Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 23, No. 2, 2026

Application of Big Data Technology to Campus Network Security Risk Assessment and Analysis

Shurui Zhang* and Hao Li

School of PLA Army Services University, Hefei, China
Corresponding author: 2388579972@qq.com

Abstract: With the continuous advancement of smart campus development, the number of terminals connected to campus networks, the diversity of business systems, and the volume of data traffic are increasing rapidly. Focusing on the operational scenario of campus network security risk assessment and analysis, this paper examines the operating mechanism of big data technology in campus network security analysis, explores its intrinsic value for risk identification and security governance, and develops an integrated application pathway from four perspectives: multisource data fusion and acquisition, risk-model optimization and construction, visualized situational assessment, and closed-loop emergency response. The proposed approach is intended to be implemented and tested using real operational data from campus networks. Practical analysis indicates that big data technology can integrate heterogeneous security data from multiple sources, reduce errors in security alerts, shift risk analysis from post-event response toward proactive prediction, and improve the intelligence level of campus network security management. The resulting practice of predictive campus network security risk assessment can provide a useful reference for university network security management.

Keywords: Big data technology; Campus network security; Risk assessment; Situational awareness.

1. Introduction

As the digital transformation of education continues to deepen, smart-campus services are expanding rapidly. A large number of services, including teaching platforms, academic administration systems, student information systems, and campus Internet of Things (IoT) terminals, are being connected to campus networks. Consequently, the internal network structure is constantly changing, and campus networks are becoming increasingly complex. Connected terminals are characterized by mobility and heterogeneity. Student-owned devices are particularly numerous, and their levels of security protection vary substantially. Meanwhile, the incidence of certain cybersecurity threats is increasing. At present, security risk assessment in many universities still relies on conventional approaches such as alerts generated by security appliances and manual log inspection. Data from different devices remain relatively isolated, massive volumes of logs cannot be effectively correlated, and operations personnel generally initiate response measures only after a security incident has occurred, making it difficult to identify potential risks in advance. Therefore, the use of big data technology to improve the quality, timeliness, and accuracy of network security risk assessment is of considerable practical significance.

2. Principles of applying big data technology to campus network security risk assessment

The essential role of big data technology in campus network security risk assessment is to aggregate heterogeneous security data from multiple sources across the campus network through a distributed data architecture, process the data using standardized procedures, and combine data-mining algorithms with a campus-specific security baseline model to identify, classify, trace, and predict cybersecurity risks effectively [1]. During data acquisition, the system collects heterogeneous data from multiple sources, including campus perimeter firewalls, intrusion detection systems, Internet behavior management systems, and server logs. Because raw data are often inconsistent in format and contain substantial noise, big data techniques can be used for preprocessing, including data cleaning, deduplication, and normalization. Sensitive data can be desensitized in a timely manner, while invalid records can be removed. Once unified data standards have been established, distributed storage frameworks can be used to persistently store massive volumes of security data and support offline historical analysis as well as online real-time computing.

During the assessment stage, a stream-processing engine continuously analyzes real-time network traffic. Machine-learning algorithms, including clustering, classification, and continuous prediction, are then used to discover intrinsic correlations among the data and establish normal behavioral baselines for faculty and student accounts, endpoint devices, and business systems. Behaviors that deviate from these baselines are marked as abnormal risks. At the same time, the system can connect to external threat-intelligence repositories, match observed behavior against known cyber threats, and classify risk levels [2]. Assessment results are visualized on a situational-awareness platform to provide security administrators with evidence for subsequent risk-mitigation decisions. In this way, a complete technical chain covering data acquisition, cleaning and storage, mining and modeling, risk assessment, and result output can be established, enabling dynamic and comprehensive campus network security risk analysis.

3. Value of big data technology in campus network security risk assessment

3.1. Breaking Down Security Data Silos

Security data silos can significantly impair the overall quality of security risk assessment. Breaking down such silos is therefore essential to effective campus network security analysis. In conventional campus environments, security appliances, including firewalls, intrusion detection systems, and server auditing systems, are commonly deployed independently. Each system generates its own log information, data are stored in dispersed locations, and data standards are often incompatible. Security operations personnel can therefore review only isolated alerts from individual devices and cannot perform cross-device or cross-system correlation analysis. As a result, they may identify only point anomalies rather than reconstruct complete attack chains, while highly covert attacks may be concealed by fragmented alert information. Big data technology enables the construction of a unified data aggregation platform that eliminates barriers among security appliances and business systems. Network traffic, account behavior, asset vulnerabilities, and externally generated threat intelligence can thus be comprehensively integrated and managed under a unified campus security data framework [3].

