Adaptive Memory Graph Transformer-Based Intrusion Detection for Secure Industrial Internet of Things

Dr. Sagar Dhanraj Pande[1], Deepak Gupta[2]

[1]Post-Doctoral Researcher, Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia; [2] Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia

[2]Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India

Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia;

Email ID: [1]sagarpande30@gmail.com, [2]myself.deepakgupta@gmail.com

---

Abstract: The rapid growth of Industrial Internet of Things (IIoT) devices has brought with it a heightened threat of cyberattacks in today's networks. In traditional IDS systems, they may not be effective in detecting new and emerging attacks, which hampers their effectiveness in real-world scenarios. To tackle this problem, this paper presents an Adaptive Memory Graph Transformer Intrusion Detection System (AMGT-IDS) based on the CIC IIoT Dataset 2025. The proposed model preprocesses the network traffic data and creates dynamic traffic graph representations to show the communication between IIoT devices. Important structural features are captured using a Graph Attention Network (GATv2) and traffic patterns and attack behavior are learned over time through a Protocol-Aware Transformer. This is then enhanced through the use of an Adaptive Memory Module to detect known and unknown attacks. The proposed model is evaluated using Accuracy(A), Precision(P), Recall(R), F1-Score(F1-S), MCC and AUROC. The experimental results indicate good performance (A of 99.2%, P of 99.0%, R of 98.9%, (F1-S) of 98.9%, MCC of 0.98, and AUROC of 0.99). The results confirm that proposed AMGT-IDS model can successfully detect cyber threats and offer reliable security solution to next generation IIoT network.

Keywords: IIoT, Intrusion Detection System, Cybersecurity, GATv2, Transformer, Adaptive Memory, Zero-Day Attack(ZDA) Detection, CIC IIoT Dataset 2025.

Introduction

IIoT is a vital technology of Industry 4.0 that connects manufacturing systems in order to allow real-time monitoring, automation, predictive maintenance, and efficient decision-making. From manufacturing to healthcare, transportation to energy, it has found its uses across a multitude of sectors, leading to a marked enhancement in operational efficiency and productivity. But as these IIoT systems became more connected, they have also presented significant cybersecurity challenges. Industrial networks are common targets for cyber attacks, which may lead to disruptions, cost, damage to equipment, and safety risks. This has made the protection of IIoT infrastructures a high priority for industries all over the world. IEDs are an important tool to detect malicious activity in industrial networks. While traditional IDS techniques are successful in identifying known attacks, they are unable to deal with unknown and evolving threats. One of the main problems is the ZDA, which target previously unknown vulnerabilities, and are not represented by any existing attack signatures. The advent of artificial intelligence and deep learning has demonstrated great promise in improving intrusion detection systems(IDS). However, the detection

of known and ZDA in dynamic IIoT environments continues to be an open research problem, as traffic is complex, network is heterogeneous and attack behavior is continuously changing. The CIC IIoT Dataset 2025 offers a realistic test bed for testing and assessing advanced intrusion detection technology. Hence, there is a need for intelligent, adaptive and scalable IDS frameworks to boost cybersecurity and enhance the resilience of next generation IIoT systems.

Related work

As the Industrial Internet of Things (IIoT) expands and cyberattacks have become more complex, IDS are playing a growing role in the security of IIoT networks. An early IDS usage method was signature and rule-based that depended on known attacks. These techniques, however, would not work well enough in dynamic industrial environments to detect unknown and ZDA. As AI, machine learning, deep learning, reinforcement learning, and federated learning techniques are becoming more advanced, they have found their way into enhancing performance of IDS in IIoT networks. Recently, Salah et al. [1] came up with a dual-model deep learning framework for Advanced Persistent Threat (APT) detection in IIoT networks, which relies on a consensus-based ensemble mechanism. In order to monitor the attacks related to botnets, Wamiq et al. [2] proposed a honeypot-based intrusion detection system (IDS) with ELK Stack. Akand and Rahman [3] proposed an Integrated Multi-Modal Ensemble (IMME) model for ZDA detection in IIoT. Priya et al. [4] proposed a Hierarchical RNN-based Multi-Agent Reinforcement Learning framework to deliver explainable industrial systems cyber defense. Gokul et al. [5] presented an AI-based proactive approach for intrusion detection and prediction system for secure Industrial IoT environments. Also, Singh et al. [6] came up with a Zero-Trust Agentic Federated Learning approach for IoT defense systems, and Arulmani et al. [7] proposed a privacy-preserving federated deep learning model for multi-class attack detection. In order to make the Industrial IoT (IIoT) more secure, Kurapathi [8] proposed an AI-based privacy-preserving optimization framework. Bakro et al. [9] presented a real-time intrusion detection method for forecasting traffic features of IIoT and operational technology networks. While these studies show considerable advances in IIoT cybersecurity, the problems of detecting increasingly sophisticated and ZDA and being adaptable in dynamic industrial environments remain.

Table 1. Comparison of the proposed method with existing studies.

