Article

# Semantic Knowledge Graph Framework for Intelligent Threat Identification in IoT

Longxiang Yan , Qi Wang , Chang Liu *

Posted Date: 20 October 2025

doi: 10.20944/preprints202510.1489.v1

Keywords: knowledge graph; IoT security; graph embedding; semantic reasoning; threat identification

*Article*

# Semantic Knowledge Graph Framework for Intelligent Threat Identification in IoT

**Longxiang Yan [1], Qi Wang [2] and Chang Liu [3,*]**

[1] University of Pennsylvania, Philadelphia, USA
[2] Purdue University, West Lafayette, USA
[3] Washington University in St. Louis, St. Louis, USA
* Correspondence: chang.liu1@wustl.edu

## Abstract

This study proposes an intelligent threat identification method based on knowledge graphs to address the challenges of security threat detection, hidden attack chains, and complex feature associations in IoT environments. The approach first extracts key features from multi-source heterogeneous device communication data and constructs a knowledge graph containing devices, protocols, behaviors, and event relationships through semantic modeling to achieve global semantic association representation. A graph embedding mechanism is then introduced to vectorize entities and relationships, while an attention-weighted graph convolution structure is used to fuse and propagate multidimensional features, capturing the global dependencies of potential threat patterns. During the graph reasoning phase, the model enhances the interpretability of abnormal behavior detection through relational aggregation and semantic propagation, and finally employs a classifier to output threat probabilities, completing the entire process from knowledge representation to risk discrimination. Experiments on real IoT security datasets show that the proposed method achieves significantly higher accuracy, recall, precision, and F1-Score than traditional deep learning models. It effectively identifies complex attack behaviors and maintains strong robustness, demonstrating the modeling potential of knowledge graph structures in IoT security and providing a systematic solution for multi-source semantic fusion and intelligent threat detection.

**Keywords:** knowledge graph; IoT security; graph embedding; semantic reasoning; threat identification

## I. Introduction

The rapid proliferation of the Internet of Things (IoT) has made the vision of an interconnected world increasingly real. From smart homes and industrial control to urban transportation and healthcare, billions of devices now exchange data and collaborate intelligently through networks. However, the explosive growth in the number of devices and the increasing complexity of system architectures have intensified IoT security challenges. Due to limited device resources, diverse communication protocols, and complex deployment environments, traditional cybersecurity systems struggle to provide comprehensive and real-time protection. As a result, incidents such as malicious attacks, data breaches, and unauthorized access occur frequently. These issues not only threaten user privacy and system stability but also pose potential risks to critical infrastructure and social security, making it urgent to establish a new protection system capable of efficiently and intelligently identifying security threats [1].

In current security protection research, most methods rely on rule-based matching or feature-based machine learning detection. These approaches depend heavily on attack samples and expert-defined rules. Although they can be effective in specific scenarios, they struggle to cope with the complex and dynamic threats present in IoT environments. The interactions among IoT devices are highly dynamic and heterogeneous. Attack behaviors often spread through covert paths, exhibiting multi-source, multi-stage, and cross-layer characteristics. Traditional models tend to suffer from detection delays or high false-positive rates when faced with unknown threats or diverse attack strategies. At the same time, the existence of data silos and semantic fragmentation hinders information sharing and knowledge transfer among different devices, protocols, and platforms, further limiting the overall intelligence and coordination of security defense systems [2].

Knowledge graph technology provides a new perspective to address these challenges [3–5]. By semantically modeling multi-source heterogeneous information-such as IoT devices, communication protocols, behavior patterns, and security events-knowledge graphs can explicitly represent the relationships among entities within a graph structure [6]. This enables the construction of a comprehensive and inferable security knowledge system with global semantic understanding. Under this framework, security threats are no longer isolated events but can be interpreted as abnormal patterns in a multi-entity, multi-relation network [7–10]. Through semantic reasoning over device attributes, behavioral sequences, and communication paths, it becomes possible to reveal potential attack chains and abnormal propagation routes. This provides a solid semantic foundation for intelligent threat identification and early warning. Compared with traditional feature-based detection methods, knowledge graphs offer greater scalability and interpretability, allowing dynamic updates and adaptive learning in complex and evolving network environments [11].

