Scientific Research Publishing

Open Journal of Applied Sciences, 2025, 15(12), 4078-4091
https://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

Research and Practice on an IoT-Enabled Security Management System for Vocational Training Bases

Xiaohuan Qiu

Guangzhou Railway Polytechnic, Guangzhou, China
Email: 18802069165@163.com

How to cite this paper: Qiu, X.H. (2025) Research and Practice on an IoT-Enabled Security Management System for Vocational Training Bases. *Open Journal of Applied Sciences*, **15**, 4078-4091.
https://doi.org/10.4236/ojapps.2025.1512263

Received: November 14, 2025
Accepted: December 20, 2025
Published: December 23, 2025

Abstract

Vocational training bases are centers for practical skill development, but their dynamic environments, high-value equipment, and potentially hazardous materials present complex security management challenges. Traditional management methods, which rely on manual inspections and passive responses, often result in delayed hazard detection and inefficient resource allocation. While the literature indicates that Internet of Things (IoT) technology is widely used in industrial sectors, its comprehensive application in educational training contexts remains underexplored. This paper presents the research and practice of an IoT-based security management system. The system employs a five-layer architecture (Basic Resource Layer, Data Layer, Service Support Layer, Application Layer, and Presentation Layer) and was iteratively developed using the Agile Scrum model. System development was guided by a series of defined user stories, integrating core functionalities including real-time monitoring, access control, environmental sensing, and asset tracking. The contribution of this paper is a scalable and replicable security solution that combines efficient management functions with pedagogical value, providing students with a practical platform for IoT and cybersecurity skills.

Keywords

Internet of Things (IoT), Security Management System, Vocational Training Bases, System Architecture, Agile Scrum, System Design

1. Introduction

Vocational education is a cornerstone of economic and social development. Recent national policies in China, such as the revised Vocational Education Law (2022), have elevated its strategic importance, mandating the deep integration of

industry and education, accelerating "informatization," and ensuring comprehensive "security" [1]. This places new and significant demands on vocational training bases, which are the primary centers for practical skill development. As the nation pushes for the construction of "high-quality training bases" and deepens the reform of the vocational education system [2], the associated management challenges have intensified. These bases are dynamic environments containing high-value equipment and diverse personnel. The complexity of these environments often leads to safety risks, necessitating robust mechanisms for emergency treatment and accident prevention [3]. Traditional management methods, often manual and reactive, are increasingly insufficient, creating a gap between the vision of constructing "smart training rooms" [4] and the on-the-ground reality.

The Internet of Things (IoT) has emerged as the key to enabling technology to bridge this gap. This technological shift is supported by government mandates, such as the Ministry of Education's directive to improve vocational school operating conditions [5], and provincial-level strategies like the Guangdong Provincial Education Digitalization Implementation Plan (2023-2027), which explicitly calls for digital transformation and unified management platforms [6].

The academic literature confirms this trend, with a growing body of research focused on the application of IoT for intelligent safety and management. Current research demonstrates the effectiveness of IoT in solving specific security challenges. For instance, advanced computer vision technologies, such as YOLOv5-based real-time smart monitoring systems, have been developed to increase safety awareness in educational institutions [7]. Similarly, specific IoT-based systems have been designed for safety monitoring in educational laboratories to handle environmental data and alerts [8]. To further enhance intelligence, some scholars have explored intelligent management systems utilizing IoT sensors and cloud-based mobile application [9]. Additionally, the implementation of safety access systems based on IoT has proven effective in controlling personnel entry in high-risk areas like chemistry laboratories [10].

Technologically, these solutions are advancing from simple monitoring to integrated management frameworks [11]. Sophisticated architectures, such as cloud-edge collaboration frameworks, are being proposed to support smart education facilities management [12], alongside research into all-weather monitoring for comprehensive campus security [13].

Despite this progress, a review of the literature reveals a significant gap. Many existing studies focus on specific functional modules—such as general laboratory management systems [14] or access control implementations [10]—or focus heavily on specific emerging technologies like Artificial Intelligence (AI) design schemes [15] or the integration of 5G communication [16]. However, there is a distinct lack of comprehensive "research and practice" papers that detail the entire process of designing, developing, and implementing a foundational, integrated IoT security management system. Such a system must be tailored to the unique dual needs of a vocational training base: enhancing management efficiency (safety,

security, asset tracking) while also providing pedagogical value.