Ref.	**Method; (Yes:Y, No:N)**	**ZDA Detection**	**AI-Based IDS**	**Adaptive Learning**	**Explainability**	**Real-Time Detection**
[1]	Dual-Model Deep Learning with Consensus Ensemble	Y	Y	N	N	Y
[2]	Honeypot-Based IDS with ELK Stack	N	Partial	N	N	Y
[3]	Integrated Multi-Modal Ensemble (IMME)	Y	Y	N	N	N

[4]	Hierarchical RNN-Based Multi-Agent Reinforcement Learning	Y	Y	Y	Y	N
Proposed AMGT-IDS	**GATv2 + Transformer + Adaptive Memory**	**Y**	**Y**	**Y**	**N**	**Y**

Major Contributions:

The main contributions of this work are :

1. Developed an intelligent intrusion detection framework for securing IIoT networks against cyberattacks and zero-day threats.
2. Integrated GATv2 and Transformer models to learn complex network traffic patterns effectively.
3. Incorporated an adaptive memory mechanism to improve the detection of evolving and previously unseen attacks.
4. Evaluated the proposed framework using the CIC IIoT Dataset 2025 under realistic industrial cybersecurity conditions.
5. Enhanced the reliability and robustness of intrusion detection for next-generation IIoT environments.

Methodology

The proposed Adaptive Memory Graph Transformer Intrusion Detection System (AMGT-IDS) aims at detecting known and zero-day cyberattacks in Industrial Internet of Things (IIoT) environment. The proposed framework has five main phases: Data Pre-processing, Dynamic Traffic Graph Building, Graph Based Feature Extraction, Temporal Pattern Learning, and Attack Classification.

Data Preprocessing

The CIC IIoT Dataset 2025 is initially preprocessed to enhance the quality of data and the performance of the models. The data is cleaned for missing values, duplicate records and irrelevant attributes. Normalization of numerical features is done using Min-Max normalization for the consistent feature scaling. Encoding techniques are used to convert categorical attributes into numbers. The processed data set is then split into respective sets.

Dynamic Traffic Graph Construction:

The preprocessed network traffic is mapped to dynamic traffic graphs to represent the communication relationships between the IIoT devices. All devices are displayed as nodes, and communication between devices is displayed as an edge. The graph structure is extended with network flow attributes, like source and destination address, protocol information, packet statistics, and traffic characteristics. This graph-based representation helps maintain the interaction patterns that exist in the IIoT network.

Structural Feature Extraction Using GATv2

Constructed traffic graphs are fed into Graph Attention Network Version 2 (GATv2). The attention mechanism gives different weights to the communications links and neighboring nodes in the model, allowing it to concentrate on important communications relevant to cyber threats. This stage mines the structural properties that are representative of both normal and malicious activities in a network.

Temporal Pattern Learning Using Protocol-Aware Transformer:

The structural features produced by GATv2 are passed to a Protocol-Aware Transformer. The transformer can analyze sequential traffic behavior and communication patterns of a protocol over time. The model also uses a self-attention mechanism to learn from long-range dependencies and temporal correlations, which could signal advanced attack activities.

Adaptive Memory Module

An Adaptive Memory Module is embedded within the framework to detect new and changing attacks better and more quickly. The memory component holds representative traffic patterns that have been learned during training, and continually adds to its knowledge as it receives observations. This mechanism is helpful to keep important information to identify known and unknown attacks and enhances the retention of the information in the model.

Attack Classification

The feature representations from the GATv2 network, the Protocol-Aware Transformer and the Adaptive Memory Module are enriched and fed into fully connected classification layers. The classifier is used to classify network traffic into normal or attack classes and then makes the final decision on intrusion detection.

