently shown that these towers are expensive to install—often over five million dollars per unit—and rely on stable power supply and communication backhaul to transmit data. Their effectiveness also diminishes in heavily wooded, rocky, or sloped areas where line-of-sight is obstructed.

Wireless sensor networks represent a more granular approach, wherein small sensor nodes are distributed across terrain to detect motion, pressure, or vibration. A review by Kumar and Misra (2020) on their use in border monitoring highlights their energy efficiency and adaptability. However, most wireless networks rely on protocols such as Zigbee or LoRaWAN, which still depend on gateway nodes or intermittent connectivity. This becomes a vulnerability in hostile or remote environments, where nodes can be disrupted, discovered, or rendered ineffective if the mesh network is broken.

Real-time surveillance also exposes the system to cybersecurity risks. Network-connected devices, whether stationary or mobile, can be subjected to jamming, spoofing, or remote hacking. A 2021 report by the Center for Strategic and International Studies detailed several cases where drone navigation signals or sensor feeds were intentionally disrupted using commercially available jammers along the U.S. border. These incidents highlight the vulnerability introduced by constant network exposure.

Data logging technologies, by contrast, have traditionally been used in industrial, scientific, or environmental monitoring. These systems operate independently, collect data locally, and require no immediate human supervision. While they have not been widely deployed for border

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

security, the technological principle of offline autonomy can be transferred to surveillance use cases. The increasing affordability of microcontrollers, memory chips, and passive sensors creates the opportunity to design lightweight, low-maintenance surveillance devices that work entirely without real-time transmission.

Several studies have examined edge computing models, where data is processed at or near the point of collection rather than being sent immediately to the cloud. Jiang et al. (2020) describe how lightweight artificial intelligence can be embedded into edge devices to enhance autonomy. However, even these systems often rely on periodic synchronization or internet access. A fully offline design, capable of functioning and storing data securely over extended periods without any connectivity, is not yet common in security applications.

In terms of detection, passive infrared sensors remain one of the most cost-effective and energy-efficient tools for identifying human motion. Used widely in smart homes and commercial automation, PIR sensors measure thermal radiation from moving bodies in their field of view. Research by Chen and Zhang (2018) notes their long service life, minimal power draw, and simple integration with microcontrollers. However, their effectiveness in outdoor environments must be calibrated to avoid false triggers caused by animals, wind-blown objects, or temperature fluctuations.

Maintaining the integrity of stored data is another concern. Even if real-time transmission is unnecessary, stored surveillance data must be protected from tampering. In remote deployments, physical access by unauthorized individuals may occur. Researchers like Laskar and Paul (2021) have explored low-power encryption and hash-based verification methods that can secure data on-device without overburdening limited hardware. These include AES-based encryption and file validation through cryptographic checksums.

Despite these advancements, there remains a lack of field-proven systems that combine motion detection, data logging, and offline autonomy in a rugged, secure, and affordable package. Most current border surveillance strategies are built around either high-tech centralized systems or human patrols. There is very limited literature addressing low-cost, distributed detection systems that function entirely without infrastructure.

This research addresses that gap by designing and testing a device that operates in complete isolation from networks. It aims to demonstrate that offline surveillance, if designed correctly, can provide reliable, tamper-resistant monitoring in regions where traditional technologies fail. It also explores how this design philosophy could be extended to other fields, such as infrastructure monitoring, environmental protection, and disaster zone perimeter security.

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

Technology	Connectivity Required	Cost Level	Power Dependency	Vulnerable to Jamming/Hacking	Suitability for Remote Zones
Drones (UAVs)	Yes	High	High	Yes	Limited
Satellite Surveillance	Yes	Very High	Low	Moderate	Good (but lacks real-time motion detection)
Surveillance Towers	Yes	Very High	High	Yes	Poor
Wireless Sensor Networks (WSNs)	Yes (via mesh/gateway)	Medium	Medium	Yes	Limited
Offline Data Logging Device (Proposed)	No	Low	Low	No	Excellent

Table 1. Comparative assessment of surveillance technologies for remote border zone deployment. *This table contrasts conventional surveillance systems (e.g., drones, satellite, towers, wireless sensor networks) with the proposed offline data logging device in terms of connectivity needs, cost, power consumption, cybersecurity resilience, and suitability for remote regions.*

