THE JOURNAL OF APPLIED ENGINEERING AND TECHNOLOGIES
2026 Vol. 1, No. 3, ISSN (O): 3154-7877

Service Interaction Profiling for Abnormal Communication Discovery in Cloud-Native Microservice Systems

Wei Jun Tan[1], Jia Hui Lim[1], Marcus Yong Chen[1*]

[1]School of Computing, National University of Singapore, Singapore 117417, Singapore

Corresponding Author*: Marcus Yong Chen E-mail: marcus.chen@xxxx.edu.sg

ARTICLE INFO

Keywords

Blockchain-enabled IoT
gateway security
anomaly detection
stacking ensemble learning
explainable AI
SHAP
network intrusion detection

Published:

01 September 2026

ABSTRACT

Blockchain-enabled IoT networks can improve device authentication and data integrity, but IoT gateways remain vulnerable to abnormal traffic, flooding attacks, and unauthorized access attempts. Since gateway devices often operate with limited computing resources, anomaly detection models must provide high accuracy, low latency, and clear decision explanations. This study proposes an interpretable gateway-level anomaly detection method for blockchain-enabled IoT networks based on stacking ensemble learning. The proposed framework uses Decision Tree, LightGBM, and K-Nearest Neighbors as base learners, while Logistic Regression is applied as the meta-classifier. SHAP analysis is used to interpret how gateway traffic characteristics contribute to anomaly detection results. Experiments are performed on the N-BaIoT and BoT-IoT datasets, containing 1.21 million and 2.46 million labeled traffic samples, respectively. After data cleaning and feature filtering, 35 gateway-level statistical features are used for model training, including packet count variance, connection interval, source port repetition, byte rate, and failed connection ratio. The stacking ensemble model achieves 98.74% accuracy, 98.03% F1-score, and 99.05% AUC on binary classification tasks. In multi-class attack detection, the model reaches 96.58% macro-F1 across scanning, DDoS, data exfiltration, and unauthorized access attacks. Compared with a standalone LightGBM model, the proposed method reduces false positives by 15.9% and improves recall for low-frequency attack classes by 3.46%. SHAP analysis shows that repeated short connections, abnormal outbound byte rates, and high packet count variance are strongly associated with compromised IoT gateway behavior. The results indicate that stacking-based explainable anomaly detection can strengthen the security monitoring capability of blockchain-assisted IoT gateways.

1. Introduction

Blockchain-enabled Internet of Things (IoT) networks have been increasingly applied in smart homes, industrial control, healthcare monitoring, intelligent transportation, and edge computing systems (Asaithambi et al., 2025; Su & Zhang, n.d.). By integrating blockchain with IoT, distributed ledgers can support device authentication, data integrity verification, secure event recording, and traceable data exchange among heterogeneous devices. These advantages are particularly valuable in decentralized IoT environments, where devices frequently interact with gateways, edge servers, and cloud-based service platforms. Nevertheless, blockchain cannot fully prevent abnormal traffic before malicious behavior reaches the ledger layer. In many practical deployments, IoT gateways remain the primary communication bridge between end devices, edge nodes, and blockchain

Citation：Tan, W. J., Lim, J. H., & Chen, M. Y. (2026). Service interaction profiling for abnormal communication discovery in cloud-native microservice systems. *The Journal of Applied Engineering and Technologies*, 1(3), 27-35.

https://doi.org/10.64744/tjaet.2026.282.

service layers. As a result, gateways are directly exposed to flooding attacks, botnet traffic, repeated connection attempts, unauthorized access requests, and abnormal data transmission patterns. Once a gateway is compromised or overloaded, malicious traffic may spread rapidly across connected devices before the blockchain layer records, verifies, or audits the event.

