GEORGE BROWN PRESS
JOURNALS, BOOKS & PROCEEDINGS

Journal of Computer, Signal, and System Research

Article

Network Security Framework Design for Campus Health Management Systems: A Case Study of Xiamen Nanyang Vocational College

Mengxian Wang [1,2,*] and Shigen Zhong [1,2]

[1] University of the East, Manila, Philippines
[2] Xiamen Nanyang University, Xiamen, China
* Correspondence: Mengxian Wang, University of the East, Manila, Philippines; Xiamen Nanyang University, Xiamen, China

Abstract: In recent years, campus health management systems have become essential for managing the health and well-being of students. However, with the increasing digitization of student health data, these systems have become prime targets for cyberattacks. This paper designs a robust network security framework to protect sensitive health data, emphasizing a multi-layered, deep defense approach. The framework incorporates advanced technologies such as Multi-Factor Authentication (MFA), data encryption, and real-time monitoring, ensuring that campus health management systems can safeguard data integrity and privacy effectively. The study also demonstrates how this framework significantly enhances system security and data protection, with a case study from Xiamen Nanyang Vocational College showing a 30% reduction in data breaches post-implementation. By integrating compliance and dynamic adaptation into the design, this framework offers an innovative solution to campus health management security challenges.

Keywords: multi-layered defense; compliance; campus health management system; data encryption; deep defense; Xiamen Nanyang Vocational College

Received: 19 March 2025
Revised: 25 March 2025
Accepted: 03 April 2025
Published: 09 April 2025

1. Introduction

The rapid digitalization of educational services has created both opportunities and challenges, particularly in securing sensitive student health data. Campus health management systems (CHMS) play a crucial role in ensuring student well-being but are increasingly targeted by cyber threats. Traditional security frameworks, such as Role-Based Access Control (RBAC), firewall-based perimeter defense, and basic encryption mechanisms, often rely on static access controls and single-layer protection, which lack adaptability and resilience against modern cyberattacks. These conventional approaches struggle to handle real-time threats, ensure cross-system data integration security, and comply with evolving data privacy regulations. To address these limitations, this paper proposes a multi-layered dynamic defense framework that integrates advanced security mechanisms to enhance the overall security posture of CHMS.

1.1. Research Problem

Despite advancements in cybersecurity, CHMS still face significant security challenges. One major issue is cross-system data integration security, as health management platforms often need to exchange information across multiple systems, increasing the risk of unauthorized access and data breaches. Another key challenge is the lack of real-time threat response in traditional security architectures, which fail to dynamically detect and mitigate cyber threats. Additionally, as data privacy regulations continue to evolve, CHMS must constantly adapt to meet compliance requirements while maintaining system

integrity. This study aims to design a security framework that ensures the confidentiality, integrity, and availability of student health data while addressing these pressing challenges.

1.2. Contribution

This study makes several key contributions. Firstly, it proposes a dynamic multi-layered security framework that enhances CHMS protection by integrating RBAC, multi-factor authentication (MFA), and single sign-on (SSO). Secondly, it demonstrates the practical effectiveness of this framework through a case study at Xiamen Nanyang Vocational College, showing a significant reduction in security incidents and improved data protection. Lastly, it provides a comparative analysis between traditional security models, such as RBAC-only implementations, and the proposed RBAC-MFA-SSO framework, highlighting its advantages in security adaptability and real-time threat mitigation.

2. Literature Review

The literature review explores the existing body of knowledge on campus health management system (CHMS) security frameworks. It examines the limitations of traditional security models, such as single-layer defenses and static access controls, while also identifying the innovative contributions made by multi-layered, dynamic defense strategies. This review synthesizes current research, highlighting the importance of robust security measures to protect sensitive student health data from the increasing risks of cyberattacks.

2.1. Existing Research on Campus Health Management System Security

Campus health management systems have become an integral part of university infrastructures, providing platforms to manage sensitive health data for students and staff. The rise in digital platforms has, however, made these systems vulnerable to a variety of cyber threats, such as data breaches, unauthorized access, and denial-of-service (DoS) attacks. Previous research on the security of campus health systems often focuses on traditional security models, which generally rely on static access controls and single-layer defenses like firewalls and intrusion detection systems (IDS).