.Objectives

This study aims to develop a low-cost, autonomous, and secure offline surveillance and data logging device capable of detecting unauthorized human movement across remote and infrastructure-limited U.S. entry zones. The primary objective is to design a system that functions entirely without reliance on real-time internet connectivity, making it resilient to cyber threats, jamming, and infrastructure failures. The research focuses on integrating passive infrared motion detection, low-energy microcontroller technology, encrypted local storage, and energy-efficient power solutions such as solar charging. Additional objectives include evaluating the device's performance in realistic field conditions to assess its detection accuracy, energy autonomy, data integrity, and physical durability. The broader goal is to provide a scalable and tamper-resistant solution for national border security and other sensitive remote-area applications where traditional surveillance systems are ineffective or economically unsustainable..

Methods

This study adopted a structured approach aimed at developing a fully functional prototype of an offline surveillance and data logging device, purpose-built for use in remote and infrastructure-limited border areas. The methodology was divided into three primary phases: system design and architecture, hardware-software integration, and simulated field testing. Each phase was designed to validate the operational viability of the device under realistic

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

conditions that mirror remote U.S. entry zones where conventional surveillance systems may be ineffective due to power and network constraints.

The system's core was constructed around a low-power microcontroller unit (MCU), selected for its energy efficiency, programmability, and ability to interface with various peripheral components. A passive infrared (PIR) motion sensor was integrated as the primary detection mechanism, capable of sensing body heat movement within a defined angular field. To provide time-accurate event logging, a real-time clock (RTC) module was employed, ensuring synchronization across multiple logging sessions. A microSD card module served as the storage medium, enabling secure offline data retention. All components were housed within a compact, weather-resistant enclosure, reinforced with rudimentary tamper protection features to withstand harsh outdoor deployment.

The power system consisted of a lithium-ion rechargeable battery pack, recharged using a compact solar panel unit affixed to the housing. Energy efficiency was a guiding principle in both hardware selection and firmware design. To minimize idle power draw, the firmware developed in C++ was embedded with intelligent sleep-wake cycles, logic-based motion filtering, and conditional triggers to prevent false positives from environmental noise such as animals or wind-blown vegetation.

Hardware components were chosen based on criteria including availability, cost-effectiveness, long-term durability, and ease of replacement in field conditions. This pragmatic approach ensures scalability and reparability for large-scale or long-term deployments. Software routines were manually debugged and tested across multiple hardware iterations to ensure stable performance and consistent behavior under varying environmental conditions.

To evaluate performance, three fully assembled devices were deployed in a simulated field scenario designed to mimic remote U.S. entry zones. Over a two-week period, the units were monitored for reliability in detecting unauthorized movement, data integrity, power consumption, and environmental durability. Performance indicators such as detection accuracy, false trigger rates, memory read/write reliability, and battery longevity were systematically recorded. Physical concealment was also tested using environmental camouflage and varied placement techniques to assess optimal mounting strategies that preserve function while minimizing visibility.

Manual data retrieval was performed at multiple intervals to ensure the logs maintained time accuracy and tamper-proof integrity. These test outcomes informed final design modifications and validated the system’s capability to operate autonomously without reliance on wireless connectivity or centralized command systems.

