China and WTO Review (CWR) Journal
2026, Vol(1)
ISSN: 2384-4388
https://cwto.net

Research Article

Dependency-Centric Security Analysis for Lateral Communication in Data Center Environments

Daan van der Meer [1], Sophie de Vries [1] Thomas Jansen [1*]

[1] Department of Computer Science, Delft University of Technology, Delft, Netherlands
* **Corresponding Author**: thomas.jansen@placeholder.edu

ARTICLE INFO

ABSTRACT

Data center networks generate large volumes of east-west traffic among servers, virtual machines, containers, and storage nodes. Abnormal east-west communication may indicate lateral movement, credential misuse, service probing, or compromised internal hosts. Traditional perimeter-based intrusion detection systems are less effective in this scenario because malicious traffic often remains inside the data center. This study proposes an interpretable ensemble learning framework for detecting east-west traffic anomalies in data center networks. The proposed model combines Histogram Gradient Boosting, Random Forest, and LightGBM through a confidence-weighted voting strategy. To improve transparency, SHAP is used to explain how flow dependency features contribute to anomaly decisions. Experiments are conducted on a simulated data center traffic environment with 320 virtual hosts, 48 application services, and 6 storage clusters. The dataset contains 4.27 million labeled flow records collected under normal workload migration, database synchronization, internal scanning, lateral movement, abnormal service discovery, and privilege-escalation traffic. After preprocessing, 52 features are extracted, including service-call frequency, host-pair communication persistence, internal port diversity, failed connection ratio, flow burst density, and cross-segment byte imbalance. The proposed framework achieves 98.29% accuracy, 97.64% F1-score, and 98.91% AUC in binary anomaly detection. In multi-class classification, it obtains a macro-F1 of 96.18% across five internal attack categories. Compared with a single LightGBM classifier, the ensemble model reduces false positives by 12.7% and improves detection recall for lateral movement traffic by 3.82%. SHAP analysis shows that abnormal host-pair persistence, sudden port diversity expansion, failed internal connections, and cross-segment byte imbalance are the most important indicators of suspicious east-west traffic. The results indicate that explainable ensemble learning can improve internal threat detection and provide interpretable evidence for data center security operations.

Keywords: Data Center Security, East-West Traffic, Network Anomaly Detection, Lateral Movement, Ensemble Learning, SHAP, Explainable Intrusion Detection

INTRODUCTION

Data center networks support massive east-west traffic among servers, virtual machines, containers, microservices, databases, and storage nodes. Such traffic is essential for workload migration, service discovery, database synchronization, distributed computing, and cross-service coordination. However, the rapid growth of internal communication also creates a hidden attack surface inside data centers. Once an attacker gains access to the internal network, lateral movement, credential misuse, service probing, privilege escalation, and internal data exfiltration may occur without crossing the network perimeter again (Zhang, Gao, & Tong, 2026; Aslam & Steltzer, 2025). This makes traditional perimeter-based intrusion detection less effective for modern data center environments (Qi & Qiao, 2026; George, Baskar, & Srikaanth, 2026). Recent research has examined abnormal traffic detection using machine learning, deep learning, graph-based analysis, and policy-driven vulnerability risk quantification for large-scale cloud infrastructure data security (Shao, 2026).

Compared with internet-facing traffic, east-west traffic has stronger dependency relationships and more complex service interaction patterns (Almuseelem, 2026; Su & Shi, n.d.). Internal flows are often generated by

