RSTDE
Remote Sensing Technology in Defense and Environment
RSTDE 2(2): 101–116
ISSN 3062-8970

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

Automated control design in a sensor and AI-based intelligence monitoring system for suspicious activity detection

Fahreza Alfarizi[1]*, Poppy Setiawati Nurisnaeny[1]
[1] *Sekolah Tinggi Inteligen Negara, Bogor, West Java 16810, Indonesia.*
*Correspondence: fahrezaalfarizi10@gmail.com

Received Date: June 13, 2025 Revised Date: August 26, 2025 Accepted Date: August 30, 2025

ABSTRACT

Background: In the modern digital landscape, intelligence monitoring systems integrating advanced sensor technology and artificial intelligence (AI) have become essential for enhancing public safety. These systems aim to not only observe but also recognize and respond to suspicious activities effectively and efficiently. Current literature highlights the transformative impact of IoT and AI in various sectors, offering significant improvements over traditional methods. **Methods**: This study explores the integration of sensor networks, AI-driven algorithms, and Internet of Things platforms. Data collection involves real-time inputs from devices such as cameras, PIR sensors, and microphones, analyzed through machine learning techniques to enhance detection precision. **Findings:** The systems demonstrate improved monitoring efficiency and have the capacity to operate autonomously, ensuring security across both public and private sectors. They offer long-term cost savings and overcome the limitations inherent in human-operated systems. **Conclusion:** These systems represent a significant advancement toward proactive and intelligent surveillance, enhancing public safety and security. **Novelty/Originality of this article:** The research underscores the novel integration of cutting-edge technologies in intelligence monitoring, establishing new benchmarks in adaptability and responsiveness, and setting the foundation for future advancements in cohesive and sustainable surveillance frameworks.

KEYWORDS: artificial intelligence; intelligence monitoring; internet of things.

1. Introduction

In the rapidly evolving and complex digital era, an intelligent and responsive monitoring system has become increasingly crucial, especially in the realms of defense and intelligence security. Artificial Intelligence (AI), smart sensor technology, and responsive control systems collaborate to detect suspicious activities automatically and in real time. A threat detection system based on machine learning for the Internet of Things (IoT) networks exemplifies the application of these technologies. Despite the limitations in computational capability and device power, this method facilitates highly accurate and rapid detection of suspicious behaviors (Aldhaheri et al., 2024).

Many situations initially appear normal in everyday life; however, upon closer inspection, anomalies that cannot be ignored are often discovered, such as unusual financial transaction patterns, suspicious behaviors, or actions that violate relevant legal standards, including frequently overlooked suspicious activities. Unfortunately, due to ignorance or reluctance to intervene, many individuals choose to disregard these warning signs. In

Cite This Article:
Alfarizi, F., Nurisnaeny, P. S. (2025). Automated control design in a sensor and AI-based intelligence monitoring system for suspicious activity detection. *Remote Sensing Technology in Defense and Environment, 2*(2), 101-116. https://doi.org/10.61511/rstde.v2i2.2025.2248

reality, ensuring environmental safety, preventing crime, strengthening societal resilience, and most importantly, maintaining a nation's defense and security are heavily reliant on the ability to comprehend and identify such suspicious activities.

One of the greatest challenges in securing a nation's physical and cyber spaces is identifying suspicious intelligence activities. Artificial Intelligence (AI) and smart sensor-based monitoring systems have been extensively developed to automatically identify anomalous patterns and potential threats to address this difficulty. Internet of Things (IoT) sensors are crucial for collecting real-time data from various monitoring devices, including motion detectors, cameras, and microphones. By integrating this data with machine learning, systems can learn to identify abnormal behavioral patterns and initiate early warnings about potentially suspicious activities (Rehman et al., 2024). AI has demonstrated its ability to identify anomalous activities across various domains, including academia. By analyzing linguistic patterns and specific textual elements, AI technologies have been developed to differentiate with up to 99% accuracy between human-written texts and those generated by AI language models such as ChatGPT, Gemini, and Blackbox AI. This highlights AI's capacity to detect subtle and nuanced patterns, which can also be applied to identify suspicious activities in defense and security systems (Desaire et al., 2023).

Smart sensor and AI-based monitoring systems that incorporate IoT enable multiple devices to communicate, collect, and share data in real time, allowing the system to respond automatically to potential threats. IoT is crucial for autonomous control design as it connects sensors to AI-driven decision-making systems. To enhance the sensitivity and selectivity of sensing systems, smart sensor technology based on nanomaterials like gold nanorods (AuNR) has been developed. Due to their dynamically tunable plasmonic characteristics, AuNRs enable the detection of changes in orientation and the surrounding environment. This technology facilitates the development of active smart sensors that can adapt to changing conditions, enhancing monitoring precision and detection on micro to nano scales (Sekizawa et al., 2024).

Modern surveillance systems are now capable of performing monitoring tasks automatically and effectively, responding to evolving threats due to the integration of advanced sensors and artificial intelligence. In the defense industry, multispectral sensors on unmanned aerial systems (sUAS) combined with AI technology have proven effective in identifying hazardous objects such as unexploded ordnance (UXO). This integration accelerates and enhances identification accuracy in hazardous environments when applied to spectral imaging. These developments demonstrate that AI and automated sensor systems can form the foundation of contemporary intelligence surveillance systems that are not only effective but also flexible enough to address various threat situations, challenges, obstacles, and disruptions (Cho et al., 2023).

While numerous sensor technologies and AI have shown significant efficacy across various applications, a primary challenge remains in developing an automated control system capable of analyzing suspicious activity data in real-time with accuracy and adaptability. Conventional surveillance systems largely depend on human operators who are susceptible to fatigue and visual errors. In urgent situations, this results in poor reactivity and detection accuracy. Therefore, a system is needed that can automatically analyze and make judgments using AI and machine learning algorithms, alongside the ability to collect data through sensors (Kang et al., 2023).