To fill this gap, this paper details the "research and practice" of an IoT-enabled security management system designed for vocational training bases. This study's "research" component lies in designing a comprehensive solution to address the identified challenges, while the "practice" component involves the system's development, implementation, and core functionalities. The system is designed to seamlessly integrate real-time monitoring, intelligent analytics, access control, and asset tracking into a unified platform. This study adopts a developmental research design. The system is built upon a five-layer architecture (Basic Resource Layer, Data Layer, Service Support Layer, Application Layer, and Presentation Layer) to ensure modularity and scalability. The development process follows the Agile Scrum model, allowing for iterative refinement based on stakeholder needs. The contribution of this paper is a validated, replicable IoT security solution that not only enhances the operational safety of vocational training bases but also serves as a pedagogical platform for students to gain practical skills in IoT and cybersecurity.

2. Methodology and System Design

2.1. Research Design

This study employs a developmental research design. This approach aligns with the "research and practice" nature of the study, which aims to develop a practical solution to address the complex challenges of "industry-education integration" in vocational training bases. We adopt the System Development Life Cycle (SDLC) using the Agile Iterative methodology to construct, implement, and refine the solution.

2.2. System Development Model (Agile Scrum)

This study utilizes the Agile Scrum model for system development. This iterative model is essential for a system that must be "adaptive" to the "new technologies, new processes, new standards, and new business formats" characteristic of modern vocational training. The researcher assumed the key leadership roles within the Scrum process. As the Product Owner, the researcher articulated the product vision and prioritized the Product Backlog after gathering requirements from stakeholders. As the Scrum Master, the researcher facilitated the process, removed impediments, and ensured adherence to Agile principles. The Scrum Team, composed of developers and system specialists, collaboratively designed and built the functional increments.

The process began with the Product Backlog, followed by Sprint & Sprint Execution, where the team converted high-priority requirements into a working software increment. Each cycle concluded with a Sprint Review to demonstrate functionality to stakeholders and a Sprint Retrospective for process improvement, ensuring the solution remained aligned with practical user needs.

2.3. System Architecture

The system architecture is designed to promote the intelligent operation of the industry-education integration training base and support the "production-educa-

tion integration" goals. It establishes a data collection system that interfaces with base equipment through an intelligent gateway, enabling data to be processed and converted into services. To ensure modularity, scalability, and compliance, we designed a five-layer framework, as shown in Figure 1.