With the deep integration of artificial intelligence, knowledge-graph-based threat identification has become increasingly intelligent and automated. By incorporating graph neural networks, relational reasoning models, and knowledge embedding techniques into security scenarios [12–14], it is possible to efficiently capture latent semantic patterns and structural dependencies within large-scale knowledge graphs. In IoT contexts, where attacks often exhibit stealth and chain-like characteristics, intelligent reasoning mechanisms can discover abnormal relationships even without explicit labels [15]. This enables early identification and continuous tracking of unknown threats. Such an approach not only improves the accuracy and timeliness of security detection but also provides transparent and interpretable support for security decision-making, promoting a shift from passive defense to proactive perception.

Overall, research on intelligent identification of IoT device security threats based on knowledge graphs holds significant theoretical and practical importance. It provides a cognitive framework that transitions from data to knowledge and from static to dynamic defense, advancing the semantic and intelligent evolution of IoT security systems. Moreover, it supports security governance in critical domains such as smart cities, industrial IoT, and vehicular networks, offering technical assurance for building a trustworthy, controllable, and sustainable IoT ecosystem. By integrating knowledge representation, graph reasoning, and intelligent perception, this direction is expected to drive the transformation from fragmented security detection toward global risk cognition, laying a solid foundation for the next generation of IoT security protection systems.

## II. Related Work

A broad spectrum of graph-based learning and semantic modeling methodologies forms the core of intelligent pattern recognition and reasoning in complex networks. Graph attention mechanisms have greatly advanced the ability to capture dynamic dependencies and selectively propagate feature information across large, heterogeneous relational structures, facilitating adaptive and interpretable knowledge modeling [16]. The use of heterogeneous network learning enables the discovery of implicit associations and multi-type relationships, supporting the fusion of diverse sources and hidden pattern mining [17].For robust anomaly detection and probabilistic representation, deep mixture density models offer powerful tools for learning uncertainty-aware representations from high-dimensional behavioral data, thus increasing detection accuracy and stability under challenging conditions [18]. Similarly, multi-head attention and semantic embedding frameworks enable context-aware representation learning, extracting complex temporal and structural dependencies essential for graph-based threat reasoning [19].

doi:10.20944/preprints202510.1489.v1

Distributed learning strategies—such as trust-constrained policy optimization and multi-agent reinforcement learning—underpin collaborative and resilient optimization in large-scale, multi-entity environments [20,21]. Meanwhile, structured path guidance and fast adaptation pipelines provide mechanisms for interpretable reasoning and rapid knowledge transfer, supporting scalable adaptation to new data and evolving patterns [22,23]. The integration of structured factor extraction and dynamic time-window modeling further enables context-aware prediction and semantic fusion in time-evolving environments [24].

Taken together, these methodologies—including graph attention, heterogeneous learning, probabilistic modeling, distributed optimization, semantic reasoning, and structured adaptation—establish the foundation for the knowledge-graph-based intelligent threat identification method developed in this work.

## III. Method

This study proposes a method for intelligently identifying security threats to IoT devices based on knowledge graphs. The overall framework includes four core components: knowledge modeling, graph embedding representation, relational reasoning, and threat identification. First, a semantically consistent security knowledge graph structure is constructed for multi-source heterogeneous device and communication data in the IoT environment. Device nodes, communication events, protocol types, and abnormal behaviors are abstracted into an entity set V, and their semantic associations are represented by edge sets E, thus forming a graph structure $G=(V,E)$. Each edge carries a semantic relationship $r_{ij}$, which defines the interaction semantics between devices. The overall relational structure can be expressed as:

$$G=\{(v_i,r_{ij},v_j)\,|\,v_i,v_j\in V,r_{ij}\in R\} \qquad (1)$$

To avoid semantic drift, a multi-layer feature fusion mechanism is introduced in the construction process to map network traffic features, system log features, and communication protocol features into the same vector space to form a unified structured knowledge representation. The overall model architecture is shown in Figure 1.