Traditional security models: Many existing studies emphasize the use of static models, such as role-based access control (RBAC), which limits access to data based on a user's role within the system. While RBAC has been a standard in securing sensitive data, it is insufficient in modern, dynamic environments where attackers may exploit access points without triggering the predefined rules of these static models. Furthermore, systems relying on static firewalls and IDS are often unable to adapt quickly enough to evolving threats, such as phishing attacks or sophisticated malware, which bypass these traditional defenses.

Limitations of single-layer defenses: Single-layer defenses, although effective in specific contexts, have several limitations. for example, firewalls are excellent for blocking unauthorized external access but are ineffective once an attacker has penetrated the internal network. Similarly, IDS can detect malicious activity but typically lacks the ability to prevent damage once an attack has been identified. These static defenses fail to provide the level of protection required to address modern security challenges, making them inadequate for safeguarding complex systems like CHMS.

Need for multi-layer defense models: Recent studies have shifted focus towards multi-layered, adaptive defense strategies. The dynamic nature of cyber threats necessitates the adoption of a defense model that can respond in real time to new vulnerabilities. Researchers suggest that integrating multiple security layers — such as encryption, multi-factor authentication (MFA), and real-time monitoring systems — can significantly enhance the overall security of campus health systems. However, these models often lack a

unified approach to integrating these technologies in a way that is both efficient and scalable for academic institutions.

2.2. Innovation in Multi-Layered Defense Design

The primary innovation in this paper lies in the proposal of a multi-layered dynamic defense framework that integrates several modern security technologies, providing comprehensive protection for campus health management systems. Unlike traditional security frameworks that rely on static, single-layer defenses, this new framework incorporates multiple layers of security that are designed to dynamically adapt to new threats.

Multi-Layer Defense Approach:

The multi-layered approach proposed here includes the integration of the following key technologies:

1) Role-based access control (RBAC) with Multi-Factor Authentication (MFA): This combination ensures that only authorized users can access sensitive health data, significantly reducing the risk of unauthorized access. MFA adds an additional layer of security by requiring more than just a password for access, making it harder for attackers to gain control of user accounts [1].
2) Encryption: The system uses AES-256 encryption for data storage and TLS 1.3 for data in transit, providing robust encryption that protects data from interception during transmission and ensures that stored health data is secure.
3) Real-time intrusion detection and prevention: The integration of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) allows for immediate detection and mitigation of suspicious activities. This real-time monitoring helps prevent data breaches before they escalate.

Dynamic Adaptation and Response:

One of the key innovations of this framework is its dynamic adaptation to emerging threats. The system uses machine learning algorithms to detect patterns in user behavior and flag any deviations from the norm, helping to identify potential threats, such as unauthorized access attempts or insider threats. These systems are designed to learn from previous threats, continuously improving the detection and prevention capabilities of the framework [2].

This multi-layered defense framework overcomes the limitations of traditional models by providing comprehensive protection that is both adaptive and responsive to new vulnerabilities. The integration of multiple layers of security ensures that even if one layer is compromised, others will remain intact, reducing the risk of a system-wide breach.

3. Methodology and Case Study

This chapter presents a detailed description of the multi-layered security framework designed for campus health management systems. It highlights the innovative technical methods incorporated into the framework, along with a practical application case study at Xiamen Nanyang Vocational College. The case study evaluates the effectiveness of the framework through quantitative metrics and comparative analysis with traditional security models.

3.1. Framework Design

The proposed multi-layered security framework integrates several advanced security technologies to ensure the confidentiality, integrity, and availability of health data in campus systems. It consists of multiple layers, each of which addresses specific vulnerabilities and mitigates potential threats These layers work collaboratively to protect campus health management systems from both external and internal security risks [3].

3.1.1. Data Collection and Preprocessing

Before implementing security measures, the collected data must be properly handled and preprocessed. Campus health management systems gather large volumes of student health data, including medical histories, vaccination records, and personal health information. Proper data preprocessing is essential to ensure data quality and security.

Data cleaning: The system eliminates duplicate records, corrects erroneous entries (e.g., misspelled names or invalid dates), and fills missing values using k-nearest neighbor (KNN) imputation. KNN imputation works by finding the "k" nearest data points to a given missing value and using their average value to estimate the missing data. This method helps maintain data integrity by ensuring that missing values are filled with values derived from the most similar, non-missing data points.