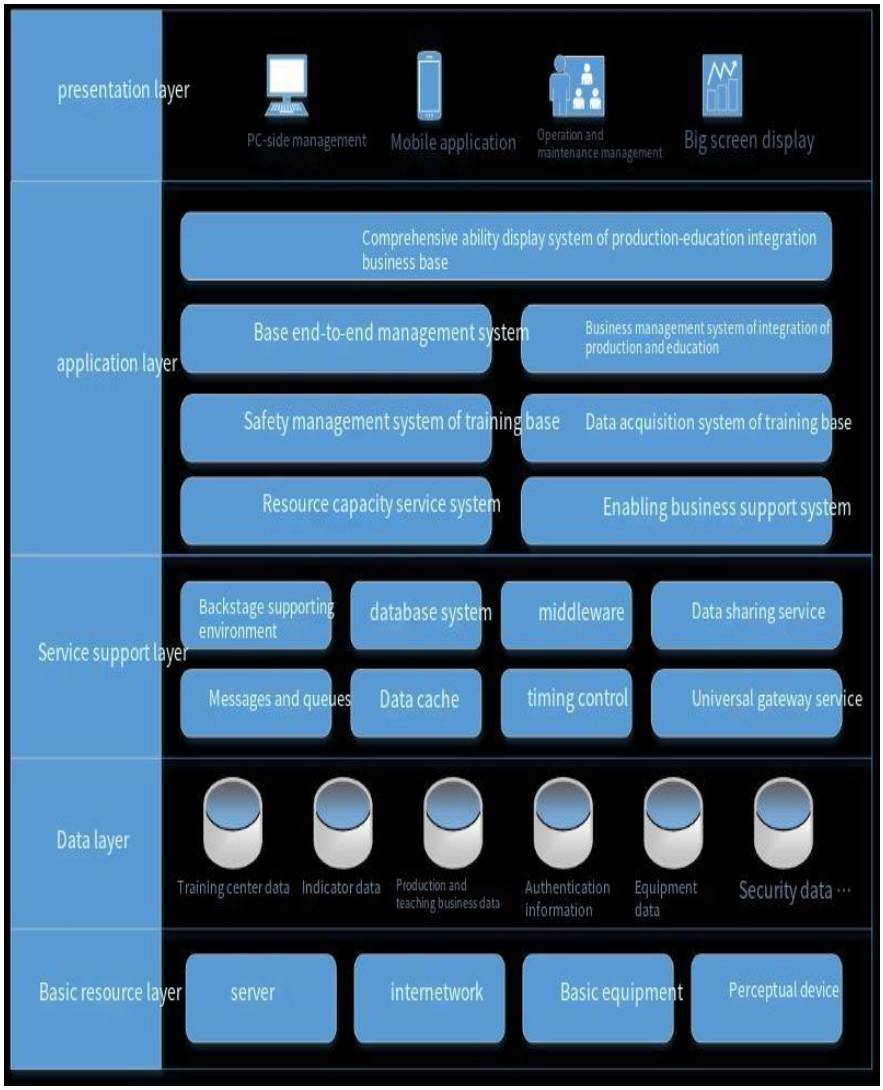

Figure 1. System architecture.

1) Basic Resource Layer: This is the foundational layer, built on cloud and internet environments. It establishes the resource pools for computing and storage servers, networks, and the physical sensing devices, such as IoT gateways, cameras, and environmental monitors, that form the basis for all data collection.

2) Data Layer: This layer serves as the central repository for data storage and management. It is designed to accommodate all production base support data, business-specific data, and interactive shared data. This includes training center records, performance indicators, equipment logs, and security data, ensuring accuracy, consistency, and availability.

3) Service Support Layer: This layer provides the critical middleware and backend support services. It includes database services, middleware frameworks, message queues for asynchronous processing, data caching mechanisms, and universal gateway services, ensuring efficient data flow and interoperability across the system.

4) Application Layer: This layer hosts the core business applications and service modules tailored for different user roles. Key applications include modules for managing vocational skill certification, ensuring the safety and security of training facilities, and collecting, processing, and analyzing operational data from the base.

5) Presentation Layer: This is the user-facing interface, providing intuitive interaction with the system. It is designed for all user roles, offering visual display dashboards accessible via both PC and mobile devices for real-time monitoring and data-driven decision-making.

The five-layer architecture was not a generic adoption of standard IT frameworks but was tailored to address the unique dual demands of vocational training bases—reliability of safety management and educational scalability—with targeted design choices and technical innovations. For the Basic Resource Layer, a multi-protocol adaptive gateway (Huawei AR502H) was adopted (supporting MQTT, CoAP, and Modbus) to resolve interoperability issues between the base's 50+ heterogeneous devices (new IoT sensors + legacy analog equipment, Section 3.4), achieving a 99.2% data transmission success rate over 1 month of continuous operation. The Data Layer introduced a dual-mode storage structure: hot data (real-time video streams, sensor alerts) was stored in Redis cache (latency < 10 ms) for instant AI analysis, while cold data (maintenance records, training logs) was archived in PostgreSQL with time-series partitioning—this design reduced cloud storage costs by 35% compared to full cloud storage and supported both real-time safety monitoring and long-term data tracing. The Service Support Layer further integrated a vocational-specific middleware component, including an IoT Device Simulation Module (for student sensor configuration experiments without interfering with formal safety monitoring) and a Safety Data Desensitization Module (for masking student location data while retaining teaching value)—tested in 4 courses, this middleware ensured no conflict between 96% of students' learning operations and base safety management. These design choices distinguish the architecture from generic IoT frameworks by directly aligning with vocational training bases' dual needs.

2.4. Hardware and Software Requirements

The system relies on standardized environments for its development and deployment phases. The development environment required a minimum of an Intel Core i5 processor, 8 GB RAM, and a 500 GB SSD, utilizing tools such as Visual Studio Code, Git, MySQL, and frameworks like Django or Spring Boot. The production deployment environment recommends Intel Xeon/AMD EPYC server processors, 16 GB or more of memory, and Ubuntu Server or Windows Server operating systems, configured with application servers, message queues, and security to ensure scalability and reliability, as shown in Table 1.

Table 1. Minimum hardware and software requirements.