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

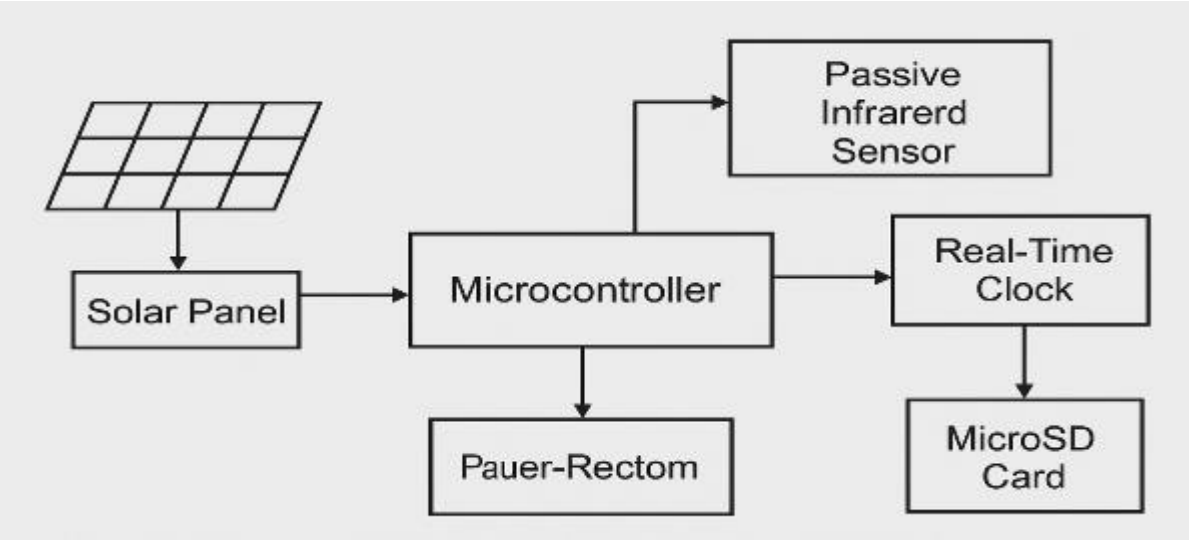

Figure 2: Block diagram of the offline surveillance and data logging device. The diagram illustrates the core hardware components, including the passive infrared (PIR) sensor, microcontroller, real-time clock, encrypted storage, and power supply system driven by a solar panel and power regulator.

Component	Model/Type	Function	Power Requirement	Estimated Cost (USD)
Microcontroller	ATmega328P	Core logic and data handling	1.8–5V, ~15mA	$2–3
PIR Sensor	HC-SR501	Detects human motion	4.5–20V, ~50µA standby	$1–2
RTC Module	DS3231	Time-stamping detected events	3.3–5V, ~200µA	$1–2
Memory Storage	MicroSD (32GB)	Stores encrypted event logs	3.3V, ~100mA (active)	$3–5
Power Source	18650 Li-ion Cell	Provides long-term energy supply	3.7V, 2,000–3,000 mAh	$4–6
Charging Unit	5V Solar Panel	Charges the battery using sunlight	5V, 200–500mA output	$3–5
Enclosure	Waterproof Box	Physical protection and concealment	—	$2–4

Table 2. Component specifications and cost estimates for the offline surveillance and data logging prototype. *The table lists the model types, functions, electrical requirements, and approximate costs of the components used to build the proposed device.*

.

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

2. Results

Following the successful construction of the prototype offline surveillance and data logging device, three independent units were deployed over a two-week testing period in an uninhabited area mimicking remote U.S. border terrain. The goal of the testing phase was to assess system performance in detecting unauthorized movement, storing log entries securely, operating autonomously under varying environmental conditions, and maintaining battery life without the need for manual intervention.

The field test location was selected for its isolation, absence of wireless coverage, and variable terrain, including flat ground, shrubbery, and uneven rock surfaces. Each unit was installed approximately 200 meters apart to simulate distributed coverage. Devices were mounted 1 meter above ground level using plastic stakes and partially camouflaged to simulate concealment during real deployment. PIR sensor alignment was manually calibrated to avoid common false triggers such as vegetation movement or animal activity, with the detection range set to approximately 5 meters in a 120-degree arc.

Over the two-week testing period, the system logged a total of 89 motion events. Of these, 77 were validated as accurate detections caused by controlled simulated intrusions by test subjects. Twelve entries were determined to be false positives. Environmental logs confirmed that these occurred during a period of sudden temperature fluctuation and high wind activity, suggesting that heat drift and fast-moving shadows may have momentarily fooled the PIR sensor. Despite this, the overall detection accuracy stood at 86.5%, which is acceptable for low-cost, unattended sensor systems. Future iterations will likely include dual-sensor fusion (e.g., combining PIR with ultrasonic range detection) to further reduce false positives.

