Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 11, No. 3, 2025

Research on Smart Campus System Architecture Design and Data Security Protection Strategy

Qijun Ni *, Yinghao Zeng

Hangzhou Hanghui Digital Technology Co., Ltd., Hangzhou Zhejiang, 310000, China

* **Corresponding author**: Qijun Ni (Email: 18969924808@163.com)

Abstract: Digital transformation has become a key aspect of the education sector's evolution, coinciding with the rapid advancements in information technology. The construction of smart campuses has become a key aspect of modern educational informatization, playing a significant role in enhancing education quality and advancing educational modernization. This paper focuses on the cutting-edge theme of the system architecture design of smart campuses and data security protection strategies. It conducts an in-depth and systematic analysis of the overall hierarchical architecture of the smart campus system. In response to the numerous complex challenges and potential risks currently faced by data security, a series of data security protection solutions that integrate advanced technologies and scientific management concepts are innovatively proposed. The aim is to build a solid data security defense line for the stable operation and sustainable development of smart campuses.

Keywords: Smart Campus; System Architecture; Data Security.

1. Introduction

In recent years, with the rapid advancement of cutting-edge information technologies such as the Internet of Things (IoT) and artificial intelligence (AI), the education sector has entered a new era of digital transformation. In 2019, the Central Committee of the Communist Party of China and the State Council issued *China Education Modernization 2035*, which called for accelerating educational reforms in the digital age, building smart campuses, and integrating intelligent teaching, management, and service platforms [1]. Consequently, the concept of the smart campus has emerged as a key carrier of educational informatization.

However, the rapid development of smart campuses is accompanied by numerous challenges. As system complexity increases and data volume expands, designing an efficient system architecture and ensuring data security have become critical issues in smart campus construction. A well-structured, flexible, and efficient system architecture is the foundation for the stable operation of a smart campus [2]. Deficiencies in architectural design may lead to slow system response times and poor coordination among functional modules, severely disrupting campus operations. Additionally, smart campuses store vast amounts of sensitive data, including personal information of faculty and students, educational resources, and scientific research results. Any data breach or tampering could compromise individual privacy and potentially damage the institution's reputation and development.

Therefore, conducting in-depth research on smart campus system architecture design and data security protection strategies is of great practical significance, aiming to promote the sustainable and healthy development of smart campuses.

2. Smart Campus System Architecture Design

The smart campus system architecture is typically designed in a hierarchical structure, encompassing the perception layer, network layer, platform layer, and application layer [3], as shown in Figure 1. These layers collaborate to form an intelligent campus ecosystem.

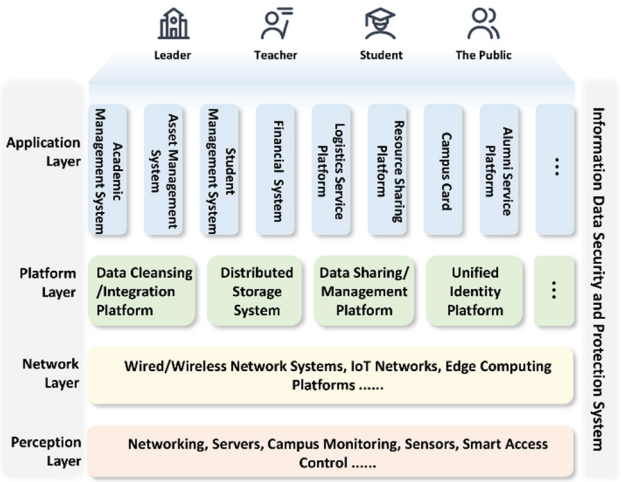

Figure 1. Smart Campus System Architecture

2.1. Perception Layer

The perception layer serves as the foundational layer of the smart campus system architecture, functioning as the "nerve endings" of the campus. It encompasses various sensors, cameras, smart terminals, and other devices. Its primary role is to collect multi-source data in real time, including campus environment conditions, personnel activities, and device operations [4]. By converting information from the physical world into digital signals that can be processed by computers, the perception layer provides essential support for subsequent data processing and application development.

2.2. Network Layer

The network layer serves as the data transmission layer of the smart campus, functioning like a "nervous system." It is responsible for securely and efficiently transmitting the vast amount of data collected by the perception layer to the platform layer while also relaying processed instructions and data from the platform layer to the perception and application layers [5]. This layer must ensure stable and reliable data

transmission, accommodating the diverse requirements of different data types, such as real-time video streams, sensor data, and user interaction data.