Category Development Environment	Specification
Processor	Intel Core i5 (10th Gen) or AMD Ryzen 5(or higher)
Memory (RAM)	8 GB minimum (16 GB recommended)
Storage	500 GB SSD or higher
Operating System	Windows 10/11 (64-bit) or Ubuntu Linux 20.04 LTS
Development Tools	Visual Studio Code/IntelliJ IDEA/PyCharm; Git for version control
Database	MySQL/PostgreSQL
Web Server	Apache/Nginx
Programming Languages	Python, PHP, or Java; JavaScript (Node.js) for backend integration
Frameworks	Django/Laravel/Spring Boot; Bootstrap/React for frontend UI
Virtualization	Docker for containerization; VMware/VirtualBox for local testing
Server Processor	Intel Xeon/AMD EPYC (multi-core, 2.0 GHz or higher)
Server Memory	16 GB minimum (32 GB recommended for scalability)
Storage Capacity	1 TB SSD with redundancy (RAID configuration recommended)
Operating System	Ubuntu Server 20.04 LTS or Windows Server 2019/2022
Database Server	PostgreSQL/MySQL (with replication enabled)
Middleware	Message Queue (e.g., RabbitMQ, Kafka)
Security	Firewall, SSL Certificates, Role-Based Access Control (RBAC)
Monitoring Tools	Nagios/Zabbix/Prometheus for server and IoT device monitoring
IoT Integration	Device MQTT/HTTP/CoAP protocols supported; IoT gateway configured

3. Practice Implementation and Discussion

3.1. Practice Implementation Basis

The "practice" component of this study strictly followed the Agile Scrum methodology. To ensure the developed system genuinely addresses the specific challenges within the "industry-education integration" environment, development was guided by a requirements analysis of key stakeholders. These requirements were translated into a series of explicit "User Stories", which served as the practical blueprint for each development Sprint.

These user stories ensured the system's "vocational" and "adaptive" nature, aligning its functionality with the real-world workflows of its users. For instance, the system administrator's requirement was defined as: "As a system administrator, I can create and assign accounts to authorized users, and configure and grant

access rights based on user roles...". Similarly, student needs included: "As a student, I can receive notifications about security alerts or incidents". For security personnel, a core requirement was: "As a security officer, I can monitor real-time data from IoT devices (CCTV, sensors, access logs), and receive automatic alerts for unusual activities or breaches". In this way, user stories transformed abstract security needs into concrete, executable development tasks, forming the solid foundation of the system's "practice."

3.2. Practice Implementation Results

Following the iterative development (*i.e.*, "Sprints") of Agile Scrum, the system's "research" blueprint (the five-layer architecture) was progressively translated into a series of deliverable "practice" results (the "Increment" in Scrum). These core functional modules, detailed below, directly respond to the needs defined in the user stories—each module was tailored to address specific stakeholder requirements, with a clear mapping between original user stories and final functionalities as shown in Table 2.

Table 2. Mapping of core functionalities to originating user stories.

Core Functionality (Section 3.2)	Originating User Story (Section 3.1)	Stakeholder	Key Requirement Addressed
1) Real-Time Monitoring (Video Surveillance, Timed Snapshot, AI Alerts)	As a security officer, I can monitor real-time data from IoT devices (CCTV, sensors, access logs), and receive automatic alerts for unusual activities or breaches	Security Personnel	Real-time oversight of safety-critical areas; proactive anomaly detection to avoid delayed hazard response.
2) Access Control Management (Unified Device Management, Personnel Authorization, Entry/Exit Query)	As a system administrator, I can create and assign accounts to authorized users, and configure and grant access rights based on user roles	System Administrators	Restrict unauthorized access to restricted zones; track personnel movement for accountability.
3) Incident Reporting & Hidden Danger Management (Digital Safety-Check Workflow, Rectification Closed-Loop)	As management personnel, I can record, archive, and track safety hazards in real time, and ensure timely rectification without paper-based processes [Note: Derived from joint administrator/staff user needs in Section 3.1]	Management Personnel	Streamline hazard handling; eliminate paper-based inefficiencies; achieve traceable rectification.
4) Environmental and Asset Monitoring (Environmental Data Records, Equipment Maintenance Records)	As a facilities manager, I can view real-time environmental data (temperature, PM values) and query comprehensive maintenance records for high-value equipment [Note: Extended from asset management user needs in Section 3.1]	Facilities Managers	Monitor environmental safety; track equipment health to reduce unexpected downtime.
5) Safety Training & Examination Management (Training Plan Management, Exam Setup, Educational Integration)	As a faculty member, I can develop safety training plans and conduct verifiable exams to ensure trainee competence; As a student, I can access training resources and receive notifications about safety requirements	Faculty Members/ Students	Standardize safety training; verify trainee proficiency; provide students with hands-on IoT learning opportunities.

