# Construction of Intelligent Safety Management System: Collaborative Innovation of Artificial Intelligence and Internet of Things Technology

**Wu Jiajun, Li Gang, Li Guanglei**
*Wulong District People's Hospital, Chongqing, China*

**Abstract: As the complexity and security threats in cities continue to escalate, traditional security management models face bottlenecks such as data silos and delayed responses. This paper proposes a new security management system centered on the collaboration of the Internet of Things (IoT) and artificial intelligence (AI). By constructing multi-source sensing networks, implementing dynamic decision-making through intelligent algorithms, and adopting adaptive protection mechanisms, this system achieves a closed-loop management process for security. Through empirical analysis in smart city transportation, environmental monitoring, and public safety, the paper verifies the significant advantages of this system in improving risk warning accuracy and optimizing emergency response efficiency, while also providing a theoretical framework for future technological integration directions.**

**Keywords: Artificial Intelligence; Internet of Things; Environmental Sensor; Cross-Modal Fusion; Collaborative Innovation**

## 1. Introduction

In the wave of digital transformation, traditional security management models are facing severe challenges. The security needs in industrial facilities, smart cities, and critical infrastructure are becoming increasingly complex. Relying solely on manual inspections or static rules is no longer sufficient to address dynamic risks (such as cyber attacks, equipment failures, and sudden public incidents). The deep integration of artificial intelligence (AI) and Internet of Things (IoT) technologies offers a breakthrough solution for building intelligent security management systems. IoT collects real-time data from the environment, equipment, and personnel through ubiquitous sensing networks, enabling comprehensive monitoring capabilities. AI endows systems with the advantages of data mining, risk prediction, and autonomous decision-making, allowing for a paradigm shift from "passive response" to "proactive defense." For example, in industrial settings, AI algorithms can analyze data such as equipment vibration and temperature transmitted by IoT sensors to predict mechanical failures in advance. In the field of smart security, AI vision combined with edge computing can identify abnormal behaviors in real-time and trigger emergency responses. Current research often focuses on optimizing individual technologies, with insufficient exploration of the collaborative mechanisms between AI and IoT, leading to issues such as data silos, computational bottlenecks, and decision delays in practical applications. This paper aims to systematically analyze the synergistic logic between the two, construct a closed-loop management framework of "perception-analysis-decision-feedback," and explore its implementation paths in key areas, providing a reference for intelligent security management that combines theoretical depth and practical value. The study will combine trends in technology convergence and industry pain points to reveal technical paths, challenges, and future directions for collaborative innovation, bridging the gap between existing theory and application.

## 2. Technological Synergy between the Internet of Things and Artificial Intelligence

### 2.1 Reconstruction of the Perception Layer of the Internet of Things

The reconstruction of the IoT perception layer forms the foundational transformation of an intelligent safety management system. In the context of modern urban safety management, traditional discrete sensing devices can no longer meet the demands for real-time and precise information. The new generation of IoT technology constructs an integrated "air-space-ground" three-dimensional perception network, achieving a comprehensive digital mapping of all elements in the physical world [1]. This transformation is specifically reflected in the following aspects:

First, at the hardware level, environmental sensors collect environmental parameters at a frequency of once every 10 seconds, ensuring real-time data updates. The smart camera uses 4K ultra-high-definition imaging combined with HDR technology to maintain image clarity and accuracy even under complex conditions throughout the day [2]. Additionally, the recognition range of RFID tags has been extended from the traditional 3 meters to 15 meters, and it supports concurrent identification of multiple targets, significantly enhancing recognition efficiency and accuracy. Taking the Yizhuang Smart City Demonstration Zone in Beijing as an example, its deployment of 8,000 multifunctional sensor nodes forms a grid monitoring capability of 200 meters by 200 meters, achieving refined management of urban safety [3].

