International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(14s) 2026 pp. 600-625
https://doi.org/10.70917/ijcisim-2026-4270
Article

Artificial Intelligence-Based Intrusion Detection Using Graph Neural Networks for Internet of Things Networks

Iqra Parveen

Birmingham city University, United Kingdom
Email: Iqraparveen0703@gmail.com

Abstract: Purpose: This work introduces a new network security paradigm called AI based intrusion detection system for IoT networks using Graph Neural Networks (GNNs) to improve their security. It solves the issue of many current IDS's that can be perceived as network traffic as discrete events, and lack the ability to detect relational, dynamic and hidden patterns of attack among IoT devices, flows and services.
Design/methodology/approach: The design of the study is quantitative research design, type of research is explanatory research and study design is cross sectional study. 510 respondents who know about IoT networks, cybersecurity, artificial intelligence, intrusion detection systems and IT security were included. The measurement model, the structural model, direct effects and mediating effects were assessed using PLS-SEM.
Findings:: The results show that the quality of the constructed graph of IoT networks, the ability of the GNN, the quality of the representation of the relation between the traffic items, and the optimization strategy for training the AI model have a positive and significant impact on the performance of IoT intrusion detection. The most significant direct effect was from the GNN model capability. The validity of the representation quality of relational traffic as a partial mediator was tested with regard to the three independent variables as well as in terms of the intrusion detection performance and as a complementary partial mediator.
Implications: It extends the graph theory, information processing theory and representation learning theory in the field of IoT cybersecurity theoretically. At a practical level, it assists in improving the design of graphs, the ability to model, the approach to optimization and the quality of the representation for cybersecurity managers, IoT engineers, AI developers, and network administrators.
Originality/value: This work is original because it emphasizes and clarifies how and why the quality of the representation of traffic in a relational model improves the safety of IoT systems while considering the relational representation of traffic as a key mediating mechanism.
Keywords: Artifical Intelligence, Graph Neural Networks, IoT security, Intrusion detection and Relational traffic representation and PLS-SEM.

1. Introduction

As the Internet of Things (IoT) networks expands rapidly, they have given rise to a large number of connected devices, vastly more communication flows and an even greater number of attack surfaces – all thwarting the traditional approach of signature-based and rule-based intrusion detection systems from being able to effectively defend against increasingly dynamic, distributed, and unseen cyberattacks. Recent studies demonstrate that an anomaly detection system with artificial intelligence can learn the complex traffic pattern and enhance the anomaly detection ability; however, most of the conventional machine learning and deep-learning based IDSs consider traffic log files to be independent samples and cannot model the relationships between the IoT devices, their traffic flows, services, and attack traces. To this end, Graph Neural Networks (GNNs) have been identified as a promising approach since they model an IoT network as a graph, where devices or flows are represented as nodes and their connections as edges in the graph, while the model learns the structural, temporal and relational attacks' patterns. Recent work on GNN-IDS shows that by incorporating information on network connectivity and the attack-graph, the uncertainty handling, explainability, and robustness of a graph-based model towards intrusions might be improved (Mohan et al., 2025). Similarly, multi-graph and attention-based GNN models have been proposed to enhance the detection accuracy at IoT/edge nodes, leveraging the fact that there are different communication patterns and that only the most relevant

neighbouring nodes (or traffic characteristics) are considered (Sayed et al., 2023). The other interest has been on lightweight and optimized GNN-based intrusion detection systems, which typically have limited computational resources in IoT devices, efficiency, scalability and real-time detection are all critical requirements. Recently, a number of systematic reviews have also validated the use of GNNs to combat malicious attacks due to its capabilities in representing non-Euclidean network data and enhancing the representation learning for anomalies (Sankaram et al., 2024). Recent research work in the areas of Bayesian graph-based IDS, dynamic graph-convolutional models, and federated graph learning also suggests that the existing research is trending towards developing more adaptive, uncertainty-aware and privacy-preserving IDS for IoT networks (Moghaddasi et al., 2025). Hence, in this study, the need to build an AI-driven framework for intrusion detection based on the GNNs that can effectively learn the relational IoT traffic patterns and enhance the performance of intrusion detection is discussed.