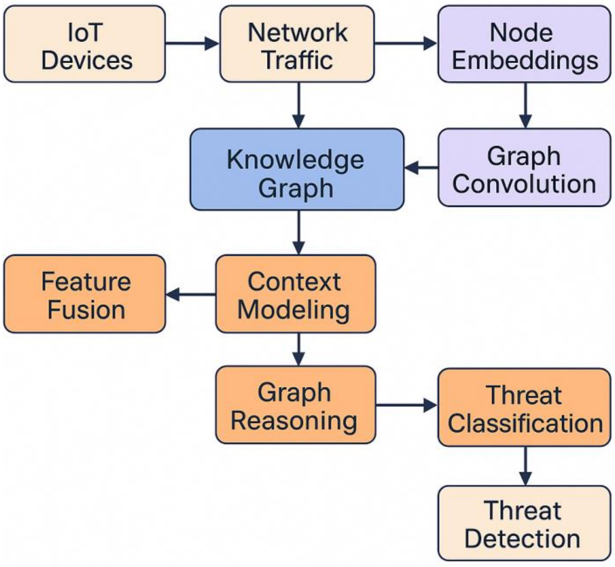

**Figure 1.** Overall model architecture.

In the knowledge representation stage, a low-dimensional vectorization method based on graph embedding is used to achieve computable modeling of devices and their interactive relationships. Given a device node $v_i$ and a relationship $r_{ij}$ , whose embedding vectors are $e_i$ and $r_{ij}$ respectively, the semantic consistency of the relationship triples is characterized by the energy function:

$$f(v_i, r_{ij}, v_j) = \| e_i + r_{ij} - e_j \|_2^2 \tag{2}$$

The smaller the energy function, the higher the semantic consistency of the triples, which reflects a more stable security interaction relationship between devices. To enhance robustness, this study further introduces contextual relationship modeling based on the attention mechanism, by calculating the importance weights of neighboring nodes:

$$\alpha_{ij} = Transformer(f(v_i, r_{ij}, v_j)) \tag{3}$$

This enables weighted aggregation of multi-dimensional relationships, ensuring that key security dependency structures are captured in complex network environments.

In the graph reasoning phase, to characterize the potential threat propagation paths between devices, a graph convolutional propagation mechanism is used to aggregate high-order features of the knowledge graph. The update method of the node representation at the lth layer is defined as:

$$P(y_i = 1 | h_i) = \frac{\exp(w^T h_i + b)}{1 + \exp(w^T h_i + b)} \tag{4}$$

Where $y_i = 1$ indicates that there is a security threat to the node, and w and b are learnable parameters. To optimize the overall recognition performance, the loss function adopts the weighted cross-entropy form:

$$L = -\sum_{i=1}^{N} [w_1 y_i \log P(y_i) + w_0 (1 - y_i) \log(1 - P(y_i))] \tag{5}$$

$w_1$ and $w_0$ are used to balance the ratio of positive and negative samples, respectively, to improve the sensitivity of identifying abnormal nodes. Through the above modeling and reasoning process, this research has achieved a complete link from knowledge graph semantic construction to intelligent reasoning and judgment, providing a unified cognitive framework and efficient semantic reasoning mechanism for security threat identification in complex IoT environments.

## IV. Experimental Results

### *A. Dataset*

The dataset used in this study is the TON_IoT (Telemetry, Network, and System Logs for the Internet of Things) dataset. It consists of real network traffic, telemetry data, and system logs collected from various IoT environments. The dataset covers multiple types of scenarios, including home IoT devices, industrial control terminals, and edge computing nodes. Its data sources include both normal communication records and several known attack behaviors, such as denial of service, data exfiltration, malicious scanning, and command injection. These features comprehensively reflect the security threats that IoT systems may face in real-world operations. The dataset also retains multi-level time series features, providing a solid foundation for dynamic modeling and behavioral pattern analysis.

In terms of structural design, the TON_IoT dataset includes three major components: network-level features, system-level logs, and device-level telemetry. The network layer records indicators such as protocol type, source and destination addresses, port numbers, traffic size, and session duration. The system layer contains user behaviors, access requests, and execution commands. The device layer telemetry reflects key operational parameters such as sensor readings, CPU utilization, and memory status. This multimodal and heterogeneous data structure provides rich semantic associations for constructing knowledge graphs. It enables the model to jointly learn potential dependencies among security events at both the entity and relational levels.

In addition, the TON_IoT dataset is large in scale and exhibits high diversity and representativeness. It has a high sampling frequency and a long time span, covering multiple stages from normal operation to complex attacks. This helps the model capture the evolution and propagation characteristics of threats during training. By leveraging this dataset, the study can effectively evaluate the adaptability and robustness of knowledge-graph-based security threat identification methods under complex, dynamic, and realistic IoT environments. It provides reliable data support for research on intelligent security protection systems.

### *B. Experimental Results*

This paper first gives the results of the comparative experiment, as shown in Table 1.