2.3. Platform Layer

The platform layer acts as the "brain" of the smart campus system. Leveraging distributed computing and storage technologies, it performs data cleansing, storage, and analysis, serving as the core support for intelligent decision-making and efficient campus management. The database built on big data technology possesses robust data integration capabilities, enabling the centralized aggregation of heterogeneous data from multiple departments, including academic affairs, student management, finance, and logistics systems. Through preprocessing steps such as data cleansing and transformation, the platform layer ensures data accuracy and consistency [6].

2.4. Application Layer

The application layer is the direct user interface for faculty, students, and administrators, positioned at the top of the system architecture. Encompassing a wide range of applications in teaching, management, and daily life, it is designed to provide user-centric, convenient, efficient, and personalized services, enabling the intelligent and digital transformation of campus operations [7]. In the teaching domain, smart teaching systems integrate various functional modules such as online course platforms and intelligent tutoring systems. In terms of management, the system includes academic affairs management, student administration, and research management. For campus services, continuously upgraded systems such as campus card services and dormitory management enhance daily operations.

3. Challenges in Smart Campus Data Security

Table 1. Challenges in Smart Campus Data Security

Challenges Domain	Specific Challenge	Main Issues
Technical	Network Security Threats	Susceptibility to hacker attacks, database intrusions, and sensitive data breaches.
Technical	Data Encryption and Management	Large data volumes increase encryption complexity; inconsistent data standards across departments hinder data classification and grading; maintaining encryption consistency and effectiveness during data transmission is challenging.
Management	Internal Personnel Misconduct	Unauthorized access, misuse, or leakage of data.
Management	Weak Security Awareness	Use of simple passwords by faculty and students, clicking suspicious links, and downloading unknown files.
Challenges Domain	**Specific Challenge**	**Main Issues**
Management	Staff Turnover	Improper data handover and access control during personnel transitions.

Data security is a critical component of the overall smart campus architecture. However, smart campus data security still faces numerous complex and severe challenges (Table 1), posing risks to the privacy and legal rights of faculty and students while potentially impacting the normal operation of schools, teaching order, and educational equity.

3.1. Data Leakage Risks

As the informatization level of smart campuses increases, their network systems have become prime targets for cyberattacks. Hackers may exploit system vulnerabilities to infiltrate smart campus servers and databases, stealing sensitive data [8]. Additionally, data leakage risks may arise due to internal personnel negligence. A lack of security awareness may lead individuals to connect mobile devices to unsecured public networks, increasing the risk of malware infiltration and the subsequent exposure of sensitive campus data.

3.2. Data Tampering Threats

Certain critical business data in smart campuses, such as student grades, teaching plans, and financial records, are essential for the institution's normal operation and educational order. Malicious attackers may alter these data for various purposes, such as modifying student grades for personal gain or disrupting academic schedules by tampering with course arrangements [9]. Such actions could severely undermine the fairness and integrity of the education system.

3.3. Data Misuse Issues

Smart campuses accumulate vast amounts of personal data from students and faculty, including interests, consumption habits, and learning preferences. Some malicious actors may collude with internal personnel or use illicit means to obtain this data for commercial marketing purposes, severely violating students' privacy rights.

4. Smart Campus Data Security Protection Strategies

4.1. Technical Measures

4.1.1. Strengthening Data Encryption Technologies

In the smart campus data security protection system, transmission encryption is crucial for ensuring data confidentiality during network transmission and effectively mitigating the risk of tampering. Currently, SSL/TLS protocols are widely used [10]. After encryption, attackers cannot obtain the decryption key, making it difficult to decipher encrypted data, thereby ensuring secure data transmission and strengthening the security of smart campus network interactions. For remote access to the smart campus system by internal personnel, Virtual Private Network (VPN) technology is employed [11]. VPN establishes a secure private tunnel over public networks, encrypting and encapsulating transmitted data to achieve a secure remote connection with the campus network. Additionally, stored data can be encrypted using the Advanced Encryption Standard (AES) algorithm [12].

4.1.2. Optimizing Access Control Mechanisms

Authentication serves as the first line of defense, and its accuracy and reliability directly affect the security of the entire system. Traditional username-password authentication methods are insufficient in complex network environments, making them vulnerable to password cracking and identity fraud. As a result, multi-factor authentication has become an inevitable trend [11]. This approach combines SMS verification codes, dynamic passwords, and biometric

authentication (such as fingerprint and facial recognition) with conventional username-password authentication. Biometric authentication, based on an individual's unique physiological characteristics, is nearly impossible to forge, enhancing both the security and convenience of identity verification [12].