Recent studies have investigated blockchain-based mechanisms for access control, identity management, secure data sharing, decentralized trust, and audit logging in IoT networks (Khayer et al., 2025; Xu et al., 2026). At the same time, machine learning methods have been widely used for IoT intrusion detection by learning traffic behavior from packet-level, flow-level, and session-level features in public datasets such as N-BaIoT and BoT-IoT (Huang, 2026; Singal et al., 2026). Recent research on SHAP-based explainable ensemble learning has also shown that ensemble models can improve network traffic anomaly detection while providing interpretable feature-level evidence for embedded security systems (Shao, 2026). This direction is highly relevant to blockchain-enabled IoT gateways because detection results should not only be accurate but also explainable enough to support real-time blocking, audit logging, and later forensic review (Salam et al., 2026; Yin et al., 2026). Traditional machine learning classifiers remain useful for IoT intrusion detection because they are suitable for structured traffic data and usually require lower computational cost than deep learning models. Decision trees, boosting models, and distance-based classifiers can identify abnormal patterns from traffic statistics, connection behaviors, and communication frequency. Deep learning models can capture more complex attack patterns, especially when traffic behavior is nonlinear or temporally dependent (Alharthi et al., 2025; Yang, 2026). However, deep models usually require more memory, larger training datasets, longer training time, and careful parameter tuning. These requirements may limit their deployment on lightweight IoT gateways with constrained computing resources. In addition, many deep learning-based detection systems operate as black-box models, making it difficult for security operators to understand why a gateway alarm is triggered (Li & Liu, 2026; Sharma et al., 2026). Although existing studies have reported promising detection performance, several limitations remain. Many models are evaluated on limited datasets, simplified traffic scenarios, or selected attack categories (Alshehri et al., 2025; Deng & Yang, 2026). Some works mainly focus on binary classification and do not sufficiently consider minority attack classes, which are often more difficult to detect but may cause serious security consequences (Zhang, 2026). Overall accuracy is also frequently emphasized, while false positive rate, class-level recall, F1-score, and minority-class detection performance receive less attention. In gateway-level security monitoring, a high false positive rate may overload operators and weaken the reliability of automatic blocking mechanisms. Missed detection of low-frequency attacks may allow malicious devices to remain active in the network and generate persistent security risks. Ensemble learning provides a practical way to improve detection stability and robustness in blockchain-enabled IoT gateway environments (Awasthi et al., 2026; Zhang et al., 2026). By combining multiple learners, an ensemble model can reduce the limitations of a single classifier and better capture diverse traffic patterns. Decision Tree models can provide clear rule-based separation of abnormal behaviors. LightGBM can efficiently learn complex feature interactions from structured gateway traffic data. K-Nearest Neighbors can identify local similarity patterns that may help distinguish abnormal connection behaviors. A stacking architecture can further integrate these base learners through a meta-classifier, allowing the final model to learn how different classifiers contribute to the detection decision (Qi & Qiao, 2026; Sultan et al., 2025). Compared with simple voting or bagging, stacking can provide a more flexible decision structure and may improve classification performance under mixed attack conditions (Alalwany et al., 2025; Ma, 2026). Explainable artificial intelligence is also necessary for practical IoT gateway security.

In blockchain-assisted environments, gateway alerts may be used for real-time access restriction, smart contract-triggered logging, incident investigation, and cross-node security auditing. Therefore, operators need to understand which traffic features contribute to each anomaly decision. SHAP analysis can provide both global feature importance and local explanations for individual detection results. This allows the system to identify whether an alarm is mainly driven by packet count variance, connection interval, source port repetition, byte rate, failed connection ratio, or other gateway-level behavioral indicators (Chen et al., 2025; Ennaji et al., 2026). Such explanations can improve trust in the detection model and support more transparent security management.

To address these gaps, this study proposes an interpretable gateway-level anomaly detection framework for blockchain-enabled IoT networks based on stacking ensemble learning. Decision Tree, LightGBM, and K-Nearest Neighbors are used as base learners, while Logistic Regression is adopted as the meta-classifier to integrate their complementary detection strengths. SHAP analysis is applied to explain the contribution of gateway traffic features and provide interpretable evidence for both normal and abnormal classifications. The purpose of this study is to improve detection accuracy, reduce false positives, strengthen minority-class detection, and maintain practical suitability for lightweight gateway security monitoring. By combining stacking ensemble learning with feature-level explanation, this research provides a more transparent and operationally meaningful intrusion detection method for blockchain-assisted IoT systems, supporting real-time gateway protection, reliable audit logging, and more effective forensic analysis.