The development of sensor-based intelligence monitoring systems using AI now heavily relies on machine learning (ML). One of its significant uses is in supporting the development of automated controls to identify suspicious behaviors in real-time. With machine learning, systems can swiftly and accurately interpret and evaluate data from various sensors, including cameras, microphones, and radar. Even in dynamic and changing contexts, computers can distinguish between suspected abnormal behavior and normal activity using supervised and unsupervised learning techniques. Moreover, the application of models such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) enables highly accurate processing of sequential and visual data (Chen et al., 2023).

Reinforcement learning algorithms are frequently employed in automated control to regulate system responses automatically, such as notifying security operators, directing cameras to focus points, or activating alarms. Furthermore, the capacity of these systems to integrate data from multiple sensors enhances detection and decision-making precision. Systems can continually improve their efficiency by learning and adapting to new patterns over time. Integrating machine learning within larger AI systems, encompassing perception to decision-making, enables the development of responsive, adaptive, and autonomous intelligence monitoring systems capable of proactively identifying and managing potential threats.

Control systems are also regularly used in automated control to manage the reactions of smart sensor systems automatically, including focusing cameras, triggering alerts, or notifying security operators. The ability of these control systems to process data from multiple sensor outputs enhances detection and decision-making accuracy. As systems learn and adapt to new patterns over time, their efficiency continues to improve. Machine learning plays a crucial role in developing intelligent, responsive, adaptive, and autonomous control systems to proactively identify and address any threats when integrated into AI systems (Gawande et al., 2024).

Moreover, by integrating technologies such as edge computing and embedded AI, smart sensor systems can collaborate with machine learning algorithms to filter relevant data in real-time, thereby enhancing overall system efficiency. For instance, they can automatically identify individuals or vehicle license plates, detect unusual activities such as crowded places or sudden movements, and operate effectively under various conditions. Smart sensors can adjust their sensitivity in response to environmental contexts, such as low lighting or noise interference. This synergy between smart sensors and machine learning-based automated controls ensures the monitoring system is not only reactive but also predictive and adaptive to evolving threats.

Responsive control systems are also vital to ensure that intelligence monitoring systems can accurately and swiftly respond to both known and unforeseen circumstances. These systems operate on the principle that any dubious information or signal from smart sensors should be promptly converted into action with minimal delay. Advanced machine learning in responsive control systems automatically recognizes threat patterns and selects optimal actions, which may include restricting access to specific areas, expanding camera focus, or activating early warning systems. This results in a mechanism that is not only reactive but also sufficiently flexible to adapt to changing threat levels. Depending on the urgency level, systems can be configured to modify response intensity. For example, the system can differentiate between suspicious activities, like movements after hours, and routine movements (Desalegn et al., 2022).

These features reduce the likelihood of false alarms and enhance system efficiency. Environmental monitoring is crucial in business, military, and public security contexts, as it can be conducted more quickly, intelligently, and accurately with the support of AI-powered responsive control systems. Advances in Artificial Intelligence (AI), autonomous control systems, and Internet of Things (IoT) technology have enabled the development of intelligent monitoring systems capable of identifying suspicious activities in real-time. Designing automation and security solutions based on sensor data is made possible by integrating IoT and machine learning within contemporary system architecture frameworks. Machine learning allows systems to learn from vast amounts of data generated by IoT sensors, thereby enhancing detection precision and autonomous event prediction.

However, AI's capacity to generate and comprehend words or data is also rapidly evolving. Advanced classification models such as XGBoost have demonstrated the effectiveness of AI-based facial recognition technology in distinguishing between artificial and human intelligence. This underscores AI's ability to understand linguistic patterns in addition to performing numerical analysis. These capabilities can be utilized in behavior recognition-based security systems by analyzing digital activities or communications. Thus, designing automated control systems for AI-driven, sensor-based monitoring of suspicious intelligence activities is a primary subject of discussion. The aim is to reduce dependency

on human operators while effectively and adaptively detecting suspicious activities, making it efficiently usable by security and defense sectors, including intelligence. This technology has the potential to become an essential solution for creating proactive and responsive contemporary security systems (Smarsly & Dragos, 2024).

2. Methods

This study employs a mixed-methods approach to explore the integration of sensor networks and AI in intelligence monitoring systems. Conducted over six months across urban and industrial environments, locations were selected for their varied security needs and relevance to public safety concerns, allowing for the implementation of comprehensive monitoring solutions. Advanced sensor equipment, including CCTV cameras, PIR motion sensors, and audio microphones, connected via IoT platforms, were utilized to monitor areas of high foot traffic and critical infrastructure. The study focused on variables such as real-time data collection efficacy, anomaly response times, and the accuracy of AI-driven threat identification, sourcing data from live feeds and historical logs provided by the sensors. Sensors were strategically installed to maximize coverage, transmitting data to centralized AI systems where machine learning algorithms categorized activities and triggered appropriate responses. Using edge computing devices, data processing was conducted locally to minimize latency, with statistical methods employed to evaluate system performance against predefined benchmarks. Information was presented through visual dashboards for real-time monitoring and decision-making. The experimental design included both observational studies for data gathering and controlled tests to assess response effectiveness, grounded in literature on AI and IoT applications and tailored to specific security challenges identified during the study.

3. Results and Discussion

3.1 Basic concepts

In sensor-based and artificial intelligence (AI) monitoring systems, automated control design is a technical approach that enables real-time detection, analysis, and response to suspicious behaviors without direct human involvement. To enhance security and surveillance effectiveness across various settings, these systems utilize smart sensors, security cameras, and AI algorithms. The design for monitoring suspicious activities involves three primary components:

3.1.1 Smart sensors

In contemporary intelligence systems, smart sensors are strategically vital for monitoring, identifying suspicious activities, and enabling automated decision-making based on data. AI-based cameras, temperature and sound sensors, and motion sensors (such as PIR) are essential components of intelligent surveillance systems used for border protection, military needs, and facility monitoring. These sensors can be deployed in interconnected networks and function similarly to applications in agricultural infrastructure, detecting environmental anomalies such as unusual noises, suspicious temperature spikes, or human activity in restricted areas (Irwanto et al., 2024).

