Research on Intelligent Security System Technology Based on the Concept of Intelligent Buildings

Yutong Wang, Jianying Weng*, Meiting Sun
Shandong Engineering Vocational and Technical University, Jinan 250000, Shandong, China

Abstract: With the advancement of IoT, artificial intelligence, and big data, intelligent building security systems are shifting from passive defense to proactive perception and intelligent decision-making. Based on the intelligent building concept, this paper proposes a "perception–transmission–analysis–execution" architecture, analyzes key technologies including multi-sensor fusion, AI-based video analytics, big data with cloud computing, edge computing, and network security, and discusses system integration, interoperability, and sustainable maintenance strategies, providing references for enhancing the intelligence and integration of building security management.
***Keywords*:** intelligent building; intelligent security; Internet of Things; artificial intelligence

1. Introduction

With the advancement of urbanization and building intelligence, security management demands are becoming increasingly diverse. Traditional security systems relying on manual monitoring and single alarm devices suffer from delayed response and information silos. The intelligent building concept emphasizes system integration and data-driven approaches, incorporating IoT, AI, and big data to enable real-time perception, intelligent analysis, and coordinated response. While foreign practices in standard systems and technologies are more mature, domestic development — though rapid — still requires improvements in integration, interoperability, and data security.

2. Overall Architecture of the Security System under the Concept of Intelligent Buildings

2.1 System Design Principles

(1) Integrity and Scalability.

The system should be built around a unified platform, integrating subsystems such as video surveillance, intrusion detection, access control, and fire alarm systems to achieve information sharing and coordinated response. The architecture should adopt a modular design to facilitate functional expansion and equipment upgrades according to building scale, functional changes, or technological updates[1].

(2) Real-time Performance and High Reliability.

The security system must respond to emergencies within milliseconds. Redundant design and dual-link communication should be employed to ensure uninterrupted transmission of critical data. Backup mechanisms at both device and network levels should be implemented to maintain normal operation even in the event of partial node failures.

(3) Intelligence and Adaptability.

Leveraging artificial intelligence algorithms, the system can automatically identify abnormal behaviors and learn patterns. It can dynamically adjust thresholds and optimize strategies based on environmental changes and historical data, thereby reducing false alarms and missed detections while improving response efficiency.

(4) Security and Privacy Protection.

Encryption, authentication, and access control technologies should be applied during data transmission, storage, and access. At the same time, relevant laws and regulations should be followed to ensure the privacy and compliance of sensitive data such as personal information and video images[2].

2.2 System Layered Structure

Intelligent security systems typically adopt a bottom-up four-layer architecture, as shown in Figure 1, forming a complete closed loop from data acquisition to execution and response. The perception layer obtains real-time information inside and outside the building through various sensing devices. The transmission layer uses wired and wireless networks to securely and quickly deliver data to the analysis platform. The analysis layer integrates multi-source information using AI and big

data algorithms to generate response strategies. The execution layer coordinates relevant security and emergency equipment based on the decision results to achieve immediate response and coordinated control. Each layer operates relatively independently in terms of function but maintains high interface compatibility, enabling smooth system upgrades and functional expansion, while ensuring overall operational stability and continuity in the event of local failures.