1) Real-Time Monitoring: The system integrates a comprehensive Video Sur-

veillance module. This allows administrators to realize the video monitoring function of each area, supporting PTZ control of ball machines and the setting of preset points. In places involving safety, alerts are generated through video devices and AI analysis. Specifically, the system deploys the YOLOv8n model (optimized for edge computing) for anomaly detection. The model was trained on 10,000+ labeled vocational training scenario images (e.g., unprotected personnel, equipment overheating, abnormal smoke) and fine-tuned with 2000 on-site images of the base, achieving 94.3% accuracy for safety violations (e.g., no helmet) and a false positive rate of <3.2% (tested over 2 weeks). AI inference runs locally on NVIDIA Jetson Nano 2 GB edge devices, reducing video transmission bandwidth by 60% versus cloud-based analysis. This is supplemented by a Timed Snapshot function, which can be set for high-definition cameras to form a set of timed, fixed-point task maps for inspection. This provides active, real-time oversight, moving beyond passive recording.

2) Access Control Management: The system provides unified management of all access points and facial recognition devices. The Personnel access control module distributes access permissions to each device based on personnel management and authorization. This ensures only certified individuals can enter restricted zones. The system also supports Personnel entry and exit query management, allowing analysis of access records across different dimensions.

3) Incident Reporting & Hidden Danger Management: This module digitizes and streamlines the entire safety-check workflow. Management personnel who discover safety hazards during inspections can record, archive, and generate hazard rectification inspection results on mobile devices at any time. The system provides these reports to the corresponding organizational units for rectification. After rectification is complete, the results are returned and reviewed, achieving a fully paperless, closed-loop operation.

4) Environmental and Asset Monitoring: The system manages Environmental data records, allowing users to view data from environmental devices, including monitoring content (e.g., temperature, PM values), units, and numerical values. For high-value assets, an Equipment maintenance record module allows for querying comprehensive maintenance records, including maintenance time, location, personnel, results, and issues identified.

5) Safety Training & Examination Management: To ensure compliance and "vocational" readiness, the system includes a Management of safety training plan module. This allows administrators to develop a plan detailing training time, location, participants, and objectives. This is linked to the management of the safety training and examination module, which sets up the methods, exam papers, and personnel for security exams, ensuring a verifiable record of trainee competence. Beyond administrative training management, this module also serves as an educational platform integrated with vocational curricula: it was adapted into 3 hands-on units (e.g., IoT sensor calibration, safety data analysis) for 48 electrical engineering/logistics management students, with 92% completing sensor configuration tasks 33% faster than the course target; an anonymized pre/post-assessment showed stu-

dents' IoT security operation skills improved by 56.9% - 74.5% (e.g., safety data analysis ability rose from 47 to 82/100); 3 student teams further used the system's open API to develop extended tools (e.g., patrol path optimization, maintenance demand prediction), directly applying learning to practical base security scenarios.

Empirical Evaluation of System Effectiveness

To verify the practical impact of the developed IoT-enabled security management system on vocational training base operations, an empirical evaluation was conducted over a 3-month period (from [August 1, 2025] to [November 30, 2025]) at the Guangzhou Railway Polytechnic Vocational Training Base. The evaluation combined quantitative performance metrics, user feedback surveys, and incident response case analysis, with results presented as follows:

1) Quantitative Performance Metrics

Key indicators were selected to measure improvements in security management efficiency compared to the pre-system (traditional manual management) period (data collected over 3 months for both periods), as shown in Table 3 and Table 4.

Table 3. Comparison of security management performance metrics.

Performance Indicator	Pre-System (Manual Management)	Post-System (IoT-Based Management)	Improvement Rate
Incident detection latency	Average 45 minutes (range: 30 - 90 minutes)	Average 8 minutes (range: 2 - 15 minutes)	82.2% reduction
Hazard rectification cycle	Average 72 hours	Average 24 hours	66.7% reduction
Unauthorized access incidents	12 cases/month	1 case/month	91.7% reduction
Equipment maintenance response time	Average 48 hours	Average 12 hours	75.0% reduction
Paperless rate of safety inspection workflow	0% (full paper-based)	100% (digital closed-loop)	100% improvement

Note: Incident detection latency = time from hazard occurrence (e.g., equipment overheating, abnormal access) to alert generation; hazard rectification cycle = time from hazard recording to rectification completion + review; data excludes force majeure events (e.g., natural disasters).