**Table 1.** Comparative experimental results.

| Model | ACC | F1-Score | Precision | Recall |
|---|---|---|---|---|
| **MLP [25]** | 0.871 | 0.862 | 0.856 | 0.868 |
| **CNN [26]** | 0.887 | 0.881 | 0.874 | 0.889 |
| **LSTM [27]** | 0.902 | 0.896 | 0.891 | 0.900 |
| **Transformer [28]** | 0.917 | 0.912 | 0.908 | 0.915 |
| **Ours** | 0.941 | 0.937 | 0.934 | 0.940 |

As shown in Table 1, there are significant differences in the performance of different models for IoT security threat identification. Traditional MLP and CNN models show relatively low accuracy and recall. The main reason is that they cannot model semantic relationships and contextual dependencies among devices. Although CNN achieves improvements in local spatial feature extraction, it still struggles to capture potential cross-device and cross-protocol interactions in heterogeneous data environments, which limits its detection capability. In contrast, LSTM performs better in time series modeling. It can capture the dynamic changes in IoT communication behaviors to some extent, resulting in higher performance across all four evaluation metrics.

The Transformer model further improves overall performance. By leveraging the self-attention mechanism, it effectively aggregates long-range dependencies between different devices and interaction events, making threat feature recognition more stable. However, Transformer mainly focuses on sequential feature modeling. It lacks explicit representation of multidimensional semantic relationships, making it difficult to interpret potential threat propagation paths and structural dependencies from a global perspective. In complex IoT environments, this sequence-centered representation still suffers from insufficient information coupling when dealing with multi-stage attacks and correlated event reasoning.

The proposed model achieves the best performance across all four metrics, indicating that incorporating a knowledge graph structure can significantly enhance semantic understanding and reasoning in security threat identification. By mapping devices, protocols, behaviors, and events into a graph structure, the model can identify not only individual attack behaviors but also reveal potential associations among different entities, thus capturing the full characteristics of attack chains. The joint design of graph reasoning and attention mechanisms allows the model to maintain high detection accuracy and robustness in complex environments, demonstrating the advantages and application potential of knowledge-driven threat identification frameworks in IoT security.

This paper also presents an experiment on the sensitivity of the learning rate to the single metric F1-Score, and the experimental results are shown in Figure 2.

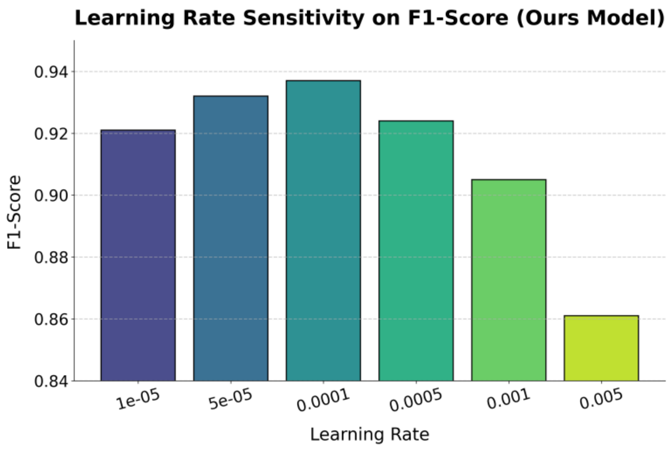

**Figure 2.** Experiment on the sensitivity of learning rate to F1-Score.

As shown in Figure 2, the learning rate has a significant impact on the model's performance in terms of the F1-Score. When the learning rate is low, such as between 1e-5 and 1e-4, the model maintains a high F1-Score. This indicates that a smaller learning rate helps the model achieve stable convergence during training, allowing it to capture the complex dependencies among devices, relations, and behavioral features in the IoT knowledge graph. At this stage, the model achieves a good balance between precision and recall, reflecting strong semantic reasoning and threat identification capabilities.

When the learning rate increases to 5e-4 or higher, the F1-Score drops significantly. A larger learning rate causes greater fluctuations in gradient updates, making it difficult for model parameters to find a stable optimum in the high-dimensional relational space. This affects the semantic consistency of the embedding representations. In particular, within a knowledge graph structure, the updating of relational and node features requires fine-grained step adjustments. An excessively high learning rate disrupts the balance between local and global semantics in the graph structure, weakening the reasoning layer's ability to characterize abnormal propagation paths.

Overall, the results show that the choice of learning rate is crucial for knowledge-graph-based IoT threat identification models. A moderate learning rate promotes coordinated optimization between the embedding layer and the graph reasoning module. It also helps prevent overfitting and gradient explosion in the early stages of training, ensuring the model's stability and generalization ability in complex and heterogeneous environments. This phenomenon further verifies the controllable sensitivity of the model to hyperparameters and the rationality of its structural design.

This paper also presents an experiment on the sensitivity of the number of attention heads to ACC, and the experimental results are shown in Figure 3.