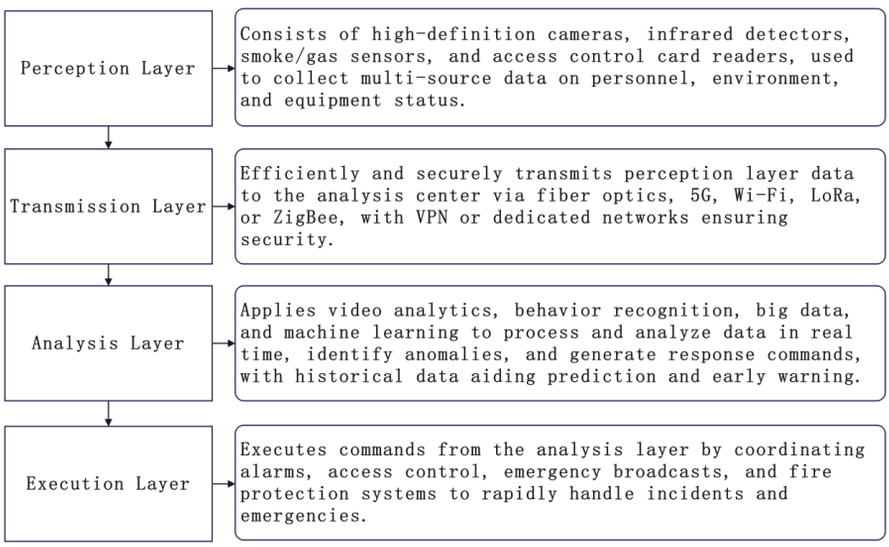

Figure 1. Schematic Diagram of the System Layered Structure

3. Key Technology Analysis

3.1 Multi-Sensor Fusion and IoT Technology

Intelligent security systems deploy a variety of sensors, including cameras, infrared detectors, smoke/gas sensors, and magnetic contacts. However, the collected data often differ in time stamps, formats, and precision. Multi-sensor fusion technology unifies heterogeneous data through time synchronization, data calibration, and weighted fusion, thereby improving detection accuracy and system robustness. The Kalman filter is commonly used for dynamic target state estimation:

$$\hat{x}_k = \hat{x}_k + K_k(z_k - H\hat{x}_k^-) \tag{1}$$

where $\hat{x}_k$ denotes the fused state estimate,K_k represents the Kalman gain, and z_k denotes the measurement observation. In practical engineering applications, different sensors may exhibit bias offsets and noise discrepancies. It is therefore necessary to introduce weighting coefficients into the fusion model, assigning higher weights to high-precision sensors to enhance overall reliability.

3.2 AI-Based Video Analysis Technology

AI-based video analysis enables a transition from passive monitoring to proactive warning. Convolutional neural network (CNN)-based detection algorithms such as YOLO and Faster R-CNN can identify pedestrians, vehicles, and objects in video streams, while tracking algorithms such as DeepSORT maintain continuous monitoring and trajectory analysis. Behavior recognition models leverage spatiotemporal features to detect anomalies such as trespassing, loitering, and unattended objects, thereby reducing the monitoring workload for security personnel. System performance is typically evaluated using precision, recall, and the F1-score:

$$F1 = \frac{2 \cdot \mathrm{Pr}ecision \cdot \mathrm{Re}call}{\mathrm{Pr}ecision + \mathrm{Re}call} \tag{2}$$

In complex lighting, weather, or background conditions, techniques such as infrared imaging and multispectral sensing can be incorporated to improve robustness. Additionally, online learning mechanisms allow continuous optimization of algorithm parameters, enabling the system to adapt to various building environments and pedestrian flow patterns while maintaining high detection accuracy.

3.3 Big Data Platform and Cloud Computing

During continuous operation, security systems generate massive amounts of video, image, and sensor data. Big data platforms utilize distributed storage and computing frameworks (e.g., Hadoop, Spark) to achieve efficient data storage and rapid retrieval, supporting historical incident tracing and pattern mining. Cloud computing provides elastic computing and storage resources, enabling centralized processing of high-concurrency tasks, while also supporting cross-regional data sharing and remote operation and maintenance.

3.4 Edge Computing and Latency Optimization

To reduce bandwidth consumption and latency in cloud processing, edge computing moves part of the data processing workload to the device side or local gateways. For example, front-end cameras can directly run object detection algorithms and upload only alarm-related clips to the cloud, significantly reducing data transmission volume. Edge nodes, through task allocation and resource scheduling mechanisms, can achieve millisecond-level response, effectively supporting immediate handling of emergencies such as intrusions and fires.