3.2. Transforming the Security Assessment Paradigm

Network security risk assessment requires not only consideration of risk types but also continual innovation and optimization of assessment methods. Conventional campus network security follows an event-driven and reactive protection model in which security devices depend primarily on known attack-signature libraries and identify risks through signature matching. Under this model, only attack techniques already recorded in the signature database can be identified, and accurate detection often occurs only after an attack has materialized. With the support of big data technology, massive volumes of historical security logs can be used by machine-learning algorithms to continuously learn normal campus network behavior and establish dynamic, adaptive behavioral baselines. This reduces dependence on fixed attack signatures for risk assessment. The system can monitor in real time the degree to which observed access behavior deviates from baseline patterns and can further identify risks such as anomalous logins, bulk outbound file transfers, and abnormal port scanning. Alerts can thus be triggered before an attack is fully formed whenever possible, enabling more accurate risk prediction. Data-driven models can therefore support a full-lifecycle dynamic governance framework integrating pre-event warning, in-event monitoring, and post-event tracing.

4. Application strategies for big data-driven campus network security risk assessment

4.1. Establishing a Multisource Data Acquisition and Governance System to Strengthen the Data Foundation for Risk Assessment

Data acquisition and governance constitute a critical foundation for predicting campus network security risks. The accuracy of campus network security risk assessment depends on the quality of the underlying raw data. Accordingly, when constructing a big data-based assessment system, priority should be given to ensuring comprehensive data coverage, standardized and controllable data management, and sufficiently diverse data sources. During data acquisition, the scope of campus-wide data collection should first be clearly defined. Collection targets can be divided into four categories: data generated by on-campus security devices, business-system logs, endpoint behavioral data, and external threat intelligence. On-campus data include records from egress firewalls, intrusion prevention systems, Web application firewalls, server audit logs, VPN login logs, and campus network access-authentication logs. Business-system data mainly comprise access records and account-operation logs from core platforms such as academic administration systems, student affairs systems, and library systems. Endpoint data mainly cover the network behavior of faculty and student PCs, mobile smart devices, and IoT devices. External intelligence is obtained by connecting to education-sector network threat-warning platforms and national cybersecurity threat-intelligence repositories, from which information such as malicious domains and Trojan signatures must be synchronized and updated [4].

When constructing the acquisition architecture, distributed collection probes can be deployed at core network nodes, within business-server zones, and at egress gateways. This arrangement can support traffic mirroring and log forwarding while avoiding adverse effects on existing campus bandwidth and normal business operations. Data desensitization should be implemented simultaneously during acquisition. Private information, such as student identity-card numbers and mobile-phone numbers, should be anonymized to satisfy regulatory requirements for information protection. A standardized data-governance workflow should then be established. Because raw logs inevitably contain numerous duplicate records and incomplete fields, automated extract-transform-load (ETL) tools based on big data technologies can be used to clean the data, remove duplicate and invalid records, unify field-naming conventions across device logs, standardize time formats and encoding specifications, and convert data into structured forms. Only standardized data obtained after cleaning should be distributed into the storage cluster. The storage architecture should also distinguish between real-time computing zones and offline analysis zones. In addition, a data-quality supervision mechanism should be established, together with validation rules for data completeness, timeliness, and consistency. Problems such as missing data, collection interruptions, and abnormal fields should be identified, and data quality should be evaluated periodically to ensure that data entering the assessment models remain stable and reliable.

4.2. Constructing a Dynamic Adaptive Assessment Model System for Intelligent Hierarchical Risk Identification

After heterogeneous security data have been aggregated and governed, big data mining algorithms can be used to construct a dynamic adaptive risk-assessment model tailored to campus environments. Through multi-model collaboration, the system can identify, categorize, and rate campus network security risks. The model system primarily consists of a basic rule engine, an unsupervised anomaly-detection model, an

attack-chain correlation model, and a quantitative risk-assessment model, thereby forming a multilevel assessment architecture. The basic rule engine retains mature static signature-matching rules and can identify fundamental attack behaviors such as access from known malicious IP addresses, requests to malicious domains, and scans of high-risk ports. The unsupervised anomaly-detection model mainly employs algorithms such as clustering and isolation forests. Based on historical records of normal campus access behavior, it trains behavioral baselines for users and devices and further detects anomalous behaviors such as logins from unusual locations, bulk access to core business systems outside working hours, and large-scale file input/output within a short period. This compensates for attacks that static rules cannot identify.

The attack-chain correlation model is mainly based on the MITRE ATT&CK framework. It correlates dispersed and isolated alert events according to attack tactics and reconstructs individual log alerts into complete attack chains. By distinguishing key stages such as reconnaissance, intrusion, privilege escalation, lateral movement, and data theft, the model can identify persistent attack behaviors that isolated alerts may fail to reveal in a timely manner [5]. The quantitative risk-assessment model is used to comprehensively evaluate asset criticality, attack severity, vulnerability exploitability, and attack success probability. It automatically calculates risk scores for security events and classifies risks into high, medium, and low levels, with each level automatically mapped to a corresponding response priority. The model can also employ a continuous iterative updating mechanism. After each security incident has been handled, the event sample can be fed back into the training dataset for periodic retraining. New threat intelligence can be incorporated to update model features and reduce false-positive and false-negative rates, thereby adapting to continuously changing attack techniques in campus network environments. To ensure rigor and authenticity in risk identification, a degree of manual review can be incorporated at the final stage, with operations personnel periodically verifying assessment results.