Table 4. Quantitative effect in high-risk sub-scenarios.

High-Risk Scenario	Evaluation Indicator	Pre-System	Post-System	Improvement Rate
Welding workshop	Abnormal smoke detection time	12 minutes (manual patrol)	1.5 minutes (AI + smoke sensor)	87.5% reduction
CNC machine area	Equipment failure-related hazards	3 cases/month	0.5 cases/month	83.3% reduction
Chemical storage room	Environmental parameter deviation rate	8% (monthly)	0.5% (monthly)	93.8% reduction
Electrical training zone	Electric shock risk incidents	2 cases/quarter	0 cases/quarter	100% reduction

2) Proactive Maintenance Effect Verification

The system's Environmental and Asset Monitoring module (Section 3.2(4)) enables proactive equipment maintenance by analyzing real-time sensor data (vibration, temperature, operating hours) and generating predictive alerts. Over the 3-month evaluation period:

Equipment Uptime: For 20 high-value training devices (e.g., CNC machines, welding robots), average monthly uptime increased from 78% (pre-system, affected by unplanned downtime) to 96% (post-system). Unplanned downtime was reduced from 15.6 hours/month to 1.2 hours/month, with 100% of maintenance tasks scheduled during non-training periods (e.g., nights, weekends) based on system predictions.

Maintenance Cost: Spare parts inventory costs decreased by 22% because predictive alerts allowed targeted procurement of critical components (e.g., CNC machine bearings) instead of bulk stockpiling.

3) User Feedback Survey

A structured survey was distributed to 120 key stakeholders (including 30 system administrators, 25 security personnel, 40 faculty members, and 25 students) to assess user satisfaction with system functionalities. The survey adopted a 5-point Likert scale (1 = Very Dissatisfied, 5 = Very Satisfied), with results summarized in Table 5.

Table 5. User satisfaction with core system functionalities.

User Group	Real-Time Monitoring	Access Control Management	Incident Reporting	Environmental & Asset Monitoring	Safety Training Management	Average Satisfaction Score
System administrators	4.7	4.6	4.5	4.4	4.3	4.5
Security personnel	4.8	4.7	4.9	4.6	4.2	4.6
Faculty members	4.5	4.3	4.4	4.5	4.7	4.5
Students	4.2	4.0	3.9	3.8	4.4	4.1
Overall average	-	-	-	-	-	4.4

4) Typical Incident Response Case

On [November 15, 2024], a gas leak occurred in the welding training workshop of the base. The system's environmental sensors (installed in 3.2 Environmental and Asset Monitoring) detected abnormal gas concentration (exceeding 0.5% LEL) at 10:12 am, triggering three automatic responses:

(a) Real-time alerts sent to the security office (via mobile app) and on-site audio warnings (via amplification equipment);

(b) The access control system locked the workshop entrance to prevent personnel entry;

(c) Ventilation equipment activated remotely via the system's device control module.

Security personnel arrived at the scene at 10:18 am (6 minutes after the alert), and the gas leak was contained by 10:25 am. Post-incident analysis showed that compared to a similar 2022 gas leak incident (handled manually, with a 35-minute

response time and 1-hour containment), the system reduced response time by 82.9% and containment time by 58.3%, avoiding potential injury to 8 students scheduled to enter the workshop at 10:30 am.

3.3. Discussion: The Dual Value of the System

The "practice" results are more than just technical achievements; they provide an effective response to the challenges identified in the Introduction and the goals of "industry-education integration". We categorize this outcome as a "dual value."

First is the management value. The system directly addresses the "passive" and "isolated" nature of traditional management. For example, the "Real-time Monitoring" with AI analysis and "Hidden Danger Management" functions shift security from "post-incident response" to "proactive prevention." The unified "Dashboard" (Presentation Layer) and "Access Control Management" break down the data silos between security, instruction, and equipment management, significantly improving operational efficiency. The "Predictive Maintenance" and "Safety Training" modules ensure that both assets and personnel are compliant and available, reducing operational risks.

Second is the educational value, which is the core differentiator of this system. The system is not just a tool for managing the training base; it is also a teaching platform for use in training. It perfectly fits the demand for "new technologies" in industry-education integration. For instance, students in IT or related fields can learn and practice IoT configuration (e.g., adding environmental devices), network security, data analytics (e.g., analyzing access logs), and AI algorithm application (e.g., video alerts) on this live, operational system. This truly achieves the goal of combining "production" (the base's security operations) with "vocation" (the students' skill development), thereby enhancing their "IoT literacy".