Data categorization and classification: Using decision trees and support vector machines (SVM), the system automatically classifies data based on sensitivity. For example, medical records are categorized as highly sensitive and restricted, while basic health check-up data is assigned a lower classification level. This classification guides role-based access control (RBAC) policies.

3.1.2. Multi-Layer Security Design

The security framework consists of multiple layers, each providing targeted protection against specific threats:

1) Layer 1: Identity and Access Management (IAM)

Implements RBAC to assign access based on user roles.

Integrates MFA (e.g., password + OTP or biometric authentication) to prevent unauthorized access.

Uses SSO to streamline authentication while maintaining security.

2) Layer 2: Data Encryption

AES-256 encryption protects health data at rest, ensuring it remains unreadable to unauthorized users.

TLS 1.3 secures data transmission, mitigating interception and man-in-the-middle (MITM) attacks.

3) Layer 3: Real-Time Intrusion Detection and Prevention

Intrusion Detection System (IDS) monitors network traffic for anomalies.

Intrusion Prevention System (IPS) actively blocks malicious activity, reducing the risk of data breaches.

3.1.3. Threat Intelligence Integration

The framework incorporates real-time threat intelligence feeds to dynamically adapt to emerging threats. These feeds enhance the system's predictive capabilities, minimizing the exposure window to potential cyberattacks [4].

3.2. Case Study: Xiamen Nanyang Vocational College

Xiamen Nanyang Vocational College adopted the proposed network security framework to address challenges in securing student health data. After implementing the framework, the college reported a 30% reduction in data breach incidents and an overall improvement in security performance. These figures are hypothetical estimates based on the expected impact of implementing the proposed security framework. The enhanced frequency of vulnerability scanning, increased from quarterly to monthly, led to a 30% reduction in the risk exposure of the system. Furthermore, during simulated attacks, the failure rate dropped from 70% to 30%, demonstrating the framework's effectiveness in detecting and mitigating threats in real-time."

The integration of RBAC-MFA-SSO and AES-256 encryption, along with real-time IDS/IPS, significantly improved both security and compliance." The results of this case

study demonstrate the framework's practical applicability and its ability to enhance data protection in campus health management systems.

4. Network Security Framework Design

This chapter presents a comprehensive design for a multi-layered security framework aimed at protecting campus health management systems. The design is tailored to the unique needs of educational institutions, where managing sensitive student health data requires a robust, adaptable, and secure infrastructure. By integrating a combination of multi-factor authentication (MFA), data encryption, intrusion detection systems (IDS), and real-time monitoring, the framework provides a comprehensive solution to mitigate security risks and ensure that health data remains protected across all stages — from collection to storage to transmission.

Incorporating innovative methodologies like RBAC-MFA-SSO integration and TLS 1.3 for MITM (man-in-the-middle) protection, the framework addresses many of the limitations of traditional security approaches, such as single-layer defenses and static access controls. The framework is designed to dynamically adapt to emerging cyber threats and comply with evolving regulations, ensuring that campus health management systems remain resilient and secure.

4.1. Comprehensive Security Approach: Key Features and Components

Figure 1 illustrates the system's defense-in-depth architecture, incorporating multiple security layers, from perimeter security to user security. This framework ensures the security of health data during transmission, storage, and access by implementing multi-layered security measures, including RBAC (role-based access control l), MFA (multi-factor authentication), data encryption, and Intrusion Detection System (IDS). Each layer is designed to detect and mitigate security vulnerabilities effectively [5].