4.3. Developing a Visualized Situational Assessment Platform to Support Comprehensive Risk Analysis and Situational Awareness

Big data storage and analytics engines can be used to develop a visualized campus network security assessment platform that transforms complex back-end analytical results into intuitive and interactive interfaces, thereby providing security administrators with an integrated workspace for assessment activities. The platform can be systematically designed around functional modules such as asset overview, real-time alerts, risk topology, attack tracing, and statistical analysis. The asset-overview module can automatically map campus network assets and label the locations, asset values, and vulnerability states of servers, business systems, and connected terminals. It can display the distribution and risk status of campus assets and maintain a dynamic asset inventory. The real-time alert module receives risk events generated by big data models and presents alert information according to risk level, labeling the event time, source IP, target asset, basic attack type, and key risk information. It can also support rapid retrieval, filtering, and tagging to clarify alert dynamics and reduce the screening workload of operations personnel.

In the risk-topology module, visual topology diagrams can be used to reconstruct attack paths, showing the complete route from an external entry point through lateral movement within the internal network to access to business systems. This directly presents relationships among attack nodes and helps operations personnel rapidly understand the overall attack process. The attack-tracing module can use historical big data storage to support retrospective queries for IP addresses, accounts, and endpoint devices. It retrieves the corresponding access logs and traffic records, reconstructs the complete timeline of attack behavior, and identifies the source [6]. Finally, the statistical-analysis module can generate periodic security-situation reports, calculate monthly and quarterly campus attack-event volumes, determine the distribution of attack types and trends in high-risk vulnerabilities, and discover periodic patterns in campus network security risks. These capabilities support periodic updating and continuous improvement of network security risk assessment.

4.4. Establishing an Assessment-Driven Closed-Loop Response Mechanism Covering Warning, Response, and Traceability

A closed-loop response mechanism is essential for comprehensively identifying network security problems and for analyzing and resolving them from multiple perspectives. Big data-based risk assessment should focus on several fundamental stages: risk assessment, warning dissemination, emergency response, and post-event review and optimization. Only by integrating big data assessment capabilities into the complete lifecycle of campus network security incident handling can the expected benefits be realized. Accordingly, after the platform completes risk identification and classification using big data models, it should automatically trigger a hierarchical warning-distribution mechanism. For high-risk events, alerts should be pushed in real time together with information on the attack chain identified by the assessment model, affected assets, and underlying risk causes, thereby providing operational evidence for security response personnel. Medium- and low-risk events should be stored in an alert work-order pool and assigned as security work orders according to operations scheduling rules. The complete processes of receipt, handling, and review should be recorded so that security incidents are processed promptly through standardized work orders.

From the perspective of security operations, once relevant personnel receive an alert, they can carry out response measures using the traceability data provided by the platform. For external attacks, for example, IP addresses can be blocked through perimeter firewalls and Internet behavior management devices to interrupt malicious traffic. Compromised internal endpoints can be isolated, malicious code can be removed, and related accounts can be reset. Vulnerable business systems can be patched promptly and security hardening measures can be implemented. After incident handling has been completed, operations personnel should record the response process and results in the work order, while the platform retains assessment data, alert records, and response records to form a complete incident archive. During the final review stage, team members can retrieve the big data assessment records for the incident, examine whether the model produced identification errors or delays, and comprehensively evaluate the effectiveness of the

response strategy. Information from all handled cases should then be added to the model-training dataset, while the threat-intelligence repository and assessment rules should be updated simultaneously, providing a basis for more accurate future assessment of campus network security risks.

5. Conclusion

As demonstrated by the preceding analysis, the increasing depth of smart-campus development is making campus network environments progressively more complex. Big data technology enables the integrated analysis of multiple data types and supports the mining of massive datasets, dynamic modeling, and real-time situational analysis. It can effectively break down campus security data silos, transform security assessment from passive post-event response toward proactive pre-event prediction, and improve both the comprehensiveness and accuracy of campus network risk identification. Accordingly, a complete big data-driven implementation framework for campus network security risk assessment can improve the quality of risk analysis and incident handling in campus environments.

References

[1] Zhong, W., & Wang, F. (2026). Research on monitoring and guidance mechanisms for university online public opinion in the context of AIGC [In Chinese]. Network Security Technology & Application, (9), 117-119.

[2] Wang, M. (2026). Research on the application of computer information security technology in university campus networks [In Chinese]. Information & Computer, 38(13), 143-145.

[3] Bu, Y. (2026). Design and implementation of an AI-driven campus network security defense system [In Chinese]. Information Recording Materials, 27(8), 39-41.

[4] Chen, X., & Liang, H. (2026). Research on an intelligent campus network security vulnerability detection framework based on big data [In Chinese]. Intelligent Internet of Things Technology, 58(3), 29-32.

[5] Shi, D. (2026). Application of electronic information technology in campus network security systems [In Chinese]. Electronic Technology, 55(1), 154-155.

[6] Deng, N. (2025). Research on campus network security construction planning integrating big data and Internet of Things applications [In Chinese]. Modern Information Technology, 9(23), 111-116.