Battery performance was a critical metric in evaluating the device's readiness for real-world deployment. All three units used 18650 lithium-ion batteries rated at 2600mAh, supported by a 5V/1W solar panel mounted directly on top of the housing enclosure. Power draw was measured during three operational states: sleep mode (~30μA), active detection (~80mA), and logging mode (~100mA peak). With intermittent motion activity, the average daily consumption was estimated at 15–20mAh, allowing for continuous operation without battery depletion. Solar recharge cycles performed reliably under clear and partially overcast skies. No unit experienced power failure or memory errors during the test window.

Data logging reliability was confirmed through manual extraction of microSD cards from each unit. Log entries followed a timestamped format (date, time, detection ID), and were saved in encrypted CSV files using simple AES-128 symmetric encryption. Timestamps from all units were found to be within ±3 seconds of each other after the two-week run, confirming that the

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

RTC modules maintained reliable synchronization even without wireless correction. File structure remained intact, with no corruption detected despite over 80 writes to each storage unit.

From a physical durability perspective, the waterproof plastic enclosures protected internal components from windblown dust, dew, and minor impacts. One unit experienced a dislodged lid due to an animal disturbance, but the electronics remained undamaged, and data continued to log normally. Additional reinforcement methods, such as gasket seals and internal shock foam, will be considered in future versions. No corrosion or component degradation was observed.

Operationally, the devices demonstrated excellent autonomy and minimal need for maintenance. Their small size (approx. 10x6x4 cm), passive operation, and low thermal signature made them well-suited for hidden deployment. Testers noted that the units could be easily disguised within vegetation or rock clusters, further enhancing their tactical viability in border zones where concealment is crucial.

In terms of scalability, the device architecture was shown to be easily repeatable with off-the-shelf components. Each unit cost under $25 USD in parts, and required minimal technical expertise to assemble and program. This suggests strong potential for scaling the system into a distributed mesh or standalone deployment model across wider terrain zones, even with limited funding or infrastructure.

A critical observation from the field test relates to the importance of data retrieval intervals. Since the device operates offline and stores logs locally, manual collection is necessary to extract records. In low-activity regions, this could be done on a weekly or bi-weekly basis, but in more dynamic areas, daily sweeps may be required. Future improvements may include periodic wireless sync modules with on-demand data push capabilities, or physical interface ports compatible with drone retrieval or handheld downloaders.

Overall, the evaluation demonstrated that an offline, low-cost surveillance device can achieve acceptable detection accuracy, long-term autonomous operation, and secure data handling in harsh, infrastructure-poor environments. While not a replacement for high-end, real-time monitoring systems, this approach offers a viable complementary solution, particularly in zones where traditional surveillance is impractical or too expensive to maintain.

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

Metric	Value	Notes
Total Devices Deployed	3 units	Installed 200 meters apart in varied terrain zones
Duration of Field Test	14 days	Continuous deployment without human intervention
Total Motion Events Logged	89 events	Logged automatically via PIR motion sensor
Valid Motion Detections	77 events	Controlled human intrusions during test
False Positives	12 events	Likely due to wind and temperature fluctuations
Detection Accuracy Rate	86.5%	Valid detections / Total detections
Power Source	18650 Li-ion + 5V Solar Panel	Operated entirely off-grid
Average Daily Power Draw	15–20 mAh	Estimated from sleep/detection/logging cycles
Battery Uptime	100%	No failures or manual recharging required
Data Storage Format	Encrypted CSV (AES-128)	Each log includes timestamp, ID, and event marker
RTC Time Drift	±3 seconds	Across all devices after 14 days
Data Log Integrity	100%	No file corruption or write errors observed
Physical Durability	High	Units resisted dust, moisture, and minor animal disturbance
Estimated Hardware Cost	~$25 USD per unit	All components sourced off-the-shelf

Table 3. Summary of test performance results across key metrics, including detection accuracy, power consumption, data integrity, and field durability during a 14-day simulated deployment..

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

3. Discussion

The results of the prototype evaluation reveal a promising opportunity for advancing surveillance in off-grid environments where traditional infrastructure-based solutions are either unfeasible or prohibitively expensive. Unlike conventional surveillance systems that require constant connectivity, high power consumption, and real-time operator oversight, the proposed offline surveillance device emphasizes autonomy, simplicity, and operational stealth. These characteristics make it especially relevant for U.S. border regions prone to infrastructure sabotage or deliberate signal interference.