To provide rapid and accurate responses, real-time data can be analyzed locally by edge computing devices using AI-based fuzzy logic or directed to central control systems. Integration with digital platforms or digital twins, similar to those used by robotic fleets for bridge monitoring, holds significant potential for intelligence systems. Sensor data can update environmental scenario models in real-time, enhancing tactical planning and predictive operational capabilities (Khazane et al., 2024).

3.1.2 Artificial intelligence detections

The potential of artificial intelligence (AI) technology has been demonstrated across various domains, such as detecting suspicious patterns, microenvironmental changes, and artificial content. The use of AI to identify images and digital content has significant implications for the intelligence community. As information grows and threats become more complex, intelligence systems must strategically identify anomalies swiftly and accurately. Similar methods can be employed in intelligence contexts to identify anomalous behavior in drone video or imagery, such as infrastructure damage related to sabotage or the presence of foreign objects in sensitive locations (Schlaeger et al., 2023).

Additionally, AI supports the automatic detection of digital content, which is highly relevant to information security and intelligence. Various AI content detection tools, such as OpenAI Classifier, GPTZero, and Copyleaks, can differentiate between human-generated and AI-produced text. Although accuracy levels vary depending on the model and AI generation used, this is a crucial aspect of intelligence systems to detect manipulative or false information that may come from social media, fake news, or false reports (Elkhatat et al., 2023). AI trained on relevant, independently verified data can serve as an "additional set of eyes and ears" for intelligence analysts, expediting monitoring without sacrificing accuracy. However, ongoing validation and training are necessary to address issues such as potential misclassification and errors in detecting small or fragile objects.

3.1.3 Responsive control systems

Responsive control systems are crucial for creating an autonomous, resilient, and adaptive intelligence monitoring infrastructure. Adapting systems in real-time to changing conditions is essential in highly volatile situations and asymmetric threats. This applies to the social and behavioral aspects of systems as well as the physical environment, such as weather, lighting, and energy supplies. An example of practical responsive control is the construction of autonomous solar-powered mini chemical plants, which use adaptive controllers to immediately respond to variations in solar intensity to maintain the quality of chemical reactions (Masson et al., 2021). This technology can be applied in sensor-based intelligence systems that automatically adjust data flow or signals based on environmental inputs, such as temperature changes, suspicious movements, or sound intensity. This concept can be further expanded in intelligence monitoring to process AI data, trigger alerts, or autonomously control drones based on field sensor data (Vassányi et al., 2024).

Responsive control systems use sensor networks and edge computing to provide active surveillance in high-risk areas. For example, AI-based cameras can be paired with motion and light sensors to track movement at borders during nighttime. Without requiring direct human interaction, responsive control systems can increase recording frame rates, divert additional power to infrared cameras, or deploy drones for visual inspection when anomalies are detected by sensors. Moreover, these devices can enhance energy efficiency and resource management for intelligence operations in remote locations. By effectively using solar energy for control devices, communication, and powering sensors, similar to the Masson plant model, these systems can increase process autonomy and make them harder to detect by adversaries (de Boer & Schroën, 2024).

3.2 Intelligence monitoring system methodology

Intelligence systems require monitoring strategies that are not only passive but also flexible and responsive to address the increasingly complex challenges of the digital era. This necessitates an approach involving intelligent data acquisition and processing, machine learning, Internet of Things (IoT) connectivity, and deep technology system integration.

3.2.1 Data acquisition and pre-processing

A crucial step in intelligence monitoring systems is data acquisition, which serves as the gateway for information entering the digital system from the real world. This data can come from various sources, including GPS, accelerometers, infrared, video, audio, and LIDAR sensors. Data capture is conducted in real-time, either statically using fixed cameras or dynamically using mobile devices like drones or legged robots. This underscores the importance of tools capable of functioning in diverse environments and settings, particularly to access areas difficult for humans to reach (Boltsi et al., 2024).

After data collection, pre-processing is vital to ensure data quality and usability for further analysis. This process ensures that only clean and relevant data are retained for subsequent steps, such as training machine learning models or integrating into larger systems. The effectiveness of pre-processing impacts overall system performance, especially when operating in real-time. To alleviate the load on central servers and accelerate system responses to urgent situations, many contemporary systems now incorporate pre-processing directly on edge devices or sensors using embedded algorithms. Consequently, data acquisition and pre-processing are not just initial technical steps but foundational to the overall quality of intelligence maintenance systems (Pereira et al., 2023).

3.2.2 Machine learning

Machine learning (ML) serves as the foundation of intelligence in smart monitoring systems, enabling them to automatically learn from data and form insights. These systems utilize ML to classify items, identify suspicious activities, detect unusual movement patterns, and predict potential threats based on historical trends. A notable application of machine learning in video surveillance transmission is the real-time identification and interpretation of human activities through deep learning algorithms. For instance, YOLOv5-based detection systems have been developed to use convolutional models to detect suspicious movements by analyzing a person's speed, direction, and style of movement (El Khediri et al., 2024).

Applications include detecting crowd density and anomalies, where machine learning algorithms can assess an area's population and alert users when a threshold is exceeded. Re-identification and face recognition allow individuals to be tracked across multiple cameras. Additionally, audio monitoring models use ML to identify specific sounds, such as gunshots, screams, or breaking glass, as emergency warning signs. The capability of machine learning to discern patterns that may be imperceptible to humans, combined with its rapid response to changes in circumstances, renders monitoring systems both predictive and reactive.

3.2.3 Internet of things

The Internet of Things (IoT) refers to a network of connected devices that can collect, exchange, and transmit data via the internet without direct human involvement. It serves as the foundation of the digital and physical infrastructure within smart monitoring systems, enabling scalable, real-time, and continuous surveillance. IoT provides a range of sensors and actuators to monitor the environment and respond to events, functioning as the sensory organs of intelligent systems. Common IoT devices include GPS trackers, motion sensors, vibration detectors, and smart IP cameras (Orzechowski et al., 2023).