2. Materials and Methods

2.1 Samples and Study Objects

The samples were taken from two public IoT traffic datasets, N-BaIoT and BoT-IoT. These datasets were used because they contain labeled traffic records from normal IoT communication and common attack scenarios. After data cleaning, 1.21 million valid samples were retained from N-BaIoT, and 2.46 million valid samples were retained from BoT-IoT. The study focused on gateway-level traffic flows generated by smart devices, edge nodes, and external network requests. Each sample described traffic behavior within a fixed time window. The traffic records covered normal communication, scanning attacks, DDoS attacks, data leakage, and unauthorized access attempts. These samples represented typical gateway traffic in blockchain-enabled IoT networks, where gateways handle device communication, traffic forwarding, and security event recording.

2.2 Experimental Design and Control Settings

The experiment was designed to test whether the stacking model could improve gateway-level anomaly detection compared with single models. The experimental group used the proposed stacking framework. Decision Tree, LightGBM, and K-Nearest Neighbors were used as base learners, and Logistic Regression was used as the final classifier. The control groups included standalone Decision Tree, LightGBM, K-Nearest Neighbors, Random Forest, and Logistic Regression models. These models were selected because they are commonly used in IoT traffic classification and represent rule-based, distance-based, linear, and ensemble methods. Binary classification was used to separate normal and abnormal traffic. Multi-class classification was used to identify different attack types. The same training, validation, and testing sets were used for all models. Stratified sampling was applied to keep the class ratio similar in each subset.

2.3 Measurement Methods and Quality Control

Gateway-level traffic features were extracted from the cleaned records. The measured

variables included packet count variance, connection interval, source port repetition, byte rate, failed connection ratio, inbound and outbound packet ratio, flow duration, and protocol frequency. These variables were used because they can reflect traffic bursts, repeated connections, and suspicious gateway behavior. Duplicate records, missing values, invalid labels, and non-numeric errors were removed before training. Continuous variables were scaled by min–max normalization. Class labels were converted into numerical labels. Feature filtering was then used to remove highly repeated or weak variables. The final feature set contained 35 gateway-level statistical variables. Five-fold cross-validation was used on the training set to reduce random bias. The test set was kept independent and was not used for model tuning.

2.4 Data Processing and Model Formulas

All samples were cleaned, scaled, and divided into training, validation, and testing sets. The stacking model was trained in two steps. First, the base learners generated prediction probabilities for each sample. Then, these probability outputs were used as input variables for the Logistic Regression classifier. The final prediction was expressed as:

$$\hat{y}=g(f_1(x),f_2(x),f_3(x))$$

where is the input traffic feature vector; are the outputs of Decision Tree, LightGBM, and K-Nearest Neighbors; and is the Logistic Regression classifier. Model performance was measured using accuracy, precision, recall, F1-score, macro-F1, AUC, and false positive rate. The F1-score was calculated as:

$$F1=\frac{2\times Precision\times Recall}{Precision+Recall}$$

This metric was used because it balances precision and recall. It is also more suitable than accuracy when attack classes are unevenly distributed.

2.5 Model Interpretation and Evaluation Procedure

SHAP analysis was used to explain how each gateway-level traffic feature affected the final detection result. SHAP values were calculated for overall feature importance and single-sample interpretation. Overall interpretation was used to find the most important traffic variables in the test set. Single-sample interpretation was used to explain why a given record was classified as normal or abnormal. The proposed model was tested from four aspects: binary anomaly detection, multi-class attack detection, false positive reduction, and recall for low-frequency attacks. The stacking model was compared with all control models under the same data split and feature setting. This evaluation tested not only detection accuracy but also model stability, class-level sensitivity, and practical interpretability for blockchain-enabled IoT gateway security monitoring.