Along with the growing adoption of AI by guardrails for securing Internet of Things (IoT) networks, there remain challenges in the field of detection of sophisticated, dynamic and zero-day attacks, where most existing approaches assume network traffic are simply lists of records, rather than lists of relationships and interactions between devices, flows, services, and paths of attack. There are several recent studies that recognize that Graph Neural Networks (GNNs) are applicable to IDS, as they model IoT devices, flows, and dependency as graph structured data, but there is still no sufficient explanation about how the quality of a graph representation of the IoT traffic, the ability of the GNN, and the AI training/optimization strategy can combine and impact the performance of the IDS, which relies on the graph representation of the IoT traffic. Most of the previous studies reported have devoted their attention to the performance of their models (accuracy, F1 score, robustness, explainability, and others) without considering the theoretical explanation of the intermediate process between the conversion of raw IoT traffic relationships and the enhanced detection performance (López Delgado & López Ramos, 2024). Most of the studies are rather controlled experiments and benchmark data-based studies than deployment-oriented security validation in different IoT environments (including industrial IoT, healthcare IoT, smart energy and edge-IoT) yet the IoT network security sector lacks significant amount of real world data in the heterogeneous real world and resource constrained IoT environments. Recent reviews have highlighted the issues with the IoT intrusion detection research, including the volatility of traffic behavior, data unbalance, real-time scalability and lightweight deployment, explainability, privacy and domain and sector generalization (Razaque et al., 2025). Additionally, although there are some signs of progress in empirical studies on spatio-temporal GNNs (Swamy & Sophia, 2025), optimized multi-channel GNNs (Araújo et al., 2025), federated GNNs (Akanksha & Naik, 2025), and explainable graph-based IDS (Rahmani et al., 2024), this evidence is fragmented and does not fully leverage and evaluate the interplay between graph construction, GNN architecture, and optimization strategy to enhance the performance of relational traffic representation and consequently intrusion detection in practical IoT network environments. Thus, in this research, we filled the theoretical gap by explaining the mediating role of relational representation quality of traffic and validated the GNN intrusion detection in targeted IoT network security area, to fill up the empirical gap.

Though recent research has acknowledged that Graph Neural Networks (GNNs) are a good fit for intrusion detection in IoT networks since they can model the relations among IoT devices, flows and communication dependencies as graph structured data, little explanation exists in the literature on how the quality of the graph construction for IoT networks, the capability of the GNN, and the AI training and optimization process interact to impact the quality of IoT network graph-based representation of relations and, in turn, the performance of intrusion detection in IoT networks. Existing studies have largely concentrated on the model performance measures such as accuracy, F1-score, robustness and explainability of the proposed models without a proper theory, which explains the underlying mechanism in which the graph-based representation learning can transform the relationship between the various raw IoT traffic elements in order to improve the detection results (Abirami & Palanikumar, 2023). In practice, the IoT network security sector still lacked a significant amount of practice-oriented and deployment-oriented data to validate network security in the heterogeneous real-world and resource-constrained IoT environments (such as industrial IoT, healthcare IoT, smart energy IoT and edge-IoT) other than benchmark data based studies and controlled experiments. In recent reviews, most of the challenges aforementioned have been experienced in ongoing studies on IoT intrusion detection, which have left all challenges unaddressed (Alkhafaji et al., 2025). Moreover, recent empirical research on spatio-temporal GNNs, optimized multi-channel GNNs, federated GNNs, and explainable graph-based IDS presents some encouraging results; however, these results are fragmented and did not test the interplay between constructing a graph, GNN architecture, and optimization approach with the goal of improving relational traffic representation and, ultimately, intrusion detection performance in relevant IoT networking environments with suitable experiments and studies (Singh et al., 2025). As such, during this study, the theoretical void (the need for the explanation of the role of RT as an intermediary variable) and the empirical void (the need to validate the GNN-based ID in the targeted IoT network security sector) are considered.