The benefits of IoT for surveillance include real-time connectivity, where information is transmitted directly from devices to servers or the cloud for swift analysis and response. Position-based monitoring solutions provide accurate positional context through GPS integration. Remote control and automation capabilities allow systems to automatically contact security personnel, lock doors, and sound alarms. High scalability is achieved without the constraints of extensive wiring or substantial infrastructure, allowing for large-

scale sensor deployment. A well-developed IoT strategy enables monitoring systems to react automatically, contextually, and cooperatively to events, rather than merely recording them passively (Zhao, 2023).

3.2.4 System integration

System integration is a crucial step in creating reliable, effective, and flexible intelligent monitoring systems by combining various technological components into a cohesive whole. This process involves merging network infrastructure (cloud, edge, and IoT), software (machine learning, recommendation systems), and hardware (sensors, actuators, edge devices) into a unified ecosystem. Beyond the complexity of individual technologies, monitoring systems must seamlessly coordinate multiple components. Without integration, machine learning outcomes may not trigger the appropriate actuators or sensor data may not reach analytic engines. Consequently, system architecture must be designed with cross-platform communication and compatibility in mind (Omoloye et al., 2024).

Integration is particularly important when discussing Intelligent Energy Management Systems (IEMS). These systems combine sensor data collection (such as temperature, motion, and power usage), machine processing, or machine learning, with device activation (e.g., lighting or HVAC) based on automated logic or user-recommended settings. These systems deliver comprehensive, data-driven assessments while enhancing operational efficiency (le Febvrier et al., 2021).

3.3 Implementation

In the modern digital era, intelligence monitoring systems have a significant impact on enhancing public safety in both urban settings and critical facilities. The implementation of tools such as CCTV cameras, motion sensors (PIR), and microphones has become essential in establishing proactive and efficient monitoring networks. These systems operate beyond static recording, enabling the swift identification of potential threats through the integration of artificial intelligence (AI) with real-time data analysis.

3.3.1 CCTV Cameras

Closed Circuit Television, commonly referred to as CCTV, plays a crucial role in contemporary intelligence and surveillance frameworks that focus on enhancing safety, monitoring, and regulating physical spaces. This technology serves not only as a means of visual recording but also as a proactive tool for real-time threat identification and decision-making, particularly when equipped with AI-driven algorithms. Technically, the latest CCTV models have transitioned from traditional analog formats to advanced digital systems facilitated by network technologies such as IP cameras, which offer high-definition (HD/4K) resolution, night vision through infrared capabilities, and motion-based recording features. A primary benefit of these systems is their capacity to collaborate with image processing applications and machine learning models (Aliero et al., 2022).

The main challenge in CCTV systems lies in the vast amount of visual data generated, necessitating intelligent strategies to filter and extract meaningful information. Feature Selection (FS) plays a critical role here. Research has led to the development of an adaptive Capuchin Search Algorithm (CSA) to identify essential features from visual data. This method is highly relevant for processing CCTV data, such as in facial recognition systems, anomaly detection, and automatic tracking of individuals. Utilizing algorithms like CSA allows the system to automatically select frames or image sections containing the most critical data, enhancing classification speed and reducing computational demands (Braik et al., 2023).

Moreover, integrating CCTV cameras with edge computing technology facilitates local analytics on devices or nearby gateways, minimizing delays and enabling immediate responses. For instance, if the camera detects suspicious activity, it can immediately trigger

an alarm without waiting for commands from a central data center. This innovation allows for the deployment of CCTV systems in areas with limited network access, such as remote or restricted industrial locations (Saleem et al., 2022). Consequently, the role of CCTV cameras in intelligence monitoring frameworks has evolved far beyond their conventional use. CCTV has become a vital element in data-driven surveillance frameworks, serving not only to record but also to analyze, assess threats, and make decisions based on visual data, positioning CCTV as a pivotal component in creating secure, adaptable, and sophisticated environments.

3.3.2 PIR motion sensors

Passive Infrared Sensors (PIR) are key components in intelligence monitoring systems, designed to detect the presence and movement of humans or objects based on changes in infrared radiation. These sensors work by detecting infrared energy emitted by living objects, particularly humans, and generate electrical signals when there is a significant change in their field of view. Technically, a PIR sensor consists of pyroelectric elements that react to variations in infrared radiation levels. When someone passes through the sensor's observation area, these changes cause a voltage difference between the sensor elements, resulting in an electrical pulse that can activate other devices such as CCTV cameras, alarm systems, or automatic lighting. The primary advantages of PIR sensors are their low power consumption, cost efficiency, and capability to operate under various lighting conditions (Labouré et al., 2023).

In modern intelligence monitoring systems, PIR sensors function not only as device triggers but also as data sources in the Internet of Things (IoT) network. Motion data collected from PIR sensors can be analyzed in real-time to map activity patterns in an area, identify critical times, and distinguish between human movements and other objects through AI-based classification. This indicates that raw data from PIR sensors must undergo filtering and feature selection to avoid false positives, such as detecting small animals or irrelevant sudden temperature changes. Using algorithmic approaches like feature selection and Capuchin Search Algorithm (CSA)-based metaheuristics, systems can focus solely on signals of high significance to security contexts (Kim et al., 2022).

Within the framework of edge computing and sensor networks, PIR sensors are often connected to microcontrollers like ESP32 or Raspberry Pi, enabling data to be analyzed locally at the edge before being sent to the cloud for further analysis. This advantage speeds up response times and reduces network bandwidth load. Furthermore, integrating PIR sensors in smart systems such as smart campuses, smart buildings, or public security systems allows for their use not only in threat detection but also for energy efficiency and user behavior modeling. For example, HVAC systems can be adjusted based on user presence detected by PIR sensors to dynamically save energy. Therefore, PIR motion sensors are vital components within the intelligence monitoring ecosystem. Their simple yet reliable detection capabilities, when combined with AI systems and IoT infrastructure, make significant contributions to the efficiency, responsiveness, and intelligence of modern surveillance systems (Mischos et al., 2023).

3.3.3 Microphones

Microphones, as acoustic input devices, play a crucial role in intelligence monitoring systems by providing audio-based information channels capable of detecting, recognizing, and classifying audio-centric events. The technology used in modern surveillance systems has evolved from passive analog microphones to low-power digital microphones with integrated signal processing, noise reduction, and directional pickup capabilities to enhance accuracy in complex environments. In intelligence systems, microphones are typically used for several key functions: detecting abnormal sounds such as screams, breaking glass, or explosions; voice recognition for authentication or speaker identification; and audio acquisition for event recording or machine learning model training. When combined with

other sensors like CCTV and PIR, microphones help systems create a multimodal representation of incidents in monitored environments.