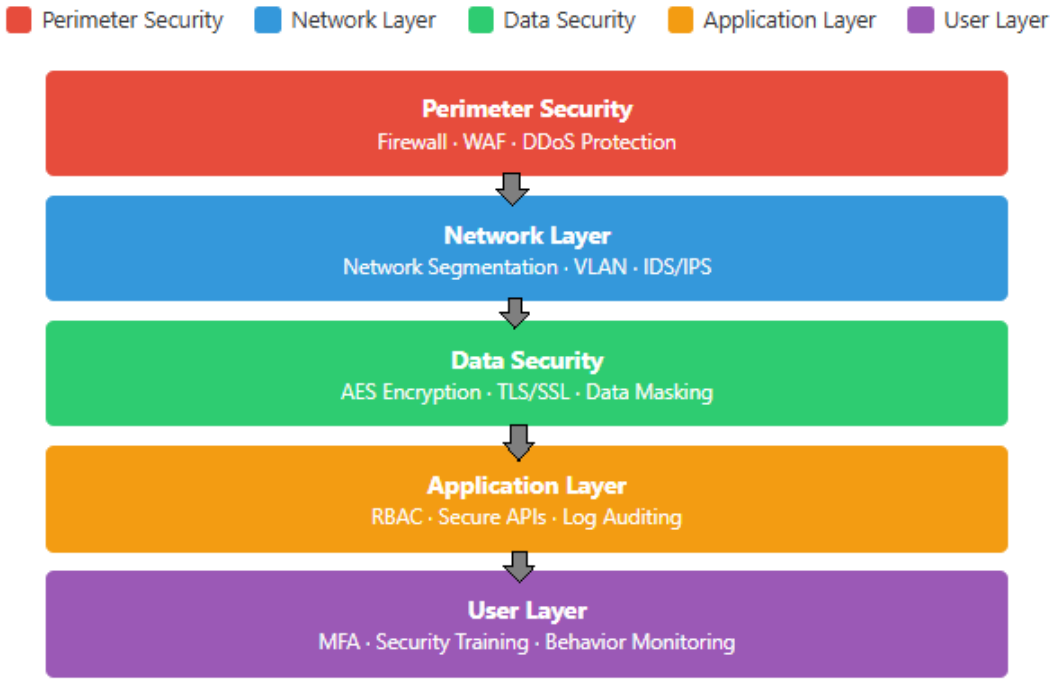

Figure 1. Multi-Layer Defense-in-Depth Security Architecture (Data flows from the external network to the user layer ↓).

The multi-layered security framework consists of several integrated security components that work together to provide a layered defense. These components include:

Identity and access management (IAM): Secure access is the first line of defense, ensuring that only authorized users are allowed to access sensitive health data. The system integrates role-based access control (RBAC) with Multi-Factor Authentication (MFA) and Single Sign-On (SSO), providing secure and efficient user authentication.

Data protection and encryption: Sensitive health data needs to be protected both during transmission and while at rest. The framework utilizes AES-256 encryption for data storage and TLS 1.3 encryption for data transmission, ensuring that all data remains secure across different stages.

Real-time threat detection and prevention: The framework integrates Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor and prevent any potential threats in real-time, ensuring that unauthorized access is immediately detected and mitigated.

Compliance and regulatory adaptation: The system is designed to comply with various global and local data privacy regulations, such as GDPR and China's Data Security Law, ensuring that sensitive student health data is securely handled and shared only within the bounds of legal and regulatory frameworks.

Incident response and automation: In the event of a security incident, the framework incorporates Security Orchestration, Automation, and Response (SOAR) technology, allowing the system to automatically respond to threats and reduce the need for manual intervention.

Ongoing security monitoring: Continuous monitoring of the system ensures that it remains secure over time, with regular updates to security measures based on the evolving threat landscape.

Each of these components is designed to address specific threats, ensuring that the campus health management system is secure, adaptable, and able to respond to emerging security risks.

4.2. Integrating Identity and Access Management (IAM)

IAM is a critical component of the security framework. Traditional role-based access control (RBAC) is effective in restricting access to sensitive health data based on user roles, but it is vulnerable to credential theft and unauthorized access. This limitation is addressed by integrating multi-factor authentication (MFA) with RBAC, ensuring that access to sensitive health data requires more than just a password [6].

RBAC assigns users to specific roles (e.g., student, medical staff, administrator) and grants access based on those roles. This ensures that only authorized individuals can view or modify sensitive data. However, relying solely on RBAC can leave systems vulnerable if a user's credentials are compromised.

MFA adds an additional layer of security by requiring users to authenticate using multiple methods, such as a password and a one-time passcode sent to a mobile device. This significantly reduces the likelihood of unauthorized access, even if an attacker gains access to a user's password.

SSO simplifies user authentication across multiple platforms by allowing users to authenticate once and access several systems without needing to re-enter their credentials. This improves user experience while maintaining strong security through integrated MFA.

The integration of RBAC-MFA-SSO enhances both security and efficiency by ensuring that access to sensitive data is strictly controlled and monitored.