Overall, the significance of this study is that it explores the potential of graph-based AI to enhance intrusion detection in IoT networks to tackle complex and ever-evolving cyber threats. The general goal of the study is to analyze how the quality of the way the graph is constructed in an IoT network (IoT-GQ), the capability of the GNN model (IoT-GNC), and the use of AI training and optimization strategy (IoT-AIOSS) affects the performance of IoT intrusion detection (IoT-ID), while the quality of the representation of the relationships between the objects (IoT-GRRQ) plays a mediating role. The objective is to provide a more meaningful graph representation of potential traffic relationships with IoT applications to facilitate more accurate, scalable, explainable and adaptive cyberattack detection. As the number of heterogeneous devices in IoT and IoT-edge grows, along with the dynamic nature of the traffic they process because of their mission-critical applications, limited resource availability, and stringent real-time constraints, AI-driven and GNN-based ID approaches are becoming more and more relevant and essential (Makhmudov et al., 2025). The study is useful to the management field as it helps in the governance of cybersecurity, management of operational risk, planning of response to incidents and planning of business continuity as well as Evidence based investment decisions of various technologies in the field. In the era of IoT, security managers have to rely on trusted security intelligence to prioritize threat and risk, allocate security resources, protect digital assets and gain trust from and among stakeholders and especially in critical infrastructures such as energy, smart cities, industrial IoT, and health care sectors that are prone to cyber incidents. AI's role in improving managerial decision-making processes is also becoming an area of significant research and development interest, as is the use of explainable AI, AI support for managerial decision-making and intelligent cybersecurity risk management approaches.In recent times, other research has shown potential for AI to support managerial decision-making processes and create more actionable, transparent, and security-strategy-driven threats, including explainable AI, AI-driven decision support, and intelligent cybersecurity risk management (Taherdoost et al., 2025). This study is therefore intended to further technical understanding of intrusion detection using GNN for IoT as well as to offer management relevant knowledge on designing a secure, adaptive and strategically governed IoT cybersecurity system.

This research is novel because it aims to develop an integrated explanatory model of how the quality of the construction of IoT network graphs, the capabilities of the GNN models, and the way that the AI is trained and optimized through a mediator variable for relational traffic representation quality (RRQ) influences IoT intrusion detection performance. While some studies recently have suggested GNN based, multi-graph, attention-based, optimized and federated models for IDS in IoT and edge environments, the majority of them primarily focus on the technical performance metrics such as accuracy, F1-score, robustness, explainability, and computational efficiency without giving any clarity to the internal mechanism on how GNN based learning enhances the detection performance (Chakraborty et al., 2023). Moreover, recent reviews also reveal that the research on AI for IoT cyber security has several unresolved issues on how to model the graphs of IoT devices, how to model dynamic traffic, how to handle heterogeneity, how to deploy it with limited resources, privacy issues, explainability and generalization across the IoT sectors (Bajpayi et al., 2025). Therefore, this paper is innovative because it does not only measure the performances of GNN models, this paper will include an explanation of the relationship between the graph design, the capability of the GNNs, training strategy, and the detection results: The mechanism is called relational traffic representation quality. It is also a more comprehensive theoretical and empirical contribution to the IoT network security field with insights into the management that can be used to select, optimize and manage AI-based IDSs in large and complex IoT applications.

Graph Neural Networks (GNN) are well suited for IoT networks intrusion detection (IDS) because of the Internet of Things (IoT) and Industrial Internet of Things (IIoT) are rapidly growing and bringing many devices in the network together, and the creation of smart cities, IoT in healthcare, and critical infrastructure.There is a need to research the Artificial Intelligence (AI) based Graph Neural Networks (GNN) for Intrusion Detection in the IoT networks to consider the many devices that are connected with each other in IoT networks and Industrial Internet of Things (IIoT), smart cities, IoT networks in healthcare, and critical infrastructure networks. Other IoT security solutions that are already available to the market have several problems that are crucial to the modern IoT application such as dynamic traffic behavior, zero day attacks, heterogeneous devices, imbalanced datasets, real time processing, and the explainable decisions (Asim et al., 2023). This study is noteworthy as GNNs can represent networks of IoT devices as graphs and learn relationships that exist in the network even though they are not immediately apparent from the individual traffic records (Talukder et al., 2024). Moreover, in recent times the critical need for lightweight, explainable, adaptive and real-time intrusion detection models applicable to IoT and IoT-edge environments with resource constraints and security governance/operational decision-making have been emphasized (Koshkin et al., 2025). Thus, this study is significant, technically, as it clarifies how the quality of the representation of relational traffic in the graph affects the performance of intrusion detection systems when an IoT-based network is utilized to detect it; and managerially, because it can be utilized to optimize resources, to respond to cybersecurity incidents, to ensure

business continuity, or to design and execute a cybersecurity strategy to protect an organization's assets when an IoT-based network is involved.