microservice calls, database replication, storage access, container orchestration, and workload migration (Freire, 2025; Xu, Ma, Liu, & Yue, 2026). These flows may appear normal at the packet level but become suspicious when viewed through host-pair persistence, service-call frequency, failed connection ratio, internal port diversity, or cross-segment traffic imbalance. Existing machine learning and deep learning methods can capture nonlinear traffic patterns and host relationships, and they have shown promising results in abnormal traffic detection (Ali, Thakur, Schmeelk, Debello, & Dragos, 2025; Huang, 2026). However, many studies still rely on public datasets that mainly describe internet-facing attacks or general intrusion scenarios (Landauer, Skopik, Stojanovic, Flatscher, & Ullrich, 2025; Ma, 2026). These datasets do not fully reflect the dependency structure, service-call behavior, and hidden lateral movement patterns of modern data center networks (Amin, 2026; Wang, Wen, Wu, Wang, & Cai, 2025). Another limitation is the lack of explainability in existing detection models. Some studies report high accuracy, precision, or F1-score, but provide limited evidence for security analysts to understand why an alert is generated (Sharma, Kumar, & Poojari, 2025; Zhu, Yao, & Yang, 2025). In real data center operations, an alarm needs to be linked to specific traffic evidence, such as abnormal service discovery, repeated failed connections, sudden flow bursts, unusual internal port usage, persistent host-pair communication, or cross-segment byte imbalance (Stolworthy, Culler, & Cerkovnik, 2026; Li & Liu, 2026). Without interpretable evidence, analysts may find it difficult to distinguish true internal threats from normal workload fluctuation, container scaling, database synchronization, or temporary service migration (Zi, Gong, Xue, Zou, Qi, & Deng, 2025; Oloruntoba, 2025). Therefore, east-west traffic anomaly detection requires not only high detection accuracy, but also feature-level explanations that can support internal threat investigation and response prioritization (Yin, Huang, & Rao, 2026; Wali, Khan, & Imran, 2025).

To address these problems, this study proposes an interpretable ensemble learning framework for detecting east-west traffic anomalies in data center networks. The framework integrates Histogram Gradient Boosting, Random Forest, and LightGBM through confidence-weighted voting to improve detection stability across different internal traffic patterns. Flow dependency features are designed to describe service-call frequency, host-pair communication persistence, internal port diversity, failed connection ratio, flow burst density, and cross-segment byte imbalance. Experiments are conducted in a simulated data center traffic environment with 320 virtual hosts, 48 application services, and 6 storage clusters. The dataset contains 4.27 million labeled flow records covering normal workload migration, database synchronization, internal scanning, lateral movement, abnormal service discovery, and privilege-escalation traffic. SHAP is used to explain how each feature contributes to anomaly decisions and to provide interpretable evidence for security analysis. The purpose of this study is to develop a practical detection method for hidden attacks in data center east-west communication. By combining ensemble learning, confidence-weighted voting, flow dependency features, and SHAP-based interpretation, the proposed framework aims to improve anomaly detection accuracy while reducing false positives and missed internal threats. This design is meaningful for data center security because it helps analysts understand whether an alert is caused by normal workload changes, abnormal service probing, lateral movement, or privilege-escalation behavior. Therefore, the study provides a risk-aware and explainable approach for detecting internal threats in modern data center networks, where traffic dependency, service complexity, and hidden attack paths must be considered together.

MATERIALS AND METHODS

Sample and Study Scenario Description

This study used a simulated data center network to collect east-west traffic data. The environment included 320 virtual hosts, 48 application services, and 6 storage clusters. The virtual hosts represented web services, application servers, database nodes, cache nodes, container instances, and internal management hosts. Traffic was collected during workload migration, database synchronization, internal service calls, and storage access. These settings were used to reflect common internal communication in cloud data centers. In this type of network, hosts exchange service requests and data packets without passing through the external network boundary. A total of 4.27 million labeled flow records were collected. Each record described one host-to-host flow and included flow duration, packet count, byte count, connection state, service type, port use, and host-pair behavior.

Experimental Design and Control Settings

The experiment included one normal traffic group and five abnormal traffic groups. The normal group included workload migration, database synchronization, and regular service communication. It was used as the control group. The abnormal groups included internal scanning, lateral movement, abnormal service discovery, privilege-escalation traffic, and compromised-host communication. These attack types were selected because they are common signs of hidden threats inside data centers. Unlike external attacks, these behaviors often occur between

trusted internal hosts and may not be detected by perimeter security tools. Each traffic group was generated under different service loads, host densities, and communication frequencies. This setting reduced the influence of a single traffic condition on the results. Single Histogram Gradient Boosting, Random Forest, LightGBM, and SVM models were used as comparison models to test the effect of the ensemble framework.