Secondly, in terms of data transmission, the application of 5G + TSN (Time-Sensitive Networking) technology effectively addresses the latency issues associated with massive data transfers [4]. Taking intelligent transportation scenarios as an example, the sampling frequency of geomagnetic sensors can reach up to 100 Hz. Through V2X communication between roadside units and vehicle terminals, a millisecond-level responsive vehicle-road coordination system is established [5]. Actual test data shows that the system's data throughput reaches 15 Gbps, with latency controlled within 20 ms. This provides real-time decision support for traffic safety management, significantly enhancing traffic efficiency and safety.

### 2.2 Breakthrough in the Cognitive Layer of Artificial Intelligence

Artificial intelligence technology has made breakthroughs at the cognitive level, endowing security management with a "smart brain." Deep learning algorithms achieve precise understanding of complex security scenarios through multi-level feature extraction and pattern recognition [6]. This breakthrough is mainly reflected in three aspects: In the field of visual analysis, the average precision (mAP) of the improved yolov5-based object detection algorithm on the COCO dataset reached 56.8%, an improvement of 12.3% over traditional methods. This significant enhancement means that the algorithm is more accurate and efficient in identifying and locating objects in images. In temporal prediction, the spatiotemporal prediction model combined with the Transformer architecture demonstrated notable advantages. The Transformer architecture's excellent handling of long-range dependencies enables the model to better capture dynamic changes and trends in time series data. The application of transfer learning addresses the challenge of model training in small sample scenarios [7]. Through transfer learning, the model can transfer knowledge learned from large datasets to new tasks with smaller data volumes, thereby achieving good performance even under limited data conditions.

### 2.3 Mechanism of Collaborative Innovation

In today's era of rapid development of science and technology, the collaborative innovation of the Internet of Things and artificial intelligence has built a complete closed-loop system of "perception-cognition-decision-optimization", which is realized by the close cooperation of three key links.

The in-depth mining of data value is the first step in the entire closed-loop system. Taking environmental safety monitoring as an example, sensors in the Internet of Things can collect real-time air quality data. After standardized processing at edge nodes, this data is fed into spatiotemporal fusion prediction models. This process not only enhances data usability but also provides a solid foundation for subsequent intelligent analysis and decision-making.

The precise execution of intelligent decisions forms the second stage of a closed-loop system. In this phase, the system continuously monitors predicted PM2.5 concentrations. If it detects that these levels exceed the preset threshold, the system immediately takes action. This includes triggering drones for patrol inspections to obtain more accurate on-site data, as well as using digital twin technology to simulate various response strategies, thereby selecting the optimal course of action. Such an intelligent decision-making process significantly enhances the efficiency and accuracy of emergency responses.

The continuous evolution of the system is the third stage of a closed-loop system. By establishing an effective feedback mechanism, each outcome of handling is used to feed back into the algorithm's optimization. This ongoing self-improvement mechanism ensures that the system can continuously adapt to new challenges and changes, thereby achieving long-term stable operation. The greatest value of this collaborative mechanism lies in creating a "data flywheel" effect: more data collection leads to better algorithms, which in turn generate greater value, and this greater value further incentivizes more data collection. This positive cycle not only enhances the overall performance of the system but also opens up new possibilities for research and application in related fields.

## 3. Core Application Scenario Verification

### 3.1 Intelligent Traffic Dynamic Control System

In the Yizhuang Demonstration Zone of Beijing, by deploying an advanced AIoT collaborative management platform, over 2,000 camera feeds and 500 sets of geomagnetic sensor data have been successfully integrated. This platform employs advanced reinforcement learning algorithms to deeply optimize traffic light timing schemes. After practical application testing, during peak morning hours, the optimized measures of this system significantly increased traffic efficiency by 23%. Additionally, the system excels in accident detection and response, reducing response time to an impressive 15 seconds. This innovative system effectively addresses the challenge of multi-intersection collaborative optimization, fully demonstrating the significant potential of technological collaboration in scale effects, providing new solutions for urban traffic management.