3. Results and Discussion

3.1 Overall Detection Performance

The stacking ensemble achieved strong results in the binary anomaly detection task. It reached 98.74% accuracy, 98.03% F1-score, and 99.05% AUC. These results show that the model separated normal gateway traffic from abnormal traffic with stable performance. Compared with the standalone LightGBM model, the stacking model reduced false positives by 15.9%. This result indicates that the combined model reduced the weakness of a single classifier. Decision Tree captured clear rule patterns. LightGBM learned nonlinear feature relations. K-Nearest Neighbors identified local traffic similarity. Logistic Regression then combined their outputs and gave the final

result. This finding is close to recent ensemble-based IoT anomaly detection studies, which reported that combined models are more stable when traffic features are mixed and attack patterns vary across datasets (Alqaraleh, 2025; Liang et al., 2025). Unlike studies that mainly report overall accuracy, this study also considered false positives, which is important for gateway use because repeated false alarms increase the burden on network administrators.

3.2 Multi-Class Attack Classification Results

In the multi-class detection task, the stacking model reached a macro-F1 score of 96.58% across scanning, DDoS, data leakage, and unauthorized access attacks. The model performed better on common attacks, such as scanning and DDoS. These attacks usually show clear traffic bursts, repeated connection requests, and abnormal packet rates. The improvement was more important for low-frequency attacks. Compared with standalone LightGBM, the stacking model improved recall for minority attack classes by 3.46%. This result shows that the ensemble structure did not only fit dominant classes but also kept sensitivity to rare attack behavior. Many IoT intrusion detection studies report high accuracy on uneven datasets but give limited analysis of minority-class recall. In blockchain-enabled IoT networks, this may cause serious risk because rare attacks, such as unauthorized access or data leakage, can be more damaging than repeated flooding events (Alqaraleh, 2025; Wang et al., 2026). Therefore, class-level metrics should be reported together with accuracy.