Measurement Methods and Quality Control

East-west traffic was measured at the flow level. The recorded variables included service-call frequency, host-pair communication persistence, internal port diversity, failed connection ratio, flow burst density, cross-segment byte imbalance, average packet size, connection interval, source-host activity, destination-host activity, and service-access frequency. Raw logs were checked before feature extraction. Duplicate flow records, incomplete connection traces, invalid timestamps, and records with missing host identifiers were removed. Traffic windows with collection errors were also excluded. Numerical features were checked against preset value ranges to remove impossible values. Class labels were assigned according to the known traffic scenario. To reduce label noise, transition periods between normal and attack states were checked separately. After preprocessing and quality control, 52 flow dependency features were retained for model training and testing.

Data Processing and Model Formulas

The dataset was divided into training, validation, and testing sets by stratified sampling. This method kept the class distribution similar across the three sets. Categorical variables, such as service type and connection state, were encoded before model training. Numerical variables were scaled for models that required feature scaling, while tree-based models used the original values. Let *xi* denote the feature vector of the *i-th* flow record, and let $h_m(x_i)$ denote the output of the *m-th* base classifier. The confidence-weighted score for class *c* was calculated as (1):

$$S_c(x_i)=\sum_{m=1}^{M} w_m p_m(c|x_i) \tag{1}$$

where w_m is the confidence weight of the m-th classifier, and $p_m(c|x_i)$ is its predicted probability for class *c* . The final class label was obtained as (2):

$$\hat{y}_i=\arg\max_c \quad S_c(x_i) \tag{2}$$

Model performance was measured by accuracy, F1-score, recall, and AUC. The false positive rate was also recorded because too many false alarms can increase the workload of security analysts.

Model Training and SHAP-Based Explanation

Histogram Gradient Boosting, Random Forest, and LightGBM were trained as base classifiers. Their outputs were combined by confidence-weighted voting. The validation set was used to select model parameters, including tree depth, learning rate, number of estimators, and minimum sample split. The final results were reported on the independent testing set. All baseline models used the same data split to keep the comparison fair. After training, SHAP was used to explain the effect of each feature on anomaly decisions. Global SHAP values were used to rank the main signs of suspicious east-west traffic. Local SHAP values were used to explain individual abnormal flows. This step showed whether an alert was mainly related to abnormal host-pair persistence, sudden port diversity expansion, failed internal connections, flow bursts, or cross-segment byte imbalance. The SHAP results were used only for explanation and did not change the original labels.

RESULTS AND DISCUSSION

Binary Detection Performance

The proposed ensemble framework achieved 98.29% accuracy, 97.64% F1-score, and 98.91% AUC in binary east-west traffic anomaly detection. These results show that flow dependency features can separate normal internal communication from suspicious host-to-host behavior. Compared with the single LightGBM model, the ensemble reduced false positives by 12.7%, which is important for data center security operations because too many false

alarms can increase manual review work. The result also shows that confidence-weighted voting can improve decision stability when normal workload migration and abnormal internal traffic have similar flow patterns (Yang, 2026; Bose, 2026). Prior network anomaly detection work has shown that Random Forest, SVM, and other supervised models can achieve high detection accuracy, but their performance may vary when anomaly rates and traffic states change. For example, Bose R. et al. reported different accuracy and false-positive behavior among Logistic Regression, Random Forest, and SVM in network anomaly detection, showing the need for stable model selection under varied traffic conditions. As shown in **Figure 1**, feature-level explanation is also needed because high scores alone do not show why a flow is abnormal.