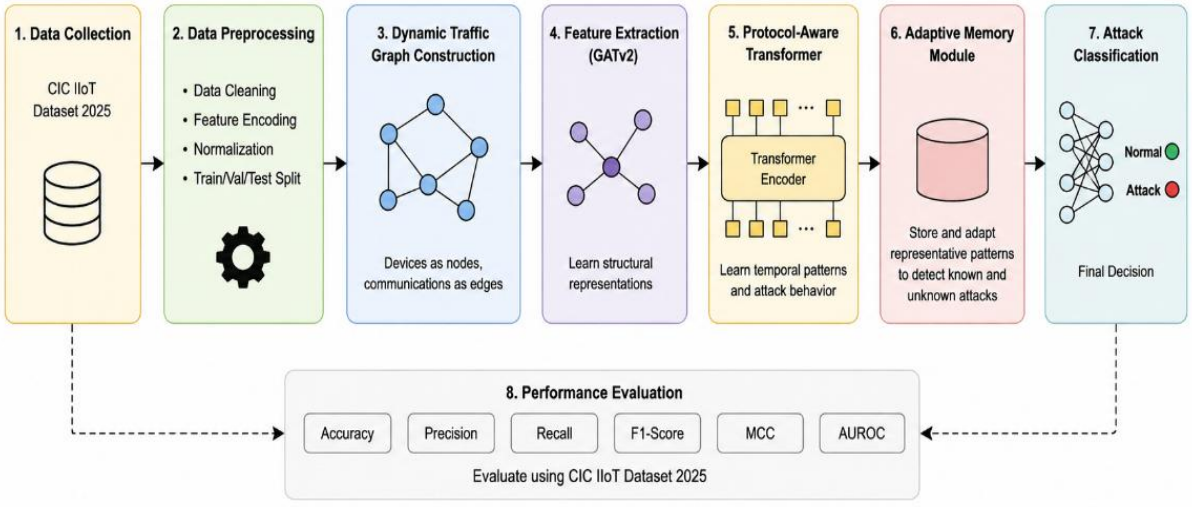

Figure 1: End-to-end architecture of the proposed AMGT-IDS for cyberattack detection

Conclusion

1.Problem Addressed:

IDS systems based on the traditional approach are facing challenges in detecting novel and emerging cyberattack activities in IIoT networks.

2.Method Used:

An Adaptive Memory Graph Transformer Intrusion Detection System (AMGT-IDS) has been developed using GATv2, Transformer and Adaptive Memory modules.

3.Key Findings

The proposed model performed well to detect attacks with 99.2% accuracy, and successfully classified both known and unknown attacks.In the future, the suggested improvements for this work are outlined as follows:

- The model was only tested with the CIC IIoT Dataset 2025.
- In the future, the deployment, testing using other datasets and making the model more efficient for resource-constrained IIoT devices will be the main focus of work.

References

1. A. H. Salah, A. Gomaa, T. Ogawa and H. M. Kasem, "A Dual-Model Deep Learning Framework With Consensus-Based Ensemble for Advanced Persistent Threat Detection in Industrial Internet of Things Networks," in IEEE Access, vol. 14, pp. 92980-93008, 2026, doi: 10.1109/ACCESS.2026.3704915.
2. M. Wamiq, P. Singh, R. Amonkar and R. Suryawanshi, "Intrusion Detection for Honeypot-Infested Networks Using Botnet-Based Frameworks with ELK Stack Integration," 2026 International Conference on Innovations in Computational Intelligence (ICICI), Ghaziabad, India, 2026, pp. 1-6, doi: 10.1109/ICICI68867.2026.11564875.
3. A. R. Akand and M. S. Rahman, "Integrated Multi-Modal Ensemble (IMME) for Zero-Day Attack Detection in IIoT," 2026 IEEE 2nd International Conference on Quantum Photonics, Artificial Intelligence & Networking (QPAIN), Chittagong, Bangladesh, 2026, pp. 1-6, doi: 10.1109/QPAIN69676.2026.11546448.
4. A. Priya, M. Arulmozhi, S. P. Santhoshkumar, S. U, R.Sowmiya and G. G. Kumar, "Hierarchical RNN-based Multi-Agent Reinforcement Learning for Explainable IIoT Cyber Defense," 2026 6th International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2026, pp. 1881-1886, doi: 10.1109/ICPCSN68523.2026.11543616.
5. A. Gokul, K. Silambarasan, S. Farook and M. Meganathan, "A Proactive AI-Driven Intrusion Detection and Prediction Framework for Secure Industrial IoT Systems," 2026 6th International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2026, pp. 1843-1848, doi: 10.1109/ICPCSN68523.2026.11543879.
6. S. K. Singh, J. Roy and M. So, "Zero-Trust Agentic Federated Learning for Secure Internet of Things (IoT) Defense Systems," 2026 IEEE 2nd International Conference on Secure IoT, Assured and Trusted Computing (SATC), Houston, TX, USA, 2026, pp. 1-10, doi: 10.1109/SATC69565.2026.11542411.
7. K. Arulmani, P. Krishnamoorthy, S. Arunkumar, P. Pandimeena, A. H. Kumar and M. Velusamy, "Privacy Preserving Federated Deep Learning for Multi-Class Attack Detection in Industrial

IoT," 2026 Fourth International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2026, pp. 1213-1220, doi: 10.1109/ICAISS68683.2026.11526137.

8. S. P. Kurapathi, "AI-Based Privacy-Preserving Optimization Framework for Secure Industrial IoT Systems," 2026 3rd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India, 2026, pp. 1-6, doi: 10.1109/RMKMATE69073.2026.11518731.
9. M. Bakro, A. Marotta, W. Tiberti, O. Odoardi, I. Salvatore and P. Di Marco, "Real-Time Intrusion Detection in IIoT/OT Networks Via Traffic-Feature Forecasting: A Testbed Study," 2026 IEEE 22nd International Conference on Factory Communication Systems (WFCS), Offenburg, Germany, 2026, pp. 1-8, doi: 10.1109/WFCS67029.2026.11511616.
10. K. Abinaya, T. Lohith and S. J. Kumar, "Enhancing Network Security with Intrusion Detection Systems in IoT Devices," 2025 5th International Conference on Expert Clouds and Applications (ICOECA), Bengaluru, India, 2025, pp. 320-325, doi: 10.1109/ICOECA66273.2025.00062