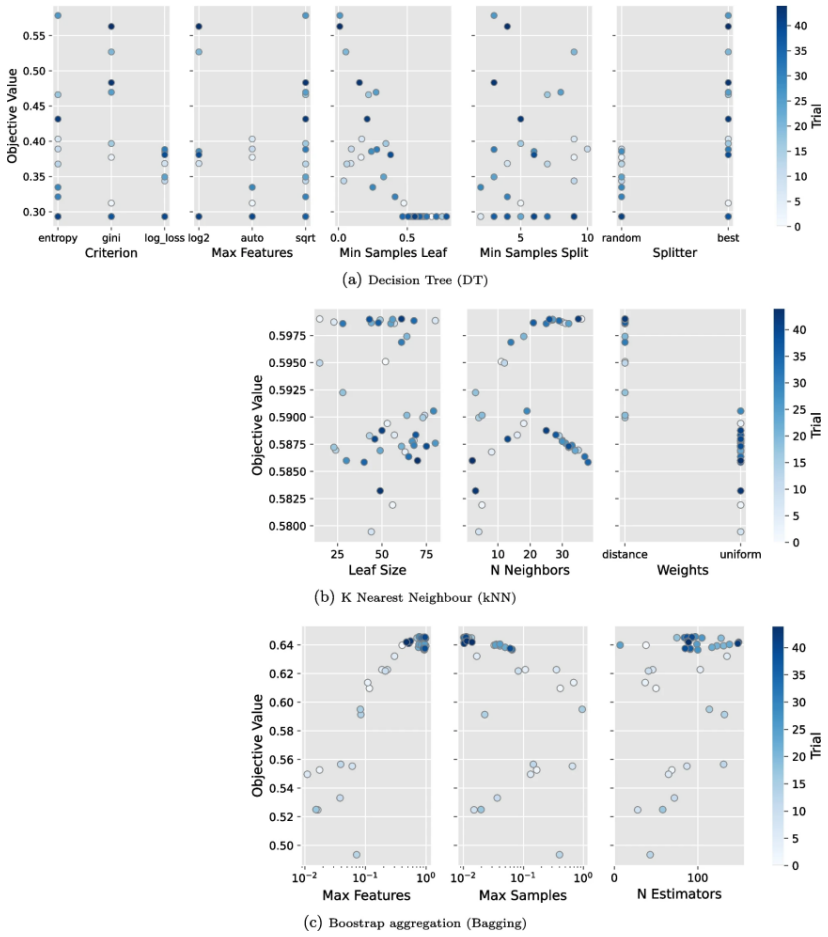

Fig. 1. Detection performance of the stacking model and baseline classifiers for gateway-level anomaly detection.

3.3 Feature Contribution and Interpretation Results

The SHAP results showed that repeated short connections, abnormal outbound byte rates, high

packet count variance, and failed connection ratio were the most important variables for detecting compromised gateway behavior. These features are reasonable in network security analysis. Repeated short connections often appear when botnets scan ports or test access points. A high outbound byte rate may indicate data leakage or abnormal forwarding from a compromised gateway. Packet count variance reflects unstable traffic bursts, which are common in flooding attacks and automated access attempts. Source port repetition also had a clear effect on unauthorized access detection. These results are consistent with recent explainable intrusion detection studies, which found that SHAP can help identify traffic variables that affect model decisions and make security alerts easier to review (Vaigandla, 2025; Zou et al., 2025). For blockchain-enabled IoT systems, this interpretation is useful because gateway alarms may be linked with audit records, smart-contract logs, or device trust updates.

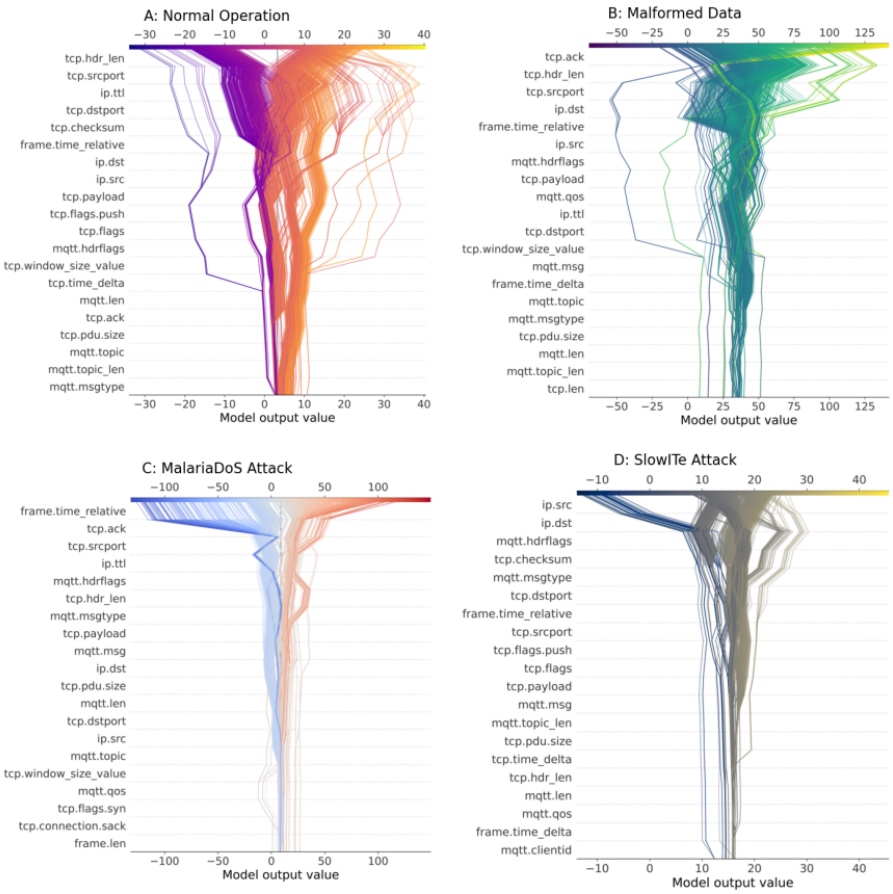

Fig. 2. SHAP feature importance for explaining abnormal gateway traffic classification.