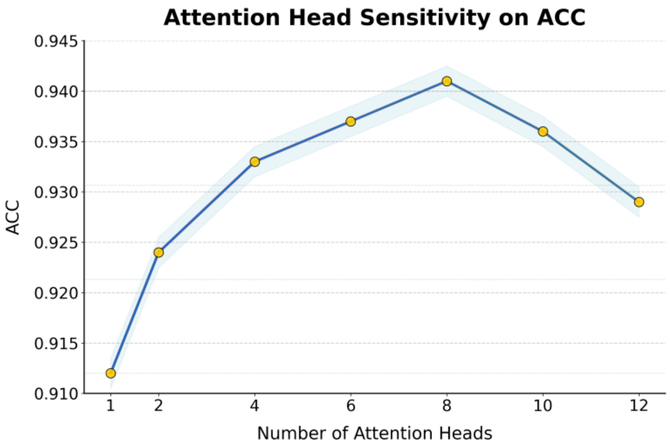

**Figure 3.** Experiment on the sensitivity of the number of attention heads to ACC.

As shown in Figure 3, the number of attention heads has a clear impact on the model's performance in terms of accuracy. When the number of attention heads increases from 1 to 8, the model's accuracy gradually improves. This indicates that the multi-head attention mechanism effectively enhances the model's ability to capture complex semantic dependencies among IoT devices. A moderate number of attention heads allows the model to learn different types of feature relationships in parallel across multiple subspaces, improving both the precision and robustness of threat pattern recognition. At this stage, the multi-entity and multi-relation structures in the knowledge graph are fully utilized, enabling a good balance between global reasoning and local feature modeling.

When the number of attention heads increases further to 10 or more, the model performance begins to decline. This may be due to excessive attention heads introducing feature redundancy and noise interference, causing the semantic aggregation process to lose focus on key relational nodes. An overly high attention decomposition dimension leads to a dispersion effect in the graph reasoning layer during feature fusion, reducing the efficiency of knowledge propagation. The results indicate that in knowledge-graph-based IoT security threat identification tasks, a proper setting of attention heads can balance representational power and computational complexity, thereby maintaining model stability and generalization performance.

## V. Conclusion

This study addresses the complexity and intelligence requirements of security threat identification in IoT environments and proposes an intelligent threat identification model based on knowledge graphs. The method constructs a knowledge graph structure from multi-source heterogeneous data to achieve unified semantic modeling of devices, protocols, and behaviors. By integrating graph embedding and graph reasoning mechanisms, it enables efficient identification of potential threat chains. Experimental results show that the proposed model outperforms traditional methods in accuracy, F1-Score, precision, and recall. These findings verify the effectiveness of knowledge-driven graph structure modeling in IoT security. The study not only provides a new theoretical framework for dynamic threat identification but also demonstrates unique advantages in interpretability, security visualization, and global risk understanding. It lays a solid technical foundation for building trustworthy and intelligent defense systems.

Future research can further expand the dynamic updating and cross-domain generalization of knowledge graphs. By introducing temporal graph learning, causal reasoning, and large-model-assisted inference mechanisms, the model's adaptability to unknown threats and emerging attack patterns can be enhanced. In addition, the deployment and migration strategies of the model in complex scenarios such as industrial IoT, vehicular networks, and smart cities can be explored. This will promote its application in real-time security monitoring and automated response systems. As the scale of IoT continues to grow and device intelligence advances, knowledge-graph-based security identification systems are expected to become a key technology for future network protection, providing continuous support for building a safer, controllable, and self-learning IoT ecosystem.

## References

1. T. Ngo, J. Yin, Y. F. Ge, et al., "Optimizing IoT intrusion detection—a graph neural network approach with attribute-based graph construction," Information, vol. 16, no. 6, 499, 2025.
2. R. Ranpara, S. K. Patel, O. P. Kumar, et al., "A computational framework for IoT security integrating deep learning-based semantic algorithms for real-time threat response," Scientific Reports, vol. 15, no. 1, 16794, 2025.
3. Y. Wang, Q. Sha, H. Feng and Q. Bao, "Target-oriented causal representation learning for robust cross-market return prediction," Journal of Computer Science and Software Applications, vol. 5, no. 5, 2025.