The application of microphones in intelligent monitoring also has implications in artificial intelligence contexts, particularly in natural language processing and data mining. As part of an integrated surveillance ecosystem, microphones are valuable tools to complement visual and movement information. In specific scenarios, such as areas without lighting or camera blind spots, audio information can be a primary indicator of suspicious activity. Thus, in modern AI and IoT-based monitoring systems, microphones have evolved from passive voice recorders to active context-based sensors that directly contribute to detection, analysis, and decision-making processes (Loughran et al., 2023).

The combination of CCTV cameras, PIR motion sensors, and microphones forms the foundation of adaptive, responsive, and intelligent modern intelligence monitoring systems. Together, they function as sensory nodes within an IoT network, generating multimodal data for automatic analysis by AI-based systems. With support from edge processing and feature selection algorithms like CSA, current monitoring systems can efficiently and accurately filter relevant information from large data volumes. This marks a paradigm shift from reactive surveillance systems to predictive monitoring systems capable of detecting threats before escalation occurs.

3.4 Impact

The development of surveillance systems using the Internet of Things (IoT) and artificial intelligence (AI) has emerged as a critical solution across various fields, including healthcare, public safety, and government operations. These systems facilitate real-time data collection, automatic analysis, and proactive measures against various threats or incidents. However, like any other technology, the outcomes are not entirely advantageous. Both the pros and cons must be thoroughly examined (Fang et al., 2023).

3.4.1 Advantages

The implementation of intelligence monitoring systems, particularly those leveraging Internet of Things (IoT) and artificial intelligence (AI) technologies, has significantly enhanced the efficiency and effectiveness of various public sectors. These systems not only facilitate monitoring and problem identification but also enable rapid responses to potential dangers by addressing physical safety and public security issues. Through effective integration, intelligence monitoring systems can function not only as reactive surveillance mechanisms but also as forward-looking platforms that promote data-driven decision-making and bolster national resilience against increasingly complex threats.

In the realm of intelligence operations, monitoring systems are crucial for detecting unusual activity trends, such as movements toward secure zones, unexpected large gatherings, or anomalous communications that may indicate intelligence initiatives, sabotage, or threats to national security. These systems operate using surveillance cameras, motion detectors, microphones, and various digital devices governed by AI-powered central networks. Comparable systems can provide early warnings derived from real-time information collected from mobile devices (Fu et al., 2023).

This concept, also relevant in the context of infectious diseases, applies to intelligence fields where information from detectors is used to identify abnormal trends, which are then analyzed by systems to issue early warnings to security personnel. For instance, if an individual frequently visits sensitive areas at unusual times or exhibits a habit of sending peculiar encrypted messages, the system can initiate additional scrutiny before the threat escalates. Thus, intelligence surveillance systems do more than record incidents; they predict and assess actions, enhancing a nation's ability to proactively address internal and external dangers (Zemenkova et al., 2022).

From a social perspective, the implementation of intelligence monitoring systems also provides indirect protection for the community. By integrating location-based information

into public applications, individuals can quickly become aware if they are near high-risk areas or suspicious activities. This shifts the public from being mere objects of surveillance to active partners in maintaining security. In the context of intelligence, such systems notify communities to avoid locations under investigation or deemed high-risk for security disruptions. This contributes to creating a more situationally aware social ecosystem, where people become accustomed to being vigilant and responsive to security changes around them. With these systems, threat information is no longer exclusive to intelligence agencies but becomes part of public communication, enhancing collective detection and broader threat management (Chaka, 2023).

3.4.2 Disadvantages

Despite the strategic benefits of intelligence monitoring systems, their implementation comes with several challenges that require attention. These difficulties encompass not only technical and operational constraints but also financial implications and long-term impacts related to infrastructure maintenance. Two of the most significant drawbacks associated with the deployment of intelligence monitoring systems are the financial burden and the complex nature of system maintenance, which can affect the ongoing efficiency of monitoring suspicious behavior (Okenyi et al., 2024).

Intelligence monitoring systems require significant investment, not only in physical components such as cameras, sensors, servers, and networks but also in digital elements like cloud technology, AI, and cybersecurity measures. This financial pressure presents a considerable challenge, especially in areas with limited budgets or varying developmental priorities. It is paradoxical, as the areas most in need of monitoring systems often lack the resources to implement them successfully. Similar to scenarios involving IoT-supported diagnostic technologies, resource limitations significantly impact the extent to which these systems can be adopted (Gómez-Quintana et al., 2021). In the realm of intelligence monitoring systems, this illustrates how inadequate financial resources can hinder the equitable allocation of surveillance technology, leading to security vulnerabilities in various areas. Over time, such situations can be exploited by malicious individuals seeking weaknesses in minimally monitored areas to engage in suspicious activities such as infiltration, espionage, or human trafficking.

Additionally, maintaining intelligence monitoring systems requires various technical components such as sensor calibration, software updates, replacement of outdated equipment, and continuous evaluation of network efficiency. This complex setup is further complicated by potential outages, which can severely impede intelligence workflows. When a component malfunctions, such as a poorly functioning camera or an overloaded server, these vulnerabilities become exploitable gaps for individuals engaging in suspicious activities. The importance of system reliability is crucial for operational success. However, in the realm of intelligence tasks, ensuring a consistently reliable system demands a dedicated technical team and significant ongoing costs (Ivanov et al., 2021).

Without carefully designed maintenance strategies, even advanced systems may struggle to identify unusual activities, particularly in challenging external environments or amidst significant cyber threats. This highlights that the ability of these monitoring systems to withstand operational disruptions is a major weakness. While monitoring systems have significant potential to enhance public safety and security through adaptive and automated technology, they also present real challenges regarding funding and maintenance. As a result, the development of these systems must incorporate technological sustainability strategies to ensure they are not only technically efficient but also viable from social and economic perspectives.