The study is valuable for its contribution to the growing body of knowledge on the application of the AI techniques with intrusion detection and the use of graph based learning to increase the security and resilience of IoT networks. The contributions of the research are both theoretical and practical: It extends the knowledge on graph construction quality for the IoT, the capability of the GNN, the strategy of using it for training AI models, the quality of the representation of the traffic in relational networks and the performance of intrusion detection in IoT. It contributes to advancing the scientific research in the IoT and IIoT domains by offering empirical proof of the implementation of intrusion detection system based on GNN to tackle the current challenges in IoT/SIIoT cyber security such as heterogeneous traffic, dynamic attacks, real-time detection requirements, resource constraints, explainability and deployment feasibility (Sokkalingam & Ramakrishnan, 2022). The study is also practical importance it gives guidelines on designing more accurate, adaptive and reliable intrusion detection system, which can learn hidden relationship of IoT device, flows and attack path becomes important as people are starting to use graph learning and AI based security models for the IoT network traffic analysis and cyber defense (Vardakis et al., 2024). The users of this study are academic researchers who can rely on the model to improve their theory and future empirical studies, cyber security research and practitioners who can apply the model to strengthen their threat detection and incident response capability, IOT system developer who can apply the model to design more secure architecture for IOT systems, organizational managers who can use the model to make better decision on the cyber security investment and risk governance in IOT systems, and policy makers and regulators who can rely on the model to strengthen their IOT security guidelines. As such, the study has both academic value and practical value, as it brings to a fusion between technical innovation in AI and managerial decision-making and cyber security defence in the context of IoT.

The relationship between the quality of the IoT network graph, the capability of the GNN model, the IoT AI training and optimization, the quality of the graph-based representation of the IoT traffic, and/or the performance of IoT ID could be interesting to study as they represent the whole process that the OAI undergoes to use raw IoT traffic and its network behavior as the base for a valuable decision that will be taken regarding the security of the IoT network. There were previous studies investigating related aspects of these relationships – such as by learning complex relationship in IoT traffic using GNNs (Gan et al., 2023); using optimized and multi-channel graph models to boost detection accuracy (Alrayes et al., 2023); leveraging spatio-temporal and attention-based architectures to learn dynamic attack behavior (Menon et al., 2023); and representation learning to enhance detection results (Taneja & Kumar, 2024). However, the novelty of this study is that these variables are not handled technically independently but as an integrated relationship model, which affects the detection performance based on the relational traffic representations learned from the IoT communication patterns and the performance of the model itself and the training strategy. It is important because recent studies have shown that the interactions between devices, flows and attack paths are non-linear, heterogeneous, dynamic and graph-based, and that increasingly more IDS mechanisms are based on these interactions.It is important since it has been proven by recent studies that interactions among devices, flows and attack paths are all non-linear, heterogeneous, dynamic and graph-based, and that more and more IDS mechanisms rely on such interactions. In this respect, the study of these relationships is valuable since it not only informs whether the use of GNN-based intrusion detection enhances the security of IoT, but also the mechanism and reasons behind this enhanced security, as the results demonstrate graph-based representation learning, which makes the study theoretically meaningful, empirically relevant, and practically applicable to IoT cybersecurity management (Rampone et al., 2025).

In this research, relational traffic representation quality is investigated as a mediator between relational traffic representation and the performance of AI based intrusion detection system with graph neural network (GNN). In particular, the study aims to investigate the relationship between the quality of the IoT network graph construction and the quality of the representation of the relational traffic, the relationship between the quality of the GNN model and the quality of the representation of the relational traffic, the relationship between AI training/optimization strategy and the quality of the representation of the relational traffic, the relationship between the quality of the representation of the relational traffic and the performance of the IoT intrusion detection, and whether there is a relationship between the quality of the IoT network graph construction and the capability of the GNN model, mediated by the quality of the representation of the relational traffic. These objectives are aimed at providing a meaningful vision on how the use of graphs can improve the intrusion detection in IoT networks, by giving operational penetration tests a meaningful representation of the relationships between the different types of devices, flows and attacks, to guide their decision making (Čisar et al., 2022).