3.5 Network Security and Data Privacy Protection

Security systems transmit and store large volumes of highly sensitive data, making it essential to employ end-to-end encryption, two-factor authentication, and access control mechanisms to prevent data breaches. Intrusion detection systems and firewalls should be deployed to protect against malicious attacks and unauthorized access. At the same time, in the use of video and sensor data, relevant privacy regulations (e.g., GDPR) must be observed, and personally identifiable information should be anonymized to ensure that the system operates on a secure and compliant basis.

4. Analysis of Key Technologies

4.1 Cross-Subsystem Linkage Design

An intelligent security system is composed of subsystems such as video surveillance, access control, alarms, fire protection, and emergency broadcasting. Operating independently can lead to information delays and fragmented responses; thus, a unified platform is required to enable multi-system collaboration upon event triggers. For example, when an intrusion alarm is activated, the system can simultaneously retrieve video for target tracking, close relevant access points, and issue broadcast alerts. Linkage requires unified communication protocols and response rules to ensure efficient collaboration among devices from different vendors, along with graded response strategies to optimize resource utilization[3].

4.2 System Interoperability and Standardization

Subsystems from different vendors often vary in protocols and interfaces, affecting integration efficiency and stability. Universal standards, such as ONVIF, BACnet, and Modbus, should be introduced during the design phase to enable seamless cross-platform integration. Standardization should cover not only communication protocols but also data formats, event encoding, and interface security, ensuring data consistency and operational coherence. A unified device authentication and version management mechanism should be established to prevent unauthorized access and provide a solid foundation for future functional expansion and system upgrades.

4.3 Operation, Maintenance, and Sustainable Upgrade Strategies

System stability depends on long-term operation, maintenance, and optimization, including inspections, fault diagnosis, log analysis, backups, and security policy updates. Modular and hot-swappable designs facilitate the addition or replacement of devices without downtime. A performance evaluation and feedback mechanism should be implemented to monitor indicators such as response time and false alarm rate, enabling configuration optimization.

5. Conclusion

Based on the concept of intelligent buildings, the intelligent security system integrates multi-sensor fusion, AI-based video analytics, big data, edge computing, and network security to achieve comprehensive perception and efficient handling of building safety. Featuring a layered, modular architecture and enhanced through cross-subsystem linkage, standardized interoperability, and sustainable upgrades, the system significantly improves response speed and protection accuracy. Future work may incorporate higher-precision sensors and adaptive AI algorithms, and explore cross-building and cross-regional collaborative defense to enhance adaptability and long-term intelligence.

Acknowledgments

This study was supported by the Science and Technology Plan Project of the Department of Housing and Urban Rural Development of Shandong Province (Project No. 2024KYKF-MLYJ010), the Education and Teaching Research Project of Shandong Province (Project No. 2024417), the Education and Teaching Research Project of Shandong Province (Project No. JG202307), the Education and Teaching Reform Research Project of Shandong Engineering Vocational and Technical University (Project No. 202410406) and the Vocational Education and Teaching Reform Research Project of Shandong Province (Project No. 2024JXY588).

References

[1] Zhang Liang. Design of an Integrated Intelligent Building Security Monitoring System Guided by IoT Technology [J]. Information & Computer, 2025, 37(13): 61-63.
[2] Min Hao. Deepening the Application of Whole-House Physical Security Systems to Fully Safeguard Thousands of Households [J]. China Security, 2025, (05): 68-72.
[3] Yang Fajun. Design and Practice of Intelligent Building Security Systems Based on IoT [J]. Science & Technology Vision, 2025, 15(06): 54-56.

Author Bio

(1) Yutong Wang (October 2004-), female, Han ethnicity, from Dezhou, Shandong Province, undergraduate student, main research direction: construction engineering.

(2) *Corresponding author: Jianying Weng (1990.03-), female, Han nationality, from Liaocheng, Shandong Province, master's student, title: lecturer, main research direction: architectural design and vocational education.

(3) Meiting Sun (August 2004-), female, Han ethnicity, from Dezhou, Shandong Province, under-graduate student, main research direction: construction engineering.