3.4 Comparison with Existing Studies and Practical Value

Compared with earlier IoT intrusion detection models, the proposed method has three practical advantages. First, it uses gateway-level statistical features rather than device-specific raw payloads. This makes the method more suitable for mixed IoT networks. Second, the stacking design improves detection stability without using a large deep neural network. This is useful for gateway devices with limited memory and computing resources. Third, SHAP interpretation gives clear evidence for each alarm. This can support real-time blocking, manual review, and later security analysis. Existing explainable intrusion detection studies have shown that model interpretation is important for trust and security decisions, but many of them rely on complex black-box models and explain the results only after training (Gao et al., 2026; Michael, 2025). In contrast, this framework keeps the final decision layer simple while still using strong base learners. This design provides a better balance among accuracy, delay, and interpretability. The results indicate that stacking-based

explainable anomaly detection can be used as a practical security layer for blockchain-assisted IoT gateways, especially when traffic records, access control logs, and device trust scores need to be reviewed together.

4. Conclusion

This study developed an interpretable gateway-level anomaly detection method for blockchain-enabled IoT networks using a stacking ensemble model. Decision Tree, LightGBM, and K-Nearest Neighbors were used as base learners, and Logistic Regression was used as the final classifier. Experiments on the N-BaIoT and BoT-IoT datasets showed strong results in both binary anomaly detection and multi-class attack classification. The model achieved high accuracy, F1-score, and AUC, while reducing false positives and improving recall for low-frequency attacks compared with standalone LightGBM. These results show that the method can detect both common attacks and rare but harmful gateway threats. SHAP analysis showed that repeated short connections, abnormal outbound byte rates, high packet count variance, and failed connection ratio were the main signs of compromised gateway behavior. The main value of this study is that it combines accurate detection with clear feature-level explanation in gateway security monitoring. This design can support real-time traffic checking, alarm review, access control, and security auditing in blockchain-assisted IoT systems. However, the study still has several limits. The experiments were based on public datasets, and the model has not been tested in live IoT networks with changing device types, traffic loads, and attack strategies. Future work should test the method in real gateway environments, further reduce computing cost, and study its use with smart contracts and adaptive trust management.

Acknowledgments
We are grateful to all respondents who participated in this study.

References

1. Alalwany, E., Mahgoub, I., Alsharif, B., & Alfahaid, A. (2025). An Intelligent Ensemble-Based Detection of In-Vehicle Network Intrusion. Applied Sciences, 15(12), 6869.

2. Alharthi, A., Alaryani, M., & Kaddoura, S. (2025). A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems. Array, 26, 100406.

3. Alqaraleh, S. (2025). An Efficient Ensemble Network Anomaly Detection System for Cyber-Attacks. Engineering, Technology & Applied Science Research, 15(4), 25549-25554.

4. Alshehri, S. M., Sharaf, S. A., & Molla, R. A. (2025). Systematic review of graph neural network for malicious attack detection. Information, 16(6), 470.

5. Asaithambi, S., Nallusamy, S., Yang, J., Prajapat, S., Kumar, G., & Rathore, P. S. (2025). A secure and trustworthy blockchain-assisted edge computing architecture for industrial internet of things. Scientific Reports, 15(1), 15410.

6. Awasthi, A., Prajapati, A. K., Vediya, P., & Battula, R. B. (2026). TICNN—A Hybrid Light-Weight CNN for Large Imbalanced Multi-Class Datasets on Intrusion Detection System in IoT. IEEE Access, 14, 23413-23427.

7. Chen, F., Liang, H., Yue, L., Xu, P., & Li, S. (2025). Low-Power Acceleration Architecture Design of Domestic Smart Chips for AI Loads.