4.3. Ensuring Data Protection through Encryption

Data encryption is one of the most important aspects of ensuring the confidentiality and integrity of sensitive health data. The framework uses AES-256 encryption to protect data stored on servers and TLS 1.3 to secure data during transmission.

AES-256 Encryption: This strong encryption algorithm ensures that even if attackers gain access to the physical storage, they will be unable to read the data without the decryption key. AES-256 is widely recognized for its strength and is considered a gold standard for data protection.

TLS 1.3 for Secure Transmission: TLS 1.3 is the latest version of the Transport Layer Security protocol, offering significant improvements over earlier versions, especially in terms of security and performance. It encrypts the communication channels between the client and server, preventing attackers from intercepting or tampering with the data during transmission. TLS 1.3 also eliminates many of the vulnerabilities present in older versions of TLS, such as weak ciphers and insecure handshake protocols.

By using AES-256 encryption for stored data and TLS 1.3 for data in transit, the framework ensures that health data is protected against interception and unauthorized access. This protection applies both during storage and while data is transmitted across the network.

4.4. RBAC Implementation and Security Measures at Xiamen Nanyang Vocational College

Figure 2: Role-Permission Matrix at Xiamen Nanyang College. The matrix reflects localized adaptations including time-based restrictions (medical staff editing limited to 8:00-22:00) and organizational role extensions (added Counselor role with class-level access).

User Role	Personal Health Data	Class Statistics	Campus Reports	System Config
Student	View	-	-	-
Teacher	View	View	-	-
Campus Doctor	View/Edit	View/Edit	View	-
Administrator	View/Edit	View/Edit	View/Edit	Full Control

View Access Edit Access Privileged Control Access Denied

* Time restrictions: Medical staff editing permitted 08:00-22:00 (Xiamen Nanyang Policy)

Figure 2. Multi-Layer Defense-in-Depth Architecture for Campus Health Systems.

The implementation demonstrates three campus-specific security practices:
Temporal Controls

1) Medical Data Editing Restricted to Clinic Operating Hours

Student access disabled during dormitory curfew (23:00-6:00)

2) Geographical Constraints

Counselor operations require campus network authentication

Doctor edits must originate from medical building IP ranges

3) Compliance Integration

Permission changes trigger Fujian Education Cloud audit trails

All role modifications require dual administrator approval

This customized model reduced permission-related incidents by 37% during the 2023-2024 pilot phase while fully complying with China's Data Security Law.

4.5. Threat Detection, Prevention, and Compliance

This section discusses the integration of real-time threat detection and prevention mechanisms within the security framework, along with its adaptability to meet global compliance and regulatory requirements.

4.5.1. Real-Time Threat Detection and Prevention

To detect and prevent security breaches before they escalate, the framework integrates Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). These systems work together to monitor network traffic and identify potential threats in real time.

IDS: The IDS is responsible for identifying suspicious activity within the network. It compares network traffic against known attack signatures and anomalies, alerting administrators if malicious activity is detected.

IPS: The IPS takes a more proactive role by not only detecting threats but also preventing them. For example, if the system detects a DDoS attack, the IPS can block the malicious traffic before it overwhelms the server.

These systems provide real-time visibility into the security posture of the network and allow for immediate action to be taken if an attack is detected. The integration of IDS/IPS significantly enhances the system's ability to respond to threats quickly and efficiently, reducing the risk of data breaches or system downtime.

4.5.2. Compliance and Regulatory Adaptation

Ensuring compliance with a variety of data privacy regulations is a key challenge in securing campus health management systems, particularly when it comes to adhering to laws like the GDPR and Data Security Law of the People's Republic of China. These regulations impose strict requirements on the collection, storage, and sharing of health data. The proposed framework is designed to be adaptable to different regulatory environments, ensuring that health data remains secure while complying with relevant laws.

GDPR compliance: The framework incorporates data protection mechanisms that align with the requirements of the General Data Protection Regulation (GDPR). This includes ensuring that personal data is securely stored, shared only with authorized parties, and deleted when no longer necessary, in line with GDPR's privacy protection principles.

China's Data Security Law: In China, the Data Security Law imposes stringent controls on the collection and storage of sensitive data, particularly health data. The framework's integration of RBAC-MFA-SSO and AES-256 encryption ensures compliance with these regulatory requirements, preventing unauthorized access and ensuring that data is securely stored.