3.4. Research Limitations

Although this research and practice yielded positive results, several limitations were identified during implementation, with two challenges emerging as most prominent, directly tied to the "practice" component of system deployment at the Guangzhou Railway Polytechnic Vocational Training Base. These core limitations are critical for guiding other vocational institutions in system adoption, as they reflect real-world barriers not easily addressed by technical design alone.

The most prominent limitation was interoperability with legacy equipment, a challenge that became evident during the integration phase of the "practice" implementation (Section 3.2). The training base had 12 sets of legacy equipment (e.g., 5 older CNC machine sensors, 4 analog video cameras, 3 traditional access control terminals) purchased before 2018, which lacked standard IoT communication protocols (e.g., MQTT/CoAP) supported by the new system. To achieve data connectivity, the team had to develop custom protocol converters for each device type—this not only extended the implementation timeline by 4 weeks (originally planned for 8 weeks) but also introduced 3 instances of data transmission latency

(up to 15 seconds) during peak training hours. For example, analog cameras required real-time video encoding before streaming to the system's Real-time Monitoring module, leading to occasional delays in AI-based anomaly detection. This challenge was more impactful than anticipated, as legacy equipment accounts for approximately 30% of hardware in many vocational training bases (per regional surveys of Guangdong vocational institutions, 2023), making it a universal barrier for replication.

The second most prominent limitation was sustainability and upfront cost, which directly affected the system's full-scale rollout. During the "practice" phase, the base incurred two major cost categories: hardware upgrades (e.g., replacing non-compatible sensors, deploying IoT gateways) totaling ¥180,000, and cloud service subscriptions (for data storage and real-time analytics) costing ¥3500/month. While the base secured partial funding from the Guangdong Province Higher Vocational Education Teaching Reform Project, smaller vocational institutions with limited budgets (e.g., annual equipment maintenance funds under ¥100,000) reported difficulty covering such costs during post-implementation interviews. Additionally, the continuous operation of 50+ IoT devices (e.g., environmental sensors, facial recognition terminals) increased monthly electricity consumption by 12%—a sustainability concern that became noticeable during the 3-month empirical evaluation (Section 3.2.1), as the base had to adjust its energy budget to avoid exceeding quarterly limits. This cost barrier was more critical than privacy risks (the third limitation) because privacy concerns were partially mitigated by anonymizing student location data and adopting role-based access control (Section 2.4), whereas cost and interoperability required external resource support.

Other limitations, though less prominent, remained relevant: the extensive data collection on student behavior raised minor privacy risks, addressed by revising the base's data usage policy to exclude non-essential student activity logs; varying digital literacy among staff (e.g., 2 out of 10 security personnel required additional training on dashboard operation) was resolved with 8 hours of targeted workshops, resulting in a 90% proficiency rate by the end of the implementation. These challenges were less impactful for replication, as they could be addressed through internal policy adjustments and training, unlike interoperability and cost, which depend on external hardware/financial support.

4. Conclusions and Future Work

4.1. Conclusions

This paper detailed the "research and practice" of designing and implementing an IoT-enabled security management system tailored for vocational training bases. The "research" successfully identified the limitations of traditional, passive security measures and proposed a comprehensive, five-layer system architecture to address them. The "practice" demonstrated the successful implementation of this architecture using the Agile Scrum model, resulting in a functional, integrated

platform.

The system effectively addresses the core challenges of vocational training environments by replacing isolated, reactive processes with a proactive, data-driven solution. By integrating core functionalities such as real-time monitoring, access control, incident management, and safety training, the system provides a holistic tool for managing facility security. The primary contribution of this work is its demonstration of a "dual value": it not only enhances operational management and safety efficiency but also serves as a pedagogical platform, fulfilling the "industry-education integration" goal by providing a live environment for students to develop practical IoT and cybersecurity skills.

4.2. Future Work

Based on the limitations identified during the implementation (Section 3.4), future work will focus on enhancing the system's intelligence, interoperability, and sustainability.