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

9. Ennaji, S., Benkhelifa, E., & Mancini, L. V. (2026). Vulnerability disclosure through adaptive black-box adversarial attacks in network intrusion detection systems: S. Ennaji et al. Complex & Intelligent Systems, 12(1), 18.

10. 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.

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

12. Khayer, B., Mirzaei, S., Alavizadeh, H., & Salehi Shahraki, A. (2025). Blockchain for Secure IoT: A Review of Identity Management, Access Control, and Trust Mechanisms. IoT, 6(4), 65.

13. 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.

14. Liang, R., Fan, F., Liang, Y., & Li, S. (2025). Constructing an Adaptive Optimization Model for Ribbon Recommendation and Interface for User Habits.

15. 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.

16. Michael, I. (2025). Visualization and Interpretability of Ensemble-Based Intrusion Decisions in SD-VANETs Using SHAP and LIME.

17. Qi, C., & Qiao, X. (2026). Efficient Data Sampling and Feature Selection Algorithms for Scalable Machine Learning Pipelines.

18. Salam, A., Shakir, A. T., Javaid, Q., Masini, B. M., Ahmad, M., & Wahid, I. (2026). Secure IIoT architecture with blockchain-enabled anomaly detection for water distribution cyber–physical systems. Scientific Reports.

19. Shao, W. (2026, March). Interpretable Ensemble Learning for Network Traffic Anomaly Detection: A SHAP-based Explainable AI Framework for Embedded Systems Security. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-4). IEEE.

20. Sharma, H., Kumar, P., & Sharma, K. (2026). Security Solutions for the Internet of Things Using Machine Learning and Deep Learning: Current Trends and Future Directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 16(1), e70059.

21. Singal, G., Rawat, M., Kumar, R., & Kushwaha, R. (2026). IoT Network Device Classification using Traffic Log by applying Machine Learning Techniques. IEEE Internet of Things Journal.

22. Su, D., & Zhang, H. (n.d.). Developing a Data-Driven Computational Framework for Scalable Special Education Practices for Autism and Intellectual Disabilities in the US Public School System.

23. Sultan, S. S., Ewieda, M., Gomaa, A., & Yahia, M. F. (2025). Enhancing Classification Accuracy Using Stacked Ensemble Learning: A Hybrid Ensemble Strategy. ALRYADA Journal For Computational Intelligence and Technology, 2(1), 1-24.

24. Vaigandla, K. K. (2025). An extensive examination on IOT and industrial IOT: Attacks, security, detection methods, blockchain solutions and challenges. Babylonian Journal of Internet of Things, 2025, 89-100.

25. Wang, Y., Chen, J., Arias, R., Wang, Y., & Yin, X. (2026). Development and Validation of a Patient-Friendly Digital Assessment Platform for Precision Screening of Oral Anti-Obesity Medications (AOMs).

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

27. Yang, J. (2026). Computational Analysis of How Digital Non-Clinical Communication Tools Influence Social Participation Among Older Adults in Community-Based Elderly Care. Available at SSRN 6682838.

28. Yin, J., Rao, H., & Huang, Y. (2026, March). Dynamic Modeling and Heterogeneity Analysis of Platform User Behavior Time Series. In 2026 International Conference on AI in Education Technology and Applications (AIETA) (pp. 30-33). IEEE.

29. Zhang, Z. (2026). A Study on the Identification of Manipulative Design in Subscription and Payment Interfaces of Digital Consumer Platforms and Its Behavioral Effects. Available at SSRN 6734760.

30. Zhang, Z., Tong, Y., & Gao, Y. (2026). Retrieval-Augmented Generation with Low-Latency Deployment for Vertical Domains Question Answering: A Case Study on Economic Resource Platforms.

31. Zou, Y., Qi, N., Deng, Y., Xue, Z., Gong, M., & Zhang, W. (2025, July). Autonomous resource management in microservice systems via reinforcement learning. In 2025 8th International Conference on Computer Information Science and Application Technology (CISAT) (pp. 991-995). IEEE.