2. Literature Review

2.1 Theoretical Foundation

The theories behind the quality of IoT network graph is rooted in Graph Theory and Network Science, which has illuminated that graph nodes, graph edges, graph paths, graph clusters, centrality and connectivity patterns can provide an understanding of complex systems. In the current study, each IoT Device, each communication between devices, each protocol, each each service, etc. will be treated as a graph element and it will be determined how well the graph is constructed, since how accurate the graph is to the actual structure of the network makes it useful and useful. Theoretically these can be explained by the concept of cyberattacks in IoT networks are relational activities, that pass through communication channel and connected devices. Recent research on graph based IDS for IoT networks (Kamruzzaman et al., 2024) indicates that representing the devices as graphs is appropriate for IoT networks to capture the dependency and flow between the devices and the structural behavior of attacks. Therefore, the quality of the graph constructed is intrinsic and important as a foundation for meaningful cybersecurity patterns to be learnt on.

The theoretical underpinning for the ability of GNNs and AI Training and Optimization is guided by Relational Learning Theory, Representation Learning Theory, Statistical Learning Theory and the notion of Relational Inductive Bias. This paper argues that: Relational Learning Theory proposes that models are more likely to work if they learn from relationships between entities, as opposed to learning one observation at a time; Relational Inductive Bias suggests that GNNs are a good fit for IoT intrusion detection because they learn neighborhood aggregation and message passing from graph-structured dependencies. Along with that, Representation Learning Theory offers the principles of allowing deep learning to automatically extract useful features, be they simple or sophisticated, from the data; and Statistical Learning Theory offers justification for training and optimization in terms of avoiding overfitting, minimizing prediction error and generalizing well. There have been recent advances in intrusion detection using GNNs, with studies showing that an optimized model, which has focused on the attention mechanism, spatio-temporal channels, and federated and multi-channel approaches is well suited for learning complex IoT traffic patterns especially in heterogeneous, dynamic and resource constrained environments (JS et al., 2024). Thus, the learning, adapting and optimizing of the AI training strategy, and graph capability of the model, is justified from a theoretical perspective because these aspects affect the effectiveness of the system to learn, adapt and generalize from the graph-based IoT traffic.

The theoretical basis for the relational traffic representation quality and the intrusion detection of the IoT system is a Representation Learning Theory, Information Processing Theory, Signal Detection Theory and Socio-Technical Systems Theory. Relational traffic representation quality is the mediator in the above-mentioned process because it understands how a graph is built, a GNN's capability is converted to useful learned representations, and how these learned representations are converted into separating normal and malicious IoT behaviors (Mehta, 2025). It asserts that, in order to enhance security decisions, it is essential to have high-quality representations that support more accurate classification, anomaly detection and generalization, which is supported by Representation Learning Theory, and can be explained by Information Processing Theory as the improved representation of raw information from the network into meaningful knowledge. In Signal Detection Theory, there is a justification of the dependent variable, as it considers the performance of intrusion detection in terms of the correctly detected pattern (attack and normal traffic) for the purpose of reducing false positive and increasing true positive, as well as improving detection reliability. The nature of IoT intrusion detection is also a socio-technical issue that plays an important part in the management aspect enabling the study, which is an organizational effort involved in governance, risk management, incident response and operational continuity in cybersecurity. It is important that explainable, adaptive, and real-time Intrusion Detection play a fundamental role in practical cybersecurity decision making for IoT, IoT-edge, and Industrial IoT (IIoT) systems and IoT Cyber Physical Systems (ICT) according to recent Researches (Huo et al., 2025). From this point, the theoretical framework of this study has demonstrated that the key issue to address in order to extend the performance of the IoT intrusion detection system into an AI-enabled system is the representation of traffic as a graph.