4. Q. Sha, "Hybrid deep learning for financial volatility forecasting: An LSTM-CNN-Transformer model," Transactions on Computational and Scientific Methods, vol. 4, no. 11, 2024.
5. X. Yan, J. Du, X. Li, X. Wang, X. Sun, P. Li and H. Zheng, "A Hierarchical Feature Fusion and Dynamic Collaboration Framework for Robust Small Target Detection," IEEE Access, vol. 13, pp. 123456–123467, 2025.
6. Q. Xu, "Unsupervised temporal encoding for stock price prediction through dual-phase learning," 2025.
7. M. Amjath, S. Henna and U. Rathnayake, "Graph representation federated learning for malware detection in internet of health things," Results in Engineering, vol. 25, 103651, 2025.
8. X. Yan, J. Du, L. Wang, Y. Liang, J. Hu and B. Wang, "The Synergistic Role of Deep Learning and Neural Architecture Search in Advancing Artificial Intelligence", Proceedings of the 2024 International Conference on Electronics and Devices, Computational Science (ICEDCS), pp. 452-456, Sep. 2024.
9. Y. Qin, "Hierarchical semantic-structural encoding for compliance risk detection with LLMs," Transactions on Computational and Scientific Methods, vol. 4, no. 6, 2024.
10. Y. Ren, "Strategic cache allocation via game-aware multi-agent reinforcement learning," Transactions on Computational and Scientific Methods, vol. 4, no. 8, 2024.
11. S. Ben Atitallah, M. Driss, W. Boulila, et al., "Enhancing internet of things security through self-supervised graph neural networks," Proceedings of the International Conference on Smart Systems and Emerging Technologies, Springer Nature Switzerland, pp. 186-197, 2024.
12. W. Cui, "Unsupervised contrastive learning for anomaly detection in heterogeneous backend system," Transactions on Computational and Scientific Methods, vol. 4, no. 7, 2024.
13. H. Wang, "Causal discriminative modeling for robust cloud service fault detection," , 2024.
14. Y. Wang, "Structured compression of large language models with sensitivity-aware pruning mechanisms," Journal of Computer Technology and Software, vol. 3, no. 9, 2024.
15. E. Gilliard, J. Liu and A. A. Aliyu, "Knowledge graph reasoning for cyber attack detection," IET Communications, vol. 18, no. 4, pp. 297-308, 2024.
16. A. S. Ahanger, S. M. Khan, F. Masoodi, et al., "Advanced intrusion detection in internet of things using graph attention networks," Scientific Reports, vol. 15, no. 1, 9831, 2025.
17. Z. Liu and Z. Zhang, "Graph-based discovery of implicit corporate relationships using heterogeneous network learning," Journal of Computer Technology and Software, vol. 3, no. 7, 2024.
18. L. Dai, W. Zhu, X. Quan, R. Meng, S. Chai and Y. Wang, "Deep probabilistic modeling of user behavior for anomaly detection via mixture density networks," arXiv preprint arXiv:2505.08220, 2025.
19. M. Gong, "Modeling microservice access patterns with multi-head attention and service semantics," Journal of Computer Technology and Software, vol. 4, no. 6, 2025.
20. Y. Ren, M. Wei, H. Xin, T. Yang and Y. Qi, "Distributed network traffic scheduling via trust-constrained policy learning mechanisms," Transactions on Computational and Scientific Methods, vol. 5, no. 4, 2025.
21. B. Fang and D. Gao, "Collaborative multi-agent reinforcement learning approach for elastic cloud resource scaling," arXiv preprint arXiv:2507.00550, 2025.
22. X. Quan, "Structured path guidance for logical coherence in large language model generation," , 2024.
23. W. Zhu, "Fast adaptation pipeline for LLMs through structured gradient approximation," Journal of Computer Technology and Software, vol. 3, no. 6, 2024.
24. X. Su, "Forecasting asset returns with structured text factors and dynamic time windows," , 2024.
25. S. Cherfi, A. Lemouari and A. Boulaiche, "MLP-based intrusion detection for securing IoT networks," Journal of Network and Systems Management, vol. 33, no. 1, 20, 2025.
26. S. T. Mehedi, A. Anwar, Z. Rahman, et al., "Dependable intrusion detection system for IoT: A deep transfer learning based approach," IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 1006-1017, 2022.
27. T. B. Ogunseyi and G. Thiyagarajan, "An explainable LSTM-based intrusion detection system optimized by firefly algorithm for IoT networks," Sensors, vol. 25, no. 7, 2288, 2025.
28. P. Wang, Y. Song, X. Wang, et al., "DIFT: A diffusion-transformer for intrusion detection of IoT with imbalanced learning," Journal of Network and Systems Management, vol. 33, no. 3, 48, 2025.

doi:10.20944/preprints202510.1489.v1

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.