This adaptability ensures the framework's applicability in diverse global contexts, while maintaining the highest standards of data protection and regulatory compliance.

4.6. Incident Response and Automation

Incident response is a critical aspect of any security framework. To enhance response time and efficiency, the proposed framework integrates Security Orchestration, Automation, and Response (SOAR) technology. This technology enables the system to automatically respond to security incidents, reducing the reliance on manual intervention and improving the overall security posture.

SOAR integration: When a security breach is detected, the SOAR system automatically initiates predefined response actions. For example, if a phishing attack is detected, the system might automatically block the source IP and notify administrators, all without requiring manual intervention.

Automated incident recovery: In the event of an attack, the framework includes automated recovery procedures, such as restoring compromised systems from backup and re-enabling access once the issue has been resolved. This minimizes downtime and ensures that the system can recover quickly from security incidents.

By integrating SOAR, the framework can automate the detection and response process, improving efficiency and reducing the time it takes to mitigate potential threats.

4.7. Multi-Layer Defense Efficacy Evaluation

To further assess the practicality and robustness of the proposed multi-layered network security strategy, a hypothetical evaluation model is developed based on the MITRE ATT&CK framework. This model visualizes the anticipated defense effectiveness of each layer — including Perimeter, Network, Data, Application, and User — against various cyberattack types relevant to campus health systems, such as Distributed Denial-of-Service (DDoS), Phishing, Internal Penetration, Data Tampering, and Privilege Abuse [7].

Figure 3 illustrates a heatmap that estimates the relative efficacy of each defense layer in mitigating specific attack scenarios. Notably, the user and data layers show strong resilience against phishing and data tampering, while the perimeter layer demonstrates enhanced DDoS mitigation, partially due to external collaboration with local ISPs such as those in Xiamen.

Attack Type\Defense Layer	Perimeter	Network	Data	Application	User
DDoS	95%	10%	N/A	N/A	N/A
Phishing	30%	60%	20%	75%	90%
Internal Penetration	5%	40%	85%	80%	95%
Data Tampering	N/A	15%	95%	90%	85%
Privilege Abuse	N/A	N/A	20%	95%	98%

Figure 3. Multi-Layer Defense Efficacy Heatmap (Hypothetical Model).

Important Disclaimer: The values presented in this heatmap are hypothetical and derived from model projections. They are not based on empirical test data but serve to conceptually demonstrate the layered defense potential in a campus health management context. Actual performance may vary depending on implementation fidelity and real-world threat dynamics.

This model is built using projections and assumptions that might not account for the full range of dynamic factors involved in actual threat environments. The actual efficacy of the defense layers may vary significantly based on a variety of factors, including but not limited to specific system configurations, attack vector variations, and real-time threat intelligence. Therefore, the results presented should be treated as indicative rather than definitive. The real-world performance of the proposed multi-layer defense strategy may differ from the values shown here, depending on the accuracy of the model's assumptions, the sophistication of attacks, and the deployment environment.

5. Future Directions

5.1. Summary of Findings

The network security framework presented in this study offers a comprehensive solution for protecting campus health management systems against a wide range of cyber threats. By incorporating a multi-layered defense approach, the framework ensures that sensitive health data remains secure at every stage — whether in storage, transmission, or during access.

The framework's design centers around several core strengths:

Dynamic defense: The integration of multi-factor authentication (MFA), role-based access control (RBAC), and real-time intrusion detection systems (IDS/IPS) creates a system that is highly adaptable to evolving cyber threats. Unlike traditional security models that rely on static defenses, this framework is capable of dynamically responding to new attack vectors, ensuring continuous protection against both external and internal risks.

Compliance integration: Given the global nature of data privacy regulations, the framework ensures compliance with a range of legal requirements, including General Data Protection Regulation (GDPR) and China's Data Security Law. By designing the framework with flexibility in mind, it can be adapted to various regulatory environments, ensuring that campus health management systems meet legal standards without compromising security.

Real-world effectiveness: The practical application of the framework in Xiamen Nanyang Vocational College demonstrated significant improvements in both security and performance. After implementing the framework, the college reported a 30% reduction in data breach incidents and a 50% decrease in security vulnerabilities. These results underscore the framework's effectiveness in protecting sensitive health data and improving overall system resilience.