2.2 Hypotheses Development

H1: IoT network graph construction quality has a positive and significant effect on IoT intrusion detection performance.

The quality of the construction of the IoT network graph is expected to enhance the performance of IoT intrusion detection, based on the manner in which an IoT application transforms an IoT application into the graph form to accurately represent the interactions between the various devices, communication flows between the application

components, services offered by the app at each of the devices, and the paths in which the attack progresses. The nodes, edges, attributes and time information are exploited for abnormal behaviour detection in the context of GNN-based intrusion detection.For intrusion detection using GNN, nodes, edges, attributes and temporal tie are the base of detecting abnormal behavior. Recent studies have shown that a graph-based IDS approach is more effective if traffic records are not viewed as independent events, but instead, network connectivity, traffic flow dynamics, and attack information (such as attack-graph) are considered (Kushwaha & Tiwari, 2025).

When the weak graph structure doesn't have the capacity to recover some of the important relationships between the IoT devices, it can produce incomplete or noisy inputs and can contribute to inaccuracy in detection and high false alarm rate. With a well-constructed graph on the other hand, the model will be able to include structural and temporal relationships that are useful to identify hidden attack patterns in IoT networks. So, it has been proved in the most recent studies on IoT/IIoT (Yang et al., 2025) that the construction of better graphs results in better intrusion detection performance in such a heterogeneous and dynamic network environment.

H2: GNN model capability has a positive and significant effect on IoT intrusion detection performance.

The GNN model capability is expected to have a positive impact on the performance of intrusion detection when dealing with IoT traffic data since the architecture dictates the learning capability of the model from graph structured IoT traffic data. The advanced GNN models, such as GCN, GAT, spatio-temporal GNNs, multi-graph GNNs and hybrid GNN+transformer models, can be used for learning complex relationships between flows and IoT devices. Such models are able to combine neighborhood information, to learn structural dependencies and detect abnormal communicational patterns, which are not captured by regular machine learning models (Gummadi et al., 2024).

These capabilities also impact the robustness, scalability, explainability and the distinguishing ability of the GNN for normal and malicious traffic. The model includes attention mechanisms, temporal learning and multi-channel graph processing, which ensures that it only considers the relevant nodes, flows and attack paths, eliminating irrelevant noise. However, in recent years, there are some optimised and explainable GNN-based IDS research studies that indicate that better accuracy, F1 score, adversarial robustness, and real-time applicability of the GNN-based IDS in the IoT and edge environments are achieved with the improvement of the GNN architectures (Sumathi & Rajesh, 2023).

H3: AI training and optimization strategy has a positive and significant effect on IoT intrusion detection performance.

How the quality of the training data affects learning attack patterns, handling data imbalances, reducing overfitting, and generalizing across attacks are likely to be crucial aspects of the effectiveness of the IoT intrusion detection strategy in the future, with the effectiveness of the training strategy being expected to have a significant impact on these factors and other metrics. Hyperparamater optimization, feature selection, semi-supervised learning, self-supervised learning, autoencoder pretraining, knowledge distillation, federated learning, and adversarial training are some of the techniques that helped with ID in the IoT. Recently, the results of detection have been reported to be improved by optimized training approaches, including the stabilization of training, reduction in computational complexity, and unconstrained deployment with limited resources (Cherukuri et al., 2024).

This relationship becomes significant due to the dynamism, heterogeneity and the presence of zero day and evolving cyberattacks in the IoT networks. For some models, optimization might not be an appropriate approach, and they may also perform well on a benchmark dataset but not on real IoT applications. Training and optimization can increase detection accuracy, decrease the false positives, increase latency, and aid in scalable IDS deployment. From the aforementioned reviews, it can be observed that there is still an unmet need to improve the lightweight learning ability, explanation and generalization across different IoT contexts of AI-based IDS for IoT systems (Son et al., 2024).

H4: Relational traffic representation quality has a positive and significant effect on IoT intrusion detection performance.

The quality of representing relational traffic is expected to be a positive impact on IoT intrusion detection performance as the quality of learned traffic representation affects the ability for the system to distinguish between normal traffic and malicious traffic. Hidden correlation between the different devices, flows, services and attack paths are part of the relationship models in a GNN-based IDS. In contrast to the standalone traffic features, these representations also offer a deeper understanding of the characteristics of IoT attacks, which are mostly based on the interactions between traffic features (Alghamdi, 2022).