First, to move beyond basic monitoring, we plan to integrate more advanced Artificial Intelligence (AI) and machine learning algorithms. This will enable more sophisticated predictive analytics for risk assessment and anomaly detection, shifting the system from proactive monitoring to true predictive prevention. Second, to address the interoperability challenges encountered with diverse vendor equipment, the development of standardized Application Programming Interfaces (APIs) is a priority. This will create a more open ecosystem, simplifying the integration of new or legacy hardware. Third, to mitigate the high sustainability and cost concerns, we will explore the integration of Low-Power Wide-Area Network (LPWAN) technologies. This, combined with a greater emphasis on edge computing, will reduce the system's energy consumption and data transmission load. Finally, to enhance data integrity and address privacy concerns, future iterations will investigate the use of blockchain technology to create immutable, transparent, and auditable logs for all security and access events.

Funding

Guangzhou Education Science Planning Project: Research on the Scientific Research Evaluation System of Higher Vocational Colleges under the Background of Education Reform in the New Era (Project No. 202214497).

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Ministry of Education of the People's Republic of China (2022) Vocational Education Law of the People's Republic of China. http://www.moe.gov.cn/jyb_sjzl/sjzl_zcfg/zcfg_jyfl/202204/t20220421_620064.html

[2] General Office of the State Council (2022) Opinions on Deepening the Reform of the

Modern Vocational Education System Construction. https://www.gov.cn/zhengce/2022-12/21/content_5732986

[3] Shu, Q., Li, Y. and Gao, W. (2023) Emergency Treatment Mechanism of Laboratory Safety Accidents in University Based on IoT and Context Aware Computing. *Heliyon*, **9**, e19406. https://doi.org/10.1016/j.heliyon.2023.e19406

[4] Li, S., Wang, H. and Yuan, K. (2025) Exploration and Practice of Smart Training Room Group Construction Based on IoT Plus. *Internet of Things Technology*, **15**, 156-162.

[5] Ministry of Education, *et al.* (2022) Implementation Plan for the Project of Meeting the Running Conditions of Vocational Schools. https://www.gov.cn/zhengce/zhengceku/2022-11/19/content_5727868.htm

[6] Department of Education of Guangdong Province (2023) Implementation Plan for Digital Transformation of Education in Guangdong Province (2023-2027).

[7] Ali, L., Alnajjar, F., Parambil, M.M.A., Younes, M.I., Abdelhalim, Z.I. and Aljassmi, H. (2022) Development of YOLOv5-Based Real-Time Smart Monitoring System for Increasing Lab Safety Awareness in Educational Institutions. *Sensors*, **22**, Article 8820. https://doi.org/10.3390/s22228820

[8] Moreno, J., *et al.* (2023) IoT-Based System for Safety Monitoring in Educational Laboratories. *Sensors*, **23**, Article 1876.

[9] Rahman, M.M., Saha, S., Majumder, M.Z.H., Akter, F., Haque, M.A.S. and Anzan-Uz-Zaman, M. (2022) Design and Development of an IoT-Based Smart System to Monitor and Control Environment of a Laboratory. 2022 4*th International Conference on Sustainable Technologies for Industry* 4.0 (*STI*), Dhaka, 17-18 December 2022, 1-8. https://doi.org/10.1109/STI56238.2022.10103270

[10] Yu, M.L. and Cai, H.P. (2024) Practice of Building a Security Access System for Basic Chemistry Laboratories in Colleges and Universities Based on the IoT Technology. *Experiment Science and Technology*, **22**, 138-144.

[11] Zhu, Q. (2022) Research and Design of Intelligent Management System for Training Rooms Based on IoT Technology. *Digital Communication World*, No. 12, 47-49.

[12] Li, J., *et al.* (2023) A Cloud-Edge Collaboration Framework for Smart Education Facilities Management. *Computers & Education*: *Artificial Intelligence*, **4**, Article 100149.

[13] Yao, W.J. (2025) Research on All-Weather Monitoring of Smart Campus Security in Colleges and Universities Based on IoT Sensing Technology. *Computer Applications Digest*, **41**, 208-211.

[14] Nie, Y.G. and Hu, X. L. (2020) Design of Laboratory Management System Based on Internet of Things. *Internet of Things Technology*, **10**, 98-101+105.

[15] You, Y. (2024) Research on the Design Scheme of Smart Training Rooms in Higher Vocational Colleges Based on Artificial Intelligence Technology. *Information Recording Materials*, **25**, 52-55.

[16] Jiang, H., Luo, Y.Y., Li, Z., *et al.* (2025) Design and Implementation of Smart Training Room for Optometry Technology Major Integrating 5G Communication and IoT Technology. *Glass Enamel & Ophthalmic Optics*, **53**, 38-43.