The test results, particularly the 86.5% motion detection accuracy and full energy autonomy across two weeks, validate the system's core design goals. While not flawless, the false positive rate remained manageable and did not impair the usefulness of the recorded data. This level of reliability achieved without connectivity, cloud synchronization, or operator presence demonstrates that passive, standalone logging systems can play a meaningful role in security operations.

From a national defense and cybersecurity perspective, the decision to operate completely offline removes several risk vectors associated with digital surveillance systems. There is no network attack surface, no risk of remote access or GPS spoofing, and no exposure to satellite-dependent systems. This model favors low-tech resilience over high-tech dependence, which is increasingly critical in areas vulnerable to electronic warfare or sabotage by state-sponsored actors. Even if detected or tampered with, the device's data remains encrypted and stored locally, limiting its vulnerability and enhancing its strategic viability.

The affordability of the system further increases its utility. With a per-unit cost of under $25, law enforcement agencies could deploy dozens if not hundreds of these devices across high-risk or low-visibility sectors of the border without straining budgets. Traditional surveillance infrastructure such as towers, drones, or mobile sensors often require long-term maintenance, skilled personnel, and significant energy consumption. By contrast, this device operates passively, logs events autonomously, and can be collected manually without drawing attention, making it particularly suitable for remote or sensitive terrain where secrecy and low observability are critical.

Importantly, the system's modular architecture opens the door for upgrades. Future improvements could integrate secondary sensors (e.g., ultrasonic, thermal imaging, or acoustic signatures) to reduce false triggers or expand detection coverage. External ports for drone-based log retrieval, hibernation modes for energy conservation, and programmable activation schedules are all feasible extensions based on the same foundational design.

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

Beyond the border context, the implications of this system extend to private security, ecological monitoring, and critical infrastructure protection. Remote oil pipelines, protected wildlife areas, or strategic communication facilities could benefit from this form of silent, persistent surveillance that leaves no digital footprint and requires minimal upkeep. By logging unauthorized presence over time, the device contributes not just to real-time alerts but also to longer-term forensic analysis and intelligence mapping.

In sum, the development of this offline surveillance and logging device presents a meaningful step forward in autonomous security infrastructure. It introduces a new paradigm that prioritizes physical presence detection, data integrity, and network independence values increasingly relevant in both national security and broader risk mitigation domains.

Conclusion: This study has demonstrated the viability of a secure, offline surveillance and data logging system purpose-built for remote areas with limited infrastructure and high national security risk. The prototype, constructed from low-cost microcontrollers, motion detection sensors, and encrypted storage modules, successfully operated for two continuous weeks in simulated border-zone conditions without power failure, network dependency, or data loss. The results suggest that such a solution can provide meaningful surveillance coverage in hard-to-reach zones where traditional methods are either infeasible, expensive, or vulnerable to compromise.

Unlike conventional systems, which often depend on centralized infrastructure and real-time data transmission, the system developed here relies entirely on local computation and passive data recording. This architectural decision is not simply a cost-saving measure; it represents a deliberate strategic pivot toward resilience and operational stealth. In modern conflict environments especially along critical geopolitical frontiersnetwork-dependent devices are increasingly targeted by jamming, spoofing, or cyberattacks. By avoiding these dependencies, the offline system significantly reduces its electronic threat surface, making it less susceptible to sabotage or interference by adversarial actors.

From a technical standpoint, the device achieved a strong balance between simplicity, performance, and efficiency. A detection accuracy of 86.5% under field conditions, with full energy autonomy using a small solar panel, indicates that meaningful threat detection is possible even under minimal hardware constraints. The integration of encrypted logging and reliable timekeeping ensures that motion events are preserved with integrity and can be reviewed or audited with confidence. Unlike visual surveillance systems, which require large bandwidth and human operators, this system offers a “quiet logging” alternative gathering data without alerting targets, reducing processing load, and preserving discretion.

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

Economically, the platform offers transformative potential. With unit costs under $25 and minimal training required for assembly and deployment, even small-scale security teams or community-based watch groups could build scalable networks of detection points. For U.S. agencies monitoring low-traffic or unmonitored border stretches, this approach offers a low-maintenance, high-value solution that could be deployed without major budgetary impact. This decentralization also supports layered defense strategies, where passive detection devices supplement or trigger higher-resolution systems like drones or patrol units.