3.5 Challenges

Intelligence monitoring systems are crucial components of national safety and public risk management in today's digital landscape. By quickly identifying unusual trends and

integrating various data channels through the Internet of Things and AI technologies, these systems serve as fundamental resources for anticipating and preventing threats. Nevertheless, their implementation faces significant hurdles, arising both from the overseeing government authorities and the increasing complexity of future scenarios.

3.5.1 Government

Governments, acting as the primary overseers of intelligence monitoring frameworks, encounter various systemic obstacles including inter-agency collaboration issues and privacy legislation. Another challenge is the gap between current technological advancements and traditionally inflexible bureaucratic frameworks. While surveillance systems provide instantaneous data, actual implementation in the field is often hindered by slow coordination or a lack of skilled personnel. Consequently, the effectiveness of decisions made through intelligence systems depends on how well agencies integrate their information; without strong systemic interoperability, the risk of persistent leaks or inefficiencies can undermine the system (Abdulkareem & Petersen, 2021).

A major challenge arises from the limited availability of data collection sources and the sluggish bureaucracy that applies to national monitoring frameworks. This is especially evident in many developing countries, where advanced monitoring frameworks lack managerial and legal support. In the intelligence arena, this implies that when potentially harmful actions are identified, responses may be delayed or entirely overlooked due to administrative constraints.

3.5.2 The future of intelligence monitoring systems

The challenges facing intelligence monitoring systems in the coming years are becoming increasingly complex, particularly with regard to the growing volume of data, the need for accurate forecasting, and the protection of civil liberties in the digital landscape. Future surveillance systems must adapt not only to passively observe suspicious actions but also to proactively predict potential threats using AI-driven predictive analytics. Nevertheless, substantial obstacles arise in the form of data overload, algorithmic bias, and the tension between preserving privacy and ensuring security. Emerging intelligence frameworks will need to manage vast amounts of data points sourced from diverse devices, including personal gadgets like smartphones, smart vehicles, and home surveillance cameras (Zeng et al., 2024).

4. Conclusions

Considering the complexity of contemporary security risks, the development of monitoring systems integrating sensor technology and artificial intelligence (AI) has emerged as a crucial necessity. These systems aim not only to observe but also to accurately recognize and respond to suspicious actions without delay. By combining advanced sensor capabilities, responsive control mechanisms, and AI programming, these configurations can provide security measures that far surpass traditional methods, which are often reactively reliant on human intervention.

These automated control systems allow various devices such as surveillance cameras, passive infrared motion detectors, and audio recording devices to function cohesively through Internet of Things platforms. These devices are responsible for gathering real-time data, subsequently analyzed by AI components to identify trends and detect potential risks. By leveraging machine learning, these systems enhance their detection precision by learning from historical data over time.

The identified information is used by control mechanisms to determine necessary responses, such as triggering alarms, notifying security personnel, or automatically capturing visual documentation. In terms of application, these systems are versatile enough to be adapted to various settings, including public spaces like airports and stations, as well

as private sectors such as industrial zones, residential areas, and corporate offices. The use of this technology offers numerous advantages, such as increased monitoring efficiency, long-term cost savings, and the ability to operate continuously without the fatigue experienced by human workers.

Nevertheless, there are significant challenges that must be addressed to ensure the quality and sustainability of these frameworks. These challenges range from technical elements such as device integration and network connection reliability to social and legal issues like privacy protection, ethical implications of data usage, and government policies that are not yet prepared for rapid technological advancements. This underscores the vital role of governments in crafting policies and regulations that foster innovation while upholding individual rights. Looking ahead, these systems are poised for further advancement by leveraging cloud computing capabilities, edge data processing, and integration with broader national security frameworks. Through these strategies, not only is effective surveillance achieved, but also intelligent and automated prevention and response capabilities, positioning these systems as crucial components in creating safe and sustainable environments. The framework for automated management in sensor and AI-based intelligence monitoring systems signifies technological progress aimed at enhancing public safety. With continued advancement and collaboration among involved stakeholders, these systems have the potential to evolve into fundamental elements for more cohesive, responsive, and accurate surveillance initiatives.

Furthermore, active community involvement is a crucial component for the effective deployment of these systems. Educating the public about the benefits, operational mechanisms, and data security policies is essential to fostering trust and gaining support from various entities. Through responsible technology utilization, these intelligence monitoring systems will not only enhance physical safety but also support emotional well-being. Looking ahead, collaboration between technology and individuals will form a core principle in building secure and adaptable environments that focus on social sustainability and the protection of human rights.

Acknowledgement
The authors express their sincere gratitude to the esteemed reviewers and editors for their valuable time, insightful comments, and constructive suggestions, which have greatly contributed to the improvement of this manuscript.

Author Contribution
The authors contributed fully to the writing of this scientific article, from the planning stage to the final editing.

Funding
This research received no external funding.

Ethical Review Board Statement
Not available.

Informed Consent Statement
Not available.

Data Availability Statement
Not available.

Conflicts of Interest
The authors declare no conflict of interest.

Open Access

References

Abdulkareem, M., & Petersen, S. E. (2021). The promise of ai in detection, diagnosis, and epidemiology for combating COVID-19: Beyond the hype. *Frontiers in Artificial Intelligence, 4*. https://doi.org/10.3389/frai.2021.652669

Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems*, *4*, 110–128. KeAi Communications Co. https://doi.org/10.1016/j.iotcps.2023.09.003

Aliero, M. S., Asif, M., Ghani, I., Pasha, M. F., & Jeong, S. R. (2022). Systematic review analysis on smart building: Challenges and opportunities. *Sustainability (Switzerland)*, *4*(5). MDPI. https://doi.org/10.3390/su14053009

Boltsi, A., Kalovrektis, K., Xenakis, A., Chatzimisios, P., & Chaikalis, C. (2024). Digital tools, technologies, and learning methodologies for education 4.0 frameworks: A STEM oriented survey. *IEEE Access*, *12*, 12883–12901. https://doi.org/10.1109/ACCESS.2024.3355282