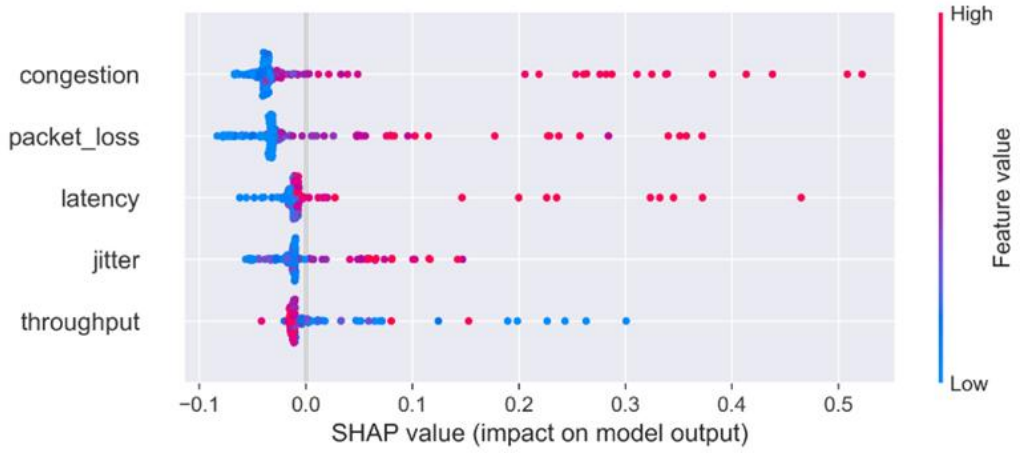

Figure 1. SHAP Ranking of the Main Features Used to Detect East-West Traffic Anomalies

Multi-Class Detection of Internal Attack Categories

In multi-class classification, the proposed model achieved a macro-F1 of 96.18% across five internal attack categories. Internal scanning and abnormal service discovery were easier to detect because they caused clear increases in port diversity, service-call frequency, and failed connection ratio. Lateral movement and privilege-escalation traffic were more difficult because they often used trusted internal paths and normal service accounts. Their traffic patterns were closer to regular database synchronization or workload migration. This class overlap explains why some samples were misclassified (Deng & Yang, 2026; Mahmood, Jamel, Salem, & Ashraf, 2025). The 3.82% recall gain for lateral movement traffic over the single LightGBM model is therefore meaningful. It suggests that host-pair persistence, failed internal connections, and cross-segment byte imbalance can provide useful evidence for weak but repeated internal attack behavior. Compared with general network anomaly studies that mainly focus on congestion, packet loss, or single-point anomalies, the present study gives more attention to dependency patterns among internal hosts and services. Zhang Z. et al. used network metrics such as congestion and packet loss for anomaly detection, while the present study focuses on flow dependency features in east-west data center traffic.

Effect of the Confidence-Weighted Ensemble Strategy

The confidence-weighted ensemble improved performance by combining Histogram Gradient Boosting, Random Forest, and LightGBM. Histogram Gradient Boosting handled nonlinear changes in high-volume flow records. Random Forest reduced unstable predictions by averaging multiple trees. LightGBM improved training efficiency and worked well with sparse flow features. The combined model performed better than a single classifier because different internal attacks show different feature patterns. Internal scanning depends more on port diversity and failed connections, while lateral movement depends more on host-pair persistence and service-call changes. A single model may focus too much on one feature group and miss weaker attack signals. Recent ensemble-based intrusion detection studies also report that combined classifiers can improve classification performance in network security tasks, especially when data are imbalanced or class boundaries are unclear (Zhang, 2026; Doost, Moghadam, Khezri, Basem, & Trik, 2025). As shown in **Figure 2**, confusion-matrix analysis is useful for checking whether the model performs evenly across attack classes rather than only improving the overall accuracy.

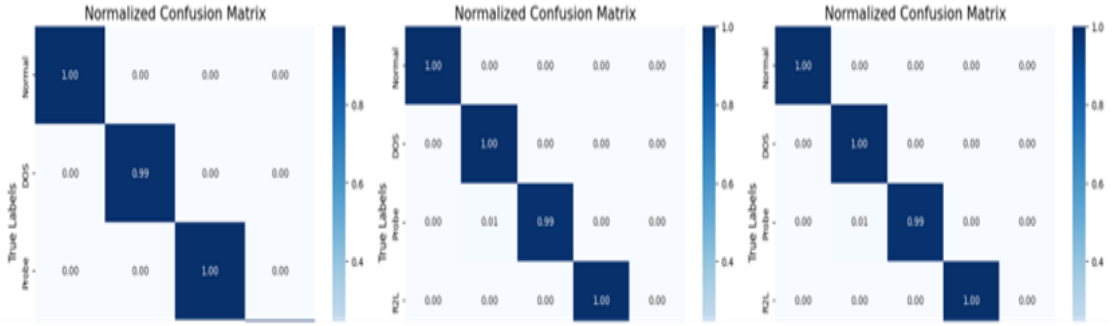

Figure 2. Confusion Matrix of the Ensemble Model for Classifying Internal Network Attacks