Misrepresentation of traffic from a relation makes detection of an attack more challenging.A good representation of relational traffic will ensure the noise is minimized, increase the separability of classes and maintain the structural and temporal characteristics of the IoT attack. When learned embeddings are definitely associated with normal vs abnormal behavior, IDS can improve accuracy, recall, precision, F1 score and robustness. The research research for a spatio-temporal GNN, optimized GNN and latent-attention IDS models confirm that representation learning is a key element in improving detection performance in IoT and industrial cyber networks (Dubey et al., 2025).

H5: IoT network graph construction quality has a positive and significant effect on relational traffic representation quality.

The quality of the graph created for the IoT network is supposed to have a positive impact on the quality of the representation of relational traffic, since the graph is the input structure used to learn embeddings from. The model is able to learn more meaningful relational patterns as long as the graph is a true representation of devices, flows, attributes, temporal sequences and communication dependencies. Example, recent works consider modeling IoT traffic as communication graphs, provenance graphs, knowledge graphs, or spatio-temporal graphs, which helps in capturing the dependencies that are not apparent on traditional tabular data (Ma et al., 2024).

This has also been supported graph theory which states that relationships between entities are important and the information in the entities models the behaviour of the system. Cyberattacks on networks are more likely to occur within interactions between devices, not a single traffic event within the IoT networks. Thus, a good graph will have a good representation in terms of the network structure, traffic context and attack-routes. The importance of structural quality of the graphs towards effective cybersecurity representations on the graph is highlighted (Shen et al., 2024).

H6: GNN model capability has a positive and significant effect on relational traffic representation quality.

The capability of the GNN has the potential to positively influence the quality of the representation of relational traffic: the capability of the GNN is directly related to the capability of processing graph-structured traffic. Different GNN architectures have different types of aggregation, attention, propagation, and temporal learning and feature-fusion mechanisms. More complex GNNs can be used to capture relationships between nodes and flows both globally and locally within the IoT system, which will include more complex representations of normal and malicious behaviour. In addition, a recent study also demonstrates that multi-channel GNNs, graph attention models and spatio-temporal GNNs work well in recognizing complex and dynamic relationships in IoT intrusion detection systems (Cheng et al., 2023).

The quality of representation relies on the data from the graph as well as how the model deals with the graph. A strong GNN can generate more discriminative embeddings, but a weak GNN can't.A weak GNN might not take into account the significant neighborhood impact, extended dependencies, alongside the temporal attack evolution. Recently, optimized and explainable GNN based intrusion detection models were also shown to have superior feature learning, robustness, and interpretability in the field of IoT cybersecurity, as shown by Al-Amiedy et al. (2022) , Zivkovic et al. (2022), and Kunaparaju (2025).

H7: AI training and optimization strategy has a positive and significant effect on relational traffic representation quality.

Last but not least, the formulation and optimization of the representation of relational traffic in this system is also expected to be enhanced by the neural network's training and optimization strategy, as it will impact the learning of meaningful patterns from the traffic generated by IoT. Techniques such as Autoencoder pretraining, Semi-Supervised learning, Self-supervised learning, Contrastive learning, Feature selection, Federated learning and Hyperparameter optimization can be used to reduce the noise and its effect on the system, build good generalization and increase the separation between classes to enhance latent representations. Our results show that autoencoder pretraining, self-supervised graph learning, and semi-supervised knowledge-graph approaches can result in better representation learning for intrusion detection, as shown in recent work (Perumal et al., 2023).

The relationship is important because in IoT environments limited, unbalanced and context-dependent attack data exists. The model might be learning biased or poor representations if it is not trained and optimised correctly, which will result in good results only in the training datasets. Optimization improves the quality of embeddings learnt, making them more robust, transferable and attack normalizing. Recently, the market has seen a surge in the number of IDSs based on artificial intelligence (AI), a requirement emphasized in various studies for AI-based system optimization, light weight, explainable and cross-domain generalizable (Darla & Naveena, 2024).