### 3.2 Intelligent Early Warning System for Environmental Risks

In Shenzhen, by applying advanced IoT spectral analyzers and artificial intelligence (AI) pollution source tracing models, an efficient "monitoring-tracing-treatment" linkage mechanism for atmospheric pollution has been successfully established. During the summer ozone exceedance incident in 2023, this system demonstrated its powerful capabilities, quickly pinpointing a non-compliant emission source 3 kilometers away within just 12 hours. Compared to traditional manual investigation methods, the efficiency was astonishingly eight times higher. This groundbreaking progress not only significantly reduced the time required to locate pollution sources but also markedly increased the response speed to environmental issues. Data statistics show that this high-tech collaborative system has reduced environmental governance costs by 37%, which not only represents economic savings but also reflects improvements in environmental quality and better protection of public health.

### 3.3 Public Safety Emergency Response Network

In a specific area of Hangzhou, people have established an advanced fire IoT platform. This platform ingeniously integrates temperature sensors, smoke detectors, and the building's BIM (Building Information Modeling) technology. When a fire unfortunately occurs, the AI engine on this platform can quickly perform intelligent analysis and fusion processing of real-time thermal maps with the building's structural data, thus rapidly calculating the optimal escape route. To more effectively guide people to evacuate safely, the system is also equipped with smart speakers that can send evacuation commands and guidance information in real time. In a simulation exercise conducted in 2022, the evacuation time guided by this system was reduced by 42% compared to traditional methods. This significant achievement fully demonstrates the great potential and value of cross-modal data fusion technology in enhancing public safety.

## 4. Technical Challenges and Optimization Paths

### 4.1 Data Security and Privacy Protection

In today's era of rapid digital development, data security and privacy protection have become indispensable issues in the process of technological progress and innovation. With the increasing diversity and heterogeneity of various devices, inconsistencies exist in encryption standards between different devices, which to some extent increases the likelihood of data leakage and security risks. For example, in a smart park scenario, the use of overly simple weak passwords by surveillance cameras led to a sensitive data leak incident, posing a serious threat to the park's security. To effectively address this challenge, we urgently need to establish a distributed authentication mechanism based on blockchain technology. This mechanism can provide decentralized secure authentication, significantly enhancing the overall system's security. At the same time, adopting federated learning methods can achieve data availability and privacy protection without directly sharing data, ensuring that data is properly protected during use and not leaked.

In addition, to address potential security vulnerabilities in IoT devices, we need to conduct regular security audits and vulnerability scans to promptly identify and fix any underlying security risks. At the same time, enhancing security awareness training and improving users' understanding of data security and privacy protection are also crucial measures for preventing data breaches and security risks. By implementing these comprehensive measures, we can build a more secure and reliable ecosystem where IoT and AI develop synergistically.

### 4.2 Bottleneck of Algorithmic Interpretability

Despite the remarkable achievements of deep neural networks in various fields such as image recognition, natural language processing, and predictive analytics, their inherent "black box" characteristics, namely lack of transparency and explainability, have become a significant barrier to their application in critical infrastructure and security-sensitive areas. These sectors often have extremely high demands for algorithmic explainability and transparency, as they need to ensure that every step of the decision-making process is clear and verifiable. To overcome this limitation, researchers and engineers have begun exploring and applying various interpretive tools, among which SHAP values are a highly effective tool. By calculating SHAP values, we can quantify the contribution of each input feature to the model's output, thereby revealing the logic behind the model's decisions. Moreover, building decision models that comply with international standards ISO/IEC 30166 not only ensures the accuracy of the model's decision-making process but also guarantees its explainability, meeting the stringent requirements for algorithmic transparency in critical facilities. Such models can provide decision-makers with necessary insights while ensuring safety and reliability, helping them understand the basis of the model's decisions and make more informed and evidence-based decisions.