4.1.3. Upgrading Network Security Protection Systems

Firewalls serve as the first layer of defense in smart campus network security, playing a vital role in blocking unauthorized external access and ensuring the security of campus network boundaries. Deploying high-performance firewalls at the campus network perimeter is essential [13]. These firewalls enforce carefully designed security policies to filter and monitor incoming and outgoing traffic. They inspect key information in data packets to prevent unauthorized external access while monitoring outbound traffic to prevent unauthorized data leaks. This also helps prevent infected internal hosts from communicating with external command-and-control servers, maintaining the integrity and reputation of the campus network.

4.2. Managerial Measures

4.2.1. Establishing Security Management Policies

A comprehensive security management policy should cover the entire lifecycle of data collection, storage, usage, and disposal. Clearly defined data classification and grading rules must be established, specifying access permissions and data-sharing boundaries. For instance, highly sensitive data such as student personal information, academic records, and medical files should only be accessible to authorized personnel. Additionally, data-sharing agreements should be included to prevent third-party institutions from misusing shared data.

4.2.2. Implementing Data Backup and Recovery Strategies

Data backup is a critical measure for preventing data loss or system failures [14]. Core sensitive data, such as student academic records, faculty personnel files, and academic administration data, should be backed up daily using specialized backup software and stored in dedicated storage devices. To ensure backup reliability, a cyclic backup strategy can be adopted, maintaining multiple backup versions from different time points. This allows for rapid restoration to the most recent valid state in the event of data corruption or loss, minimizing disruptions and potential damage.

5. Conclusion and Future Outlook

This study systematically examines the design of smart campus system architecture and data security protection strategies. The system architecture is built using a layered design, forming a comprehensive smart campus framework. In terms of data security, targeted technical and managerial measures are proposed to address potential risks, ensuring system stability and data integrity.

Looking ahead, smart campuses will integrate deeply with emerging technologies, presenting vast development opportunities. Future research will focus on multi-technology integration and innovative applications, strengthening data security and privacy protection, and enhancing user experience. Continuous exploration of new possibilities in education informatization and intelligent systems will contribute to cultivating innovative talents and driving high-quality educational development.

References

[1] CPC Central Committee and State Council issue China Education Modernisation 2035 [N]. People's Daily,2019-02-24(001).

[2] Zhu X H. Research on the construction of smart campus under the background of 5G [D]. Heilongjiang University,2021.

[3] Liu S H, Zhu D N, Gao Z H, et al. The application of face recognition technology in the construction of smart campus [J]. Computer Knowledge and Technology, 2024, 20(31):21-23+30.

[4] Xu X, et al. Research on Key Technologies of Smart Campus Teaching Platform Based on 5G Network [J].IEEE Access, 2019, (7):20664-20675.

[5] Wang X. Three-dimensional Construction and Application Study on "Internet+ Smart Campus" [J]. China Educational Technology, 2016,(10):107-111.

[6] Che H, Wang S, Yang B, et al. Top-level Architecture Design of Smart CampusBased on Internet of Things [J]. Technology of IoT & AI, 2021, 4(01):39-44.

[7] Li L Q. Thesis/Dissertation Guide for Postgraduatesof XIDIAN UNIVERSITY [D]. Xidian University, 2017.

[8] Wang J P, Teng R H. Research on network security prevention countermeasures for smart colleges and universities under the background of informationisation [J]. Network Security Technology & Application, 2024, 12:82-83.

[9] Zhao H J. Research on the Application of Internet of Things technologyin Smart Campuses of Universities [J]. Digital Communication World, 2024, 5:96-98.

[10] Zhang B, Fan J W, Li Z G, et al. Network security protection under smart campus [J]. Network Security Technology & Application, 2022, 4:93-95.

[11] Gan Y J, Liang S L. Application of Data Governance in the Construction of Smart Campus [J]. Sport Science and Technology, 2024, 45(06):176-178+180.

[12] Pang F. Resarch on th Application of Smart Campus Password Service Platform Under the Background of Digital Transfomation [J]. Heilongjiang Science, 2024, 15(23):99-101.

[13] Li X. Research on the Application of Network Security Optimization on Campus [J]. Journal of Shanxi Datong University(Natural Science), 2020, 36(02):32-34.

[14] Zhang L. Optimization Measures of College Education Managementin the Big Data Era [J]. The Theory and Practice of Innovation and Entrepreneurship, 2023, 6(08):59-61.