Braik, M., Awadallah, M. A., Al-Betar, M. A. A., Hammouri, A. I., & Alzubi, O. A. (2023). Cognitively enhanced versions of capuchin search algorithm for feature selection in medical diagnosis: COVID-19 Case Study. *Cognitive Computation*, *15*(6), 1884–1921. https://doi.org/10.1007/s12559-023-10149-0

Chaka, C. (2023). Detecting AI content in responses generated by ChatGPT, YouChat, and Chatsonic: The case of five AI content detection tools. *Journal of Applied Learning and Teaching*, *6*(2), 94–104. https://doi.org/10.37074/jalt.2023.6.2.12

Chen, W., Zhao, G., Wang, J., Qian, B., & Dou, W. (2023). Power supply station equipment status monitoring and evaluation system based on wireless network technology. *International Journal of Thermofluids*, *20*. https://doi.org/10.1016/j.ijft.2023.100514

Cho, S., Ma, J., & Yakimenko, O. A. (2023). Aerial multi-spectral AI-based detection system for unexploded ordnance. *Defence Technology*, *27*, 24–37. https://doi.org/10.1016/j.dt.2022.12.002

de Boer, K., & Schroën, K. (2024). Polymer-based stimuli-responsive systems for protein capture: capacity, reversibility, and selectivity. In *Separation and Purification Technology* (Vol. 337). Elsevier B.V. https://doi.org/10.1016/j.seppur.2024.126288

Desaire, H., Chua, A. E., Kim, M. G., & Hua, D. (2023). Accurately detecting AI text when ChatGPT is told to write like a chemist. *Cell Reports Physical Science*, *4*(11). https://doi.org/10.1016/j.xcrp.2023.101672

Desalegn, B., Gebeyehu, D., & Tamirat, B. (2022). Wind energy conversion technologies and engineering approaches to enhancing wind power generation: A review. *Heliyon, 8*(11). https://doi.org/10.1016/j.heliyon.2022.e11263

El khediri, S., Benfradj, A., Thaljaoui, A., Moulahi, T., Ullah Khan, R., Alabdulatif, A., & Lorenz, P. (2024). Integration of artificial intelligence (AI) with sensor networks: Trends, challenges, and future directions. *Journal of King Saud University - Computer and Information Sciences*, *36*(1). https://doi.org/10.1016/j.jksuci.2023.101892

Elkhatat, A. M., Elsaid, K., & Almeer, S. (2023). Evaluating the efficacy of AI content detection tools in differentiating between human and AI-generated text. *International Journal for Educational Integrity*, *19*(1). https://doi.org/10.1007/s40979-023-00140-5

Fang, X., Zang, J., Zhai, Z., Zhang, L., Shu, Z., & Liang, Y. (2023). Exploring potential dual-stage attention based recurrent neural network machine learning application for dosage prediction in intelligent municipal management. *Environmental Science: Water Research and Technology*, *9*(3), 890–899. https://doi.org/10.1039/d2ew00560c

Fu, Y., Liu, Y., Song, W., Yang, D., Wu, W., Lin, J., Yang, X., Zeng, J., Rong, L., Xia, J., Lei, H., Yang, R., Zhang, M., & Liao, Y. (2023). Early monitoring-to-warning Internet of Things system for emerging infectious diseases via networking of light-triggered point-of-care testing devices. *Exploration*, *3*(6). https://doi.org/10.1002/EXP.20230028

Gawande, U., Hajari, K., & Golhar, Y. (2024). Novel person detection and suspicious activity recognition using enhanced YOLOv5 and motion feature map. *Artificial Intelligence Review*, *57*(2). https://doi.org/10.1007/s10462-023-10630-0

Gómez-Quintana, S., Schwarz, C. E., Shelevytsky, I., Shelevytska, V., Semenova, O., Factor, A., Popovici, E., & Temko, A. (2021). A framework for ai-assisted detection of patent ductus arteriosus from neonatal phonocardiogram. *Healthcare (Switzerland)*, *9*(2). https://doi.org/10.3390/healthcare9020169

Irwanto, F., Hasan, U., Lays, E. S., De La Croix, N. J., Mukanyiligira, D., Sibomana, L., & Ahmad, T. (2024). IoT and fuzzy logic integration for improved substrate environment management in mushroom cultivation. *Smart Agricultural Technology*, *7*. https://doi.org/10.1016/j.atech.2024.100427

Ivanov, O., Neagu, B. C., Gavrilas, M., & Grigoras, G. (2021). A phase generation shifting algorithm for prosumer surplus management in microgrids using inverter automated control. *Electronics (Switzerland)*, *10*(22). https://doi.org/10.3390/electronics10222740

Kang, C. C., Tan, J. D., Ariannejad, M., Bhuiyana, M. A. S., Ng, Z. N., & Yong, S. C. H. (2023). Smart sensor controller for HVAC system. *Energy Reports*, *9*, 60–63. https://doi.org/10.1016/j.egyr.2023.09.113

Khazane, H., Ridouani, M., Salahdine, F., & Kaabouch, N. (2024). A Holistic Review of Machine Learning Adversarial Attacks in IoT Networks. In *Future Internet* (Vol. 16, Issue 1). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/fi16010032

Kim, T. eun, Perera, L. P., Sollid, M. P., Batalden, B. M., & Sydnes, A. K. (2022). Safety challenges related to autonomous ships in mixed navigational environments. *WMU Journal of Maritime Affairs*, *21*(2), 141–159. https://doi.org/10.1007/s13437-022-00277-z

Labouré, V. M., Schunert, S., Terlizzi, S., Prince, Z. M., Ortensi, J., Lin, C. S., Charlot, L. M., & DeHart, M. D. (2023). Automated power-following control for nuclear thermal propulsion startup and shutdown using MOOSE-based applications. *Progress in Nuclear Energy*, *161*. https://doi.org/10.1016/j.pnucene.2023.104710

le Febvrier, A., Landälv, L., Liersch, T., Sandmark, D., Sandström, P., & Eklund, P. (2021). An upgraded ultra-high vacuum magnetron-sputtering system for high-versatility and software-controlled deposition. *Vacuum*, *187*. https://doi.org/10.1016/j.vacuum.2021.110137