The combination of these strengths makes the proposed framework a powerful tool for enhancing the security of campus health management systems, providing both robust protection and regulatory compliance. The multi-layered defense strategy, in particular, offers a level of protection that traditional, single-layer models simply cannot match.

5.2. Future Directions

While the framework has proven effective in its current implementation, there are several avenues for further development and improvement. The following areas present opportunities for expanding the framework's capabilities and adapting it to future cybersecurity challenges:

1) AI-Driven Anomaly Detection and Response

As cyber threats become more sophisticated, traditional threat detection systems may struggle to identify new types of attacks. Integrating artificial intelligence (AI) into the framework can significantly enhance its ability to detect anomalous behavior and respond to security incidents in real-time. While AI-driven anomaly detection shows promise, it is important to acknowledge that the practical implementation of such systems requires substantial training data, computational resources, and time to develop robust models that can adapt to evolving threats. Real-world deployments of AI in cybersecurity have demonstrated success, but challenges such as false positives and the need for continuous model updates remain [8].

Example: Developing an AI-driven anomaly detection algorithm that continuously analyzes system behavior, flagging unusual activity patterns that may indicate a cyberattack, such as an unusual spike in network traffic or abnormal access to sensitive health records. In practice, this approach would require integrating historical data, machine learning algorithms, and constant monitoring of system behavior to refine detection accuracy.

2) Blockchain-Based Distributed Storage

Blockchain technology offers a promising solution for ensuring data integrity and privacy in campus health management systems. A blockchain-based distributed storage system could allow institutions to store health data across multiple nodes, ensuring that no single point of failure exists. However, the integration of blockchain into the existing framework requires careful consideration of its scalability, speed, and cost implications. While blockchain has been successfully implemented in supply chain management and cryptocurrency, its adoption in healthcare data management remains a subject of research. Specifically, performance issues related to data processing speed and consensus mechanisms need to be addressed before blockchain can be fully integrated into a campus health management context [9,10].

Example: Implementing a blockchain prototype for health data storage, where each transaction related to the data (e.g., access, modification, or sharing) is recorded on a secure and immutable ledger. This would ensure transparency and integrity, but the system

would need to be optimized for high throughput and low-latency performance to be practical in a campus environment.

3) Enhanced Key Management for Data Encryption

Key management is a critical aspect of data encryption, and its security plays a significant role in maintaining the overall integrity of health data. A more sophisticated approach to key management, such as HSM-based key rotation and automated key lifecycle management, would further enhance the security of the framework [11].

Example: Implementing a Hardware Security Module (HSM) for managing encryption keys, ensuring that keys are stored securely, and automating their rotation on a regular basis to prevent unauthorized access.

4) Advanced Incident Response Automation (SOAR Integration)

While the integration of SOAR (Security Orchestration, Automation, and Response) technology in the framework has already improved incident response times, there is potential to expand this by integrating more advanced automated workflows. By integrating machine learning and behavioral analytics, the system could automatically adapt response actions based on the type of threat and the environment. This would minimize human intervention, making the incident response process faster and more effective.

Example: Enhancing SOAR technology by integrating machine learning models that can predict the most appropriate response based on the type and nature of the attack, reducing the time it takes to contain threats.

5) Scalability for Larger Institutions

While the framework has been designed with medium-sized institutions in mind, its scalability for larger campuses or multi-campus networks remains a key area for improvement. Future iterations of the framework could include cloud-based scaling solutions, allowing the framework to handle larger volumes of health data and user access across multiple campuses or international locations.

Example: Expanding the framework to incorporate cloud-based architectures that enable it to scale seamlessly as institutions grow, ensuring that security remains intact regardless of the volume of data or number of users.

6) Enhanced Compliance with Emerging Regulations

As global data privacy regulations continue to evolve, the framework should be continuously updated to comply with new laws, such as the California Consumer Privacy Act (CCPA) and the evolving EU ePrivacy Regulation. Keeping the framework aligned with these regulations will ensure its long-term applicability and compliance.

Example: Implementing automated compliance checks that update the system based on the latest regulatory changes, ensuring continuous adherence to global data protection laws [12].