SHAP Explanation and Security Interpretation

SHAP analysis showed that abnormal host-pair persistence, sudden port diversity expansion, failed internal connections, flow burst density, and cross-segment byte imbalance were the main indicators of suspicious east-west traffic. These features have clear security meaning. Persistent communication between unusual host pairs may indicate lateral movement. A sudden increase in internal port diversity may suggest scanning or abnormal service discovery. A high failed connection ratio may reflect credential misuse or blocked privilege-escalation attempts (Gao, Gao, Gao, Zhou, & Lu, 2026). Cross-segment byte imbalance may indicate unusual data movement between service zones. This explanation helps security analysts connect model alerts with concrete traffic evidence. It also reduces the weakness of black-box detection, where the model gives an alert but does not show the reason. However, this study still has limitations. The dataset was generated in a simulated data center environment. Real production networks may include encrypted service calls, short-lived containers, incomplete flow logs, and mixed attack paths. Future work should test the framework on production flow records and add online updating for long-term security monitoring.

CONCLUSION

This study presented an interpretable ensemble method for detecting east-west traffic anomalies in data center networks. The method combined Histogram Gradient Boosting, Random Forest, and LightGBM through confidence-weighted voting. SHAP was used to explain the effect of flow dependency features on model decisions. The proposed framework achieved 98.29% accuracy, 97.64% F1-score, and 98.91% AUC in binary anomaly detection. It also reached 96.18% macro-F1 in multi-class classification. Compared with a single LightGBM model, the ensemble reduced false positives by 12.7% and improved recall for lateral movement traffic by 3.82%. SHAP results showed that abnormal host-pair persistence, sudden port diversity expansion, failed internal connections, flow bursts, and cross-segment byte imbalance were closely related to suspicious internal traffic. These results indicate that flow dependency features can help identify hidden threats that are hard to detect with perimeter-based security tools. The method can support internal threat monitoring, alert review, and incident analysis in cloud data centers. However, this study was based on simulated traffic data. Real production networks may include encrypted service calls, short-lived containers, incomplete logs, and mixed attack paths. Future work should test the method on real data center flow logs and improve online updating for long-term use.

REFERENCES

Ali, M. L., Thakur, K., Schmeelk, S., Debello, J., & Dragos, D. (2025). Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study. *Applied Sciences, 15*(4), 1903.

Almuseelem, W. (2026). Collaborative intrusion detection systems in SD-WAN enterprise networks with federated learning: a comprehensive survey. *Journal of King Saud University Computer and Information Sciences*.

Amin, T. B. (2026). An Empirical Analysis of AI-Enabled Network Observability Platforms for Financial Infrastructure Security. *American Journal of Advanced Technology and Engineering Solutions, 6*(01), 460-505.

Aslam, N., & Steltzer, H. (2025). Cybersecurity and Network Security: Strengthening Defenses Against Emerging Threats. Preprint]. *ResearchGate*. https://doi. org/10.13140/RG, 2(16350.96321).

Bose, R. (2026). Agentic RAG: Autonomous Information Systems. In *Mastering Retrieval-Augmented Generation: Advanced Techniques and Production-Ready Solutions for Enterprise AI* (pp. 611-691). Berkeley, CA: Apress.

Deng, X., & Yang, J. (2026). Design of a Quantitative Futures Trading Model Incorporating Multimodal Feature Fusion and Tail Risk Control. Available at SSRN 6702398.

Doost, P. A., Moghadam, S. S., Khezri, E., Basem, A., & Trik, M. (2025). A new intrusion detection method using ensemble classification and feature selection. *Scientific Reports, 15*(1), 13642.

Freire, G. M. (2025). *A distributed architecture of reactive microservices orchestrated by kubernetes case study on load balancing in local cloud* (Doctoral dissertation, Universidade de São Paulo).

Gao, G., Gao, R., Gao, R., Zhou, H., & Lu, C. (2026, March). Performance Study of Enterprise SMS Communication Scheduling Mechanisms in Triple-Play Convergence Environments. In *2026 IEEE 8th International Conference on Communications, Information System and Computer Engineering (CISCE)* (pp. 82-86). IEEE.

George, A. S., Baskar, T., & Srikaanth, P. B. (2026). Beyond the Perimeter Rethinking Enterprise Network Security in an Age of Distributed Threats.