H8: Relational traffic representation quality mediates the relationship between IoT network graph construction quality and IoT intrusion detection performance.

To prevent this, we hypothesize that the quality of relational traffic representation (RTRQ) is in between the quality of IoT network graph construction (INGCQ) and the detection performance of the IoT intrusion detector model as better construction of an IoT network graph will ease the learning of better relational representations which in turn will boost the detection performance. High quality graph does not necessarily have the ability to detect attacks, and one of its aims is to make the structural and contextual information accurate to create meaningful representations of traffic. What our recent GNN-IDS works have shown is that connectivity, attack path and connection-oriented attributes like static features and dynamic features of traffic are helpful for graph-based intrusion detection (Saba et al., 2022).

Results show that the overall detection performance, given the quality of the graph construction, takes place in part through the learned representation of the quality of the traffic in the relations. With a good graph, the embedding will be more likely to classify normal traffic as normal and malicious traffic as malicious, aiding detection performance. Even though the graph is good and informative, the graph can be learned by a good model, which could produce a non optimal result on detection if the graph is incomplete or noisy. There have been several recent research efforts toward the use of graph representation learning (Dapel et al., 2023), spatio-temporal knowledge graphs (Karim et al., 2024), and optimized graph-based IDS (Kavitha, 2025), and this is the proposed explanatory pathway.

H9: Relational traffic representation quality mediates the relationship between GNN model capability and IoT intrusion detection performance.

The relationship between the ability of the GNN and the performance of the IoT-based intrusion detection is expected to be moderated by relational traffic representation quality because the main functionality of a GNN is to derive useful representations from the graph structure of the traffic. With improved GNN, the embeddings of IoT network behaviour are improved, as well as the detection performance is improved. For instance, attention mechanisms can highlight the relevant neighboring nodes, spatio-temporal GNNs can capture the attack changes over time and multi-graph models can learn various types of relationships between networks. The results of the recent research support the use of advanced GNN architectures for improving the feature learning and intrusion detection performance (Almehdhar et al., 2024).

In this mediation, we shall speak about how GNN's capability translates to improved intrusion detection performance. The architecture of the model enables a good performance in the detection of anomalies because it enhances the relational representations employed for classification or for anomaly detection. The structure may not be strong enough to be “meaningful” embeddings learned by GNN, and this can result in poorer detection performance. In recent optimized, explainable and hybrid GNN based IDS studies, it is seen that the better performance of the IDS can be gained by using more robust model designs which leads to improved learned representations, robustness and interpretability (Khuwuthyakorn et al., 2025).

H10: Relational traffic representation quality mediates the relationship between AI training and optimization strategy and IoT intrusion detection performance.

The performance of the IoT intrusion detection is expected to be distributed through relational traffic representation quality since the better they can be trained and optimized, the better they can detect the intrusions in the IoT traffic represented in the relational format. Effective measures include optimization methods that produce more reliable and stable solutions to model the traffic in IoT networks, in order to generate more generalizable and reliable representations. Pretraining using autoencoder, knowledge distillation, self-supervised learning, semi-supervised learning, federated learning and optimization-based IDS are recently found to be effective for representation learning when detecting the performance in IoT, edge and cloud-edge environment (Sana et al., 2024).

This mediation is important for three reasons: Firstly, training and optimization techniques are not only improvements to the models but actually the improvement of the learned relational traffic pattern which forms the basis for decisions on intrusion detection. Secondly, the correction of the learned traffic pattern errors is something that needs to be achieved in the end. Finally, the rest is only a pure technical implementation of the relevant algorithms, which use the learned traffic pattern as their basis. 2) How this mediation is achieved is very important to the improvement of the learned traffic pattern. 3) The needed mediation in order to use the methods for improving the learned traffic pattern is essential for the improvement. Better training can yield with the improvement of overfitting, dealing with the imbalanced classes, adversarial behaviour and robustness in deployment to resource limited IoT environments. The reviews and empirical studies have emphasized on optimization and adaptation of IDS system

based on AI for achieving the highest real-time performance, explanation efficiency, scalability, and adaptability to different application domain in the IoT sector (Terumalasetti, 2025).