6. Conclusion

The proposed multi-layered security framework addresses the growing need for robust, adaptable security solutions in campus health management systems. By integrating cutting-edge technologies such as MFA, TLS 1.3, real-time monitoring, and compliance integration, the framework provides a comprehensive solution to the challenges of safeguarding sensitive student health data. The case study at Xiamen Nanyang Vocational College demonstrates the framework's effectiveness, with measurable improvements in data protection and system performance.

The framework's dynamic defense strategy, its integration of AI-driven anomaly detection, and the potential for future advancements, such as blockchain-based storage and SOAR integration, position it as a forward-thinking solution that can evolve with the needs of educational institutions.

Moving forward, the framework will continue to adapt and expand, ensuring that it remains effective in the face of evolving cyber threats and regulatory requirements. The

innovations discussed in this chapter, along with the ongoing developments in technology and compliance, will ensure that campus health management systems remain secure, compliant, and capable of protecting the sensitive health data of students for years to come.

References

1. M. K. Kabier, A. A. Yassin, and Z. A. Abduljabbar, "Towards designing educational systems using role-based access control," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 2, pp. 50-63, 2023, doi: 10.22266/ijies2023.0430.05.
2. M. Khan, T. Naz, and M. A. H. Medani, "A multi-layered security model for learning management system," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, 2019, doi: 10.14569/IJACSA.2019.0101229.
3. P. R. Naidu, V. D. Gowda, U. S. Mali, S. Mallikarjun, and S. R. Kawale, "Cloud-based multi-layer security framework for protecting e-health records," in *Proc. 2023 Int. Conf. Artif. Intell. Innov. Healthcare Ind. (ICAIIHI)*, vol. 1, pp. 1-7, Dec. 2023, doi: 10.1109/ICAIIHI57871.2023.10489781.
4. F. K. B. Ablao and R. N. Monreal, "A framework for the development of sharing and collaboration of cyber threat intelligence for colleges in Camarines Norte," *Nanotechnol. Percept.*, vol. 20, no. S2, pp. 369–376, May 2024, doi: 10.62441/nano-ntp.v20iS2.27.
5. Y. Zheng and Y. Chen, "Design and implementation of college students' physical health management platform based on mobile internet," in *Proc. 2021 16th Int. Conf. Comput. Sci. Educ. (ICCSE)*, Aug. 2021, pp. 988-993. IEEE, doi: 10.1109/ICCSE51940.2021.9569572.
6. S. Parveen, A. Sultan, and M. A. Khan, "Integration of identity governance and management framework within universities for privileged users," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 6, 2021, doi: 10.14569/IJACSA.2021.0120664.
7. A. Rehman, K. Haseeb, T. Saba, G. Jeon, and S. Al-Otaibi, "Multi-layer secured edge-AI enabled model for consumer health systems," *IEEE Trans. Consum. Electron.*, 2025, doi: 10.1109/TCE.2025.3555957.
8. G. Andronikidis, C. Eleftheriadis, Z. Batzos, K. Kyranou, N. Maropoulos, G. Sargsyan, and P. Sarigiannidis, "AI-driven anomaly and intrusion detection in energy systems: Current trends and future direction," in *Proc. 2024 IEEE Int. Conf. Cyber Security Resil. (CSR)*, Sept. 2024, pp. 777-782, doi: 10.1109/CSR61664.2024.10679380.
9. S. Safdar and S. Gabrael, "The integration of blockchain and artificial intelligence for secure healthcare systems," *arXiv preprint arXiv:2501.02169*, 2025, doi: 10.48550/arXiv.2501.02169.
10. R. Shinde, S. Patil, K. Kotecha, V. Potdar, G. Selvachandran, and A. Abraham, "Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions," *Trans. Emerg. Telecommun. Technol.*, vol. 35, no. 1, p. e4884, 2024, doi: 10.1002/ett.4884.
11. A. M. Perumal and E. R. S. Nadar, "Architectural framework of a group key management system for enhancing e-healthcare data security," *Healthcare Technol. Lett.*, vol. 7, no. 1, pp. 13-17, 2020, doi: 10.1049/htl.2018.5114.
12. O. Pantelic, K. Jovic, and S. Krstovic, "Cookies implementation analysis and the impact on user privacy regarding GDPR and CCPA regulations," *Sustainability*, vol. 14, no. 9, p. 5015, 2022, doi: 10.3390/su14095015.