Huang, R. (2026). ConfSched: Confidence-Threshold Routing for Efficient Edge-Cloud Activity Recognition. *World Journal of Engineering and Technology, 14*(2), 471-486.

Landauer, M., Skopik, F., Stojanovic, B., Flatscher, A., & Ullrich, T. (2025). A review of time-series analysis for cyber security analytics: from intrusion detection to attack prediction. *Int. J. Inf. Sec., 24*(1), 3.

Li, Y., & Liu, S. (2026, May). A Study on Dynamic Optimization of Alerting Policies and Multi-Agent Decision-Making Mechanisms in Cloud Environments. In *2026 7th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)* (pp. 703-706). IEEE.

Ma, Y. (2026). Industrial Financial Risk Prediction Model Based on Graph Neural Network and Knowledge Graph Inference. *Journal of Circuits, Systems and Computers, 35*(16), 2650103.

Mahmood, Z., Jamel, L., Salem, D. A., & Ashraf, I. (2025). Improving learning from the complex multi-class imbalanced and overlapped data by mapping into higher dimension using SVM++. *Scientific Reports, 15*(1), 31245.

Oloruntoba, O. (2025). Architecting resilient multi-cloud database systems: distributed ledger technology, fault tolerance, and cross-platform synchronization. *International Journal of Research Publication and Reviews, 6*(2), 2358-2376.

Qi, C., & Qiao, X. (2026). Building Reliable AI Systems: A Framework That Bridges Architecture and Operations. Available at SSRN 6795298.

Shao, W. (2026). Policy-Driven Vulnerability Risk Quantification framework for Large-Scale Cloud Infrastructure Data Security. *arXiv preprint arXiv:2604*.06252.

Sharma, A., Kumar, V. K., & Poojari, A. (2025). Prioritize threat alerts based on false positives qualifiers provided by multiple AI models using evolutionary computation and reinforcement learning. *Journal of The Institution of Engineers (India): Series B, 106*(4), 1305-1322.

Stolworthy, R. V., Culler, M. J., & Cerkovnik, J. A. (2026). Threat Hunt Guide for BESS Environments (No. INL/RPT-25-89299). *Idaho National Laboratory (INL), Idaho Falls, ID* (United States).

Su, D., & Shi, X. Optimizing Family–School Collaboration to Improve Educational and Social Outcomes for Children with Intellectual Disabilities in Inclusive Public Schools.

Wali, S., Khan, M. I., & Imran, M. (2025). Semantic-aware reinforcement and ensemble learning for signal management and anomaly detection in IoT systems. *Scientific Reports, 15*(1), 42594.

Wang, Y., Wen, Y., Wu, X., Wang, L., & Cai, H. (2025). Assessing the Role of Adaptive Digital Platforms in Personalized Nutrition and Chronic Disease Management.

Xu, S., Ma, Q., Liu, H., & Yue, L. (2026). Continuous Reorganization and Performance Preservation of Agent Memory Structure Under Distributed Change Environments.

Yang, J. (2026). Stage-Coupled Computational Framework for Stratified Accessibility and Equity Analysis in Community-Based Elderly Care Services.

Yin, J., Huang, Y., & Rao, H. (2026). A Study on User Behavior Signal-Driven Predictive Models for Digital Platform Consumption Trends. Available at SSRN 6607298.

Zhang, Z. (2026). A Study on Return Optimization in E-commerce for Complex Consumer Goods Driven by Installation Information Quality. Available at SSRN 6734720.

Zhang, Z., Gao, Y., & Tong, Y. (2026). CausalML4CX: A Causal Inference and Machine Learning Framework for Customer Experience Optimization with Application in Banking.

Zhu, W., Yao, Y., & Yang, J. (2025). Optimizing Financial Risk Control for Multinational Projects: A Joint Framework Based on CVaR-Robust Optimization and Panel Quantile Regression.

Zi, Y., Gong, M., Xue, Z., Zou, Y., Qi, N., & Deng, Y. (2025, August). Graph neural network and transformer integration for unsupervised system anomaly discovery. In *2025 5th International Conference on Computer Science and Blockchain (CCSB)* (pp. 158-162). IEEE.

ETHICAL DECLARATION

Conflict of interest: No declaration required. **Financing:** No reporting required. **Peer review:** Double anonymous peer review.