However, enhancing the explainability of algorithms is not an overnight process; it requires improvement without compromising model performance. This means that in pursuing algorithmic explainability, we must balance the accuracy of the model with its explainability. To achieve this, some researchers have proposed hybrid models, which combine deep learning models with traditional machine learning models to leverage the explainability of traditional models to compensate for the shortcomings of deep learning models. Additionally, developing more intuitive and user-friendly visualization tools is also a crucial approach to improving algorithmic explainability. These tools can help non-experts better understand the decision-making process of the model, thereby promoting the broader application of algorithms.

### 4.3 Improvement of System Fault Tolerance

In extreme environmental conditions, sensors may experience data drift due to various unpredictable factors such as temperature fluctuations, humidity changes, and electromagnetic interference. This data drift can directly impact the stability and reliability of the entire system. To effectively enhance the system's fault tolerance and ensure efficient operation in complex environments, it is recommended to use digital twin technology to build a virtual mirror system. The core of digital twin technology lies in creating a virtual replica that corresponds to physical entities in the real world. This virtual replica can monitor and analyze the state of the physical entity in real time. Through this real-time monitoring and analysis, data drift issues can be identified and corrected promptly, ensuring the accuracy of the data and the stability of the system. Additionally, by applying reinforcement learning to train robust algorithms, self-learning and self-optimization capabilities can be achieved within the system. This self-learning and self-optimization capability means that the system can maintain over 80% functional integrity even when faced with challenges such as a 30% node failure. Therefore, adopting digital twin technology and reinforcement learning algorithms can significantly improve the stability and reliability of the system, ensuring its efficient operation in various extreme environments.

## 5. Conclusions

As the sixth-generation communication technology (6G) continues to advance and neural mimicry chip technology rapidly develops, future security management systems are expected to exhibit three significant characteristics. First, the autonomous collaboration capabilities of edge intelligent devices will be significantly enhanced. These devices will be able to communicate information and collaborate on tasks more efficiently without excessive human intervention. They will be capable of autonomously identifying the environment, making decisions, and achieving intelligent interaction between devices without central control. Second, the application of knowledge graph technology will make cross-domain risk simulation a reality. By constructing complex data relationship networks, it can more accurately predict and respond to various potential security threats. Knowledge graphs will integrate data from different fields, providing a comprehensive perspective that helps security experts understand the root causes and propagation paths of risks. Third, the hybrid augmented intelligence model of human-machine coexistence will become widely popular. In this model, humans and intelligent systems will form a close partnership, jointly improving decision quality and work efficiency. Human intuition and the computational power of intelligent systems will complement each other, making the decision-making process more precise and efficient. With the deep integration of these technologies, we can expect to witness a new phase in security management, an era of "self-awareness, self-learning, and self-evolution," which will greatly enhance the adaptability and foresight of security management systems. Security systems will be able to perceive environmental changes in real-time, autonomously learn new security strategies, and continuously evolve to address evolving threats, thereby providing solid support for social stability and safety.

## Acknowledgments

This paper is supported by Discussion Project on Enhancing Safety Management through Intelligent Construction of Wulong District People's Hospital in Chongqing City

## References

[1] Chen Binbin. Analysis on the Application of Intelligent Sensors in Ecological Environment Monitoring [J]. Leather Making and Environmental Protection Technology, 2024,5(23):41-42+48.

[2] Lin Wanxia. Cross-modal Information Retrieval Algorithm Based on Multimodal Fusion and Communication [D]. Nanjing University, 2012.

[3] Yang Kejie. From the Internet Era to the "Internet of Things" Era [N]. Guangming Daily, 2009-02-23 (008).

[4] Huang Xinya. RFID (Radio Frequency Identification) Technology [J]. Police Technology, 1994, (04): 29-30.

[5] Zhang Haiyuan. A Practical View of Artificial Intelligence [J]. Social Science Journal, 1983, (01): 19-28.

[6] M. Samorvico, G. Guieda, Qing Song. Problems and Future of Artificial Intelligence [J]. Foreign Automation, 1981, (06):1-7+21.

[7] Zhu Qing. Collaborative Innovation: Basic Strategy of Technological Innovation after China's Entry into the WTO [N]. Guangming Daily, 2001-11-20 (A04).