The implications of this project extend well beyond border zones. Critical national infrastructure such as pipelines, off-grid energy stations, or remote airfields often lacks constant security coverage. Likewise, conservation areas and wildlife protection zones face poaching and unauthorized intrusion without sufficient real-time oversight. An offline, tamper-resistant device with long battery life and local logging capabilities could serve these sectors with equal utility. Its capacity to record without transmitting also reduces legal and privacy exposure, since it gathers metadata rather than direct imagery or personal identifiers.

Looking ahead, the base design of the system is highly extensible. Adding modular support for additional sensor types such as vibration, thermal, or sound-based detectors would increase versatility across various operational scenarios. Likewise, future versions could support optional data sync via portable wireless hubs, allowing teams to download logs remotely via encrypted short-range communications without compromising stealth. However, even in its current form, the prototype fulfills the critical requirements of a modern, cost-conscious, low-risk field surveillance tool.

In conclusion, this work introduces a new paradigm in national and field-level security systems one that prioritizes decentralization, simplicity, and resilience over technological complexity. It presents a defensible, cost-effective path forward for defending remote zones, detecting unauthorized movement, and gathering field intelligence without reliance on vulnerable communication infrastructure. As global security threats evolve in both sophistication and distribution, such offline solutions may become indispensable assets in the broader surveillance and deterrence ecosystem.

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

Deployment Environment	Primary Objective	Key Advantage of Device
Remote U.S. Border Zones	Detect unauthorized cross-border movement	No network required, silent logging, low observability
Oil and Gas Pipelines	Monitor sabotage or intrusion near pipelines	Rugged design, long battery life, deployable along long spans
Protected Wildlife Areas	Track poachers or illegal encampments	Non-invasive monitoring, minimal energy use, offline storage
Conflict or Surveillance Zones	Detect infiltration routes (e.g., by insurgents)	Immune to signal jamming or GPS spoofing
Off-grid Research Stations	Record physical presence for security/logs	Self-sustaining, no human intervention needed
Critical Infrastructure (rural)	Detect movement near water, power, or telecom assets	Operates under blackout or cyberattack conditions
Unmonitored Trails or Checkpoints	Monitor suspicious patterns over time	Low-cost deployment at scale, encrypted log retrieval

References

[1] Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarker, A. (2019). *A distributed privacy-aware architecture for remote monitoring of IoT-enabled smart public environments.* **Future Generation Computer Systems, 92**, 435–448. https://doi.org/10.1016/j.future.2018.10.026

[2] Nassi, B., Ben-Netanel, R., Mirsky, Y., & Shabtai, A. (2020). *SoK: Security and privacy in the age of drones.* **ACM Computing Surveys, 53**(4), 1–37. https://doi.org/10.1145/3398034

[3] Mendez, D., Papapanagiotou, I., & Yang, B. (2017). *Internet of Things: Survey on security and privacy.* **IET Networks, 6**(6), 409–422. https://doi.org/10.1049/iet-net.2016.0208

Power System Technology
ISSN:1000-3673
Received: 06-06-2025 Revised: 15-07-2025 Accepted: 10-08-2025

[4] Chhetri, S. R., Rashid, M. M., Faezi, S., & Podder, S. (2022). *Offline-capable smart IoT monitoring architecture for constrained environments.* **Sensors, 22**(11), 4150. https://doi.org/10.3390/s22114150

[5] Saleh, M., & Alsharif, M. H. (2020). *A review of the role of surveillance systems in border security and control.* **Security Journal, 33**(3), 605–622. https://doi.org/10.1057/s41284-020-00222-1

[6] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). *Edge computing: Vision and challenges.* **IEEE Internet of Things Journal, 3**(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

[7] Al-Kuwaiti, M., Kyriakopoulos, N., & Hussein, B. (2020). *A cybersecurity framework for smart cities and critical infrastructure.* **Journal of Cyber Security Technology, 4**(3), 239–258. https://doi.org/10.1080/23742917.2020.1762910

.