Loughran, B., Streeter, M. J. V., Ahmed, H., Astbury, S., Balcazar, M., Borghesi, M., Bourgeois, N., Curry, C. B., Dann, S. J. D., Diiorio, S., Dover, N. P., Dzelzainis, T., Ettlinger, O. C., Gauthier, M., Giuffrida, L., Glenn, G. D., Glenzer, S. H., Green, J. S., Gray, R. J., Palmer, C. A. J. (2023). Automated control and optimization of laser-driven ion acceleration. *High Power Laser Science and Engineering*, *11*. https://doi.org/10.1017/hpl.2023.23

Masson, T. M., Zondag, S. D. A., Kuijpers, K. P. L., Cambié, D., Debije, M. G., & Noël, T. (2021). Development of an off-grid solar-powered autonomous chemical mini-plant for producing fine chemicals. *ChemSusChem*, *14*(24), 5417–5423. https://doi.org/10.1002/cssc.202102011

Mischos, S., Dalagdi, E., & Vrakas, D. (2023). Intelligent energy management systems: a review. *Artificial Intelligence Review*, *56*(10), 11635–11674. https://doi.org/10.1007/s10462-023-10441-3

Okenyi, V., Bodaghi, M., Mansfield, N., Afazov, S., & Siegkas, P. (2024). A review of challenges and framework development for corrosion fatigue life assessment of monopile-supported horizontal-axis offshore wind turbines. In *Ships and Offshore Structures* (Vol. 19, Issue 1, pp. 1–15). Taylor and Francis Ltd. https://doi.org/10.1080/17445302.2022.2140531

Omoloye, A., Weisenburger, S., Lehner, M. D., & Gronier, B. (2024). Menthacarin treatment attenuates nociception in models of visceral hypersensitivity. *Neurogastroenterology and Motility*, *36*(4). https://doi.org/10.1111/nmo.14760

Orzechowski, M., Skuban-Eiseler, T., Ajlani, A., Lindemann, U., Klenk, J., & Steger, F. (2023). User perspectives of geriatric German patients on smart sensor technology in healthcare. *Sensors*, *23*(22). https://doi.org/10.3390/s23229124

Pereira, R. C. A., da Silva, O. S., de Mello Bandeira, R. A., dos Santos, M., de Souza Rocha, C., Castillo, C. dos S., Gomes, C. F. S., de Moura Pereira, D. A., & Muradas, F. M. (2023). Evaluation of smart sensors for subway electric motor escalators through AHP-Gaussian method. *Sensors*, *23*(8). https://doi.org/10.3390/s23084131

Rehman, Z., Tariq, N., Moqurrab, S. A., Yoo, J., & Srivastava, G. (2024). Machine learning and internet of things applications in enterprise architectures: Solutions, challenges, and open issues. *Expert Systems*, *41*(1). https://doi.org/10.1111/exsy.13467

Saleem, M. U., Usman, M. R., Usman, M. A., & Politis, C. (2022). design, deployment and performance evaluation of an iot based smart energy management system for demand side management in smart grid. *IEEE Access*, *10*, 15261–15278. https://doi.org/10.1109/ACCESS.2022.3147484

Schlaeger, S., Shit, S., Eichinger, P., Hamann, M., Opfer, R., Krüger, J., Dieckmeyer, M., Schön, S., Mühlau, M., Zimmer, C., Kirschke, J. S., Wiestler, B., & Hedderich, D. M. (2023). AI-based detection of contrast-enhancing MRI lesions in patients with multiple sclerosis. *Insights into Imaging*, *14*(1). https://doi.org/10.1186/s13244-023-01460-3

Sekizawa, Y., Hasegawa, Y., Mitomo, H., Toyokawa, C., Yonamine, Y., & Ijiro, K. (2024). Dynamic orientation control of gold nanorods in polymer brushes by their thickness changes for plasmon switching. *Advanced Materials Interfaces*, *11*(11). https://doi.org/10.1002/admi.202301066

Smarsly, K., & Dragos, K. (2024). Advancing civil infrastructure assessment through robotic fleets. *Internet of Things and Cyber-Physical Systems*, *4*, 138–140. https://doi.org/10.1016/j.iotcps.2023.10.003

Vassányi, I., Szakonyi, B., Loi, D., Mantur-Vierendeel, A., Quintas, J., Solinas, A., Blažica, B., Raffo, L., Guicciardi, M., Manca, A., Gaál, B., & Rárosi, F. (2024). Impact of information technology supported serious leisure gardening on the wellbeing of older adults: The turntable project. *Geriatric Nursing*, *55*, 339–345. https://doi.org/10.1016/j.gerinurse.2023.12.014

Zemenkova, M. Y., Chizhevskaya, E. L., & Zemenkov, Y. D. (2022). Intelligent monitoring of the condition of hydrocarbon pipeline transport facilities using neural network technologies. *Journal of Mining Institute*, *258*, 933–944. https://doi.org/10.31897/PMI.2022.105

Zeng, H., Yunis, M., Khalil, A., & Mirza, N. (2024). Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity. *Journal of Innovation and Knowledge*, *9*(4). https://doi.org/10.1016/j.jik.2024.100601

Zhao, Y. (2023). Digital governance with smart sensors: Exploring grid administration in Zhejiang's "future Community." *Journal of Computer-Mediated Communication*, *28*(5). https://doi.org/10.1093/jcmc/zmad016

Biographies of Authors

Fahreza Alfarizi, Sekolah Tinggi Inteligen Negara, Bogor, West Java 16810, Indonesia.
- Email: fahrezaalfarizi10@gmail.com
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Poppy Setiawati Nurisnaeny, Sekolah Tinggi Inteligen Negara, Bogor, West Java 16810, Indonesia.
- Email: poppyseiawati@gmail.com
- ORCID: 0000-0003-0531-0019
- Web of Science ResearcherID: KBC-6127-2024
- Scopus Author ID: 57222902846
- Homepage: https://sinta.kemdiktisaintek.go.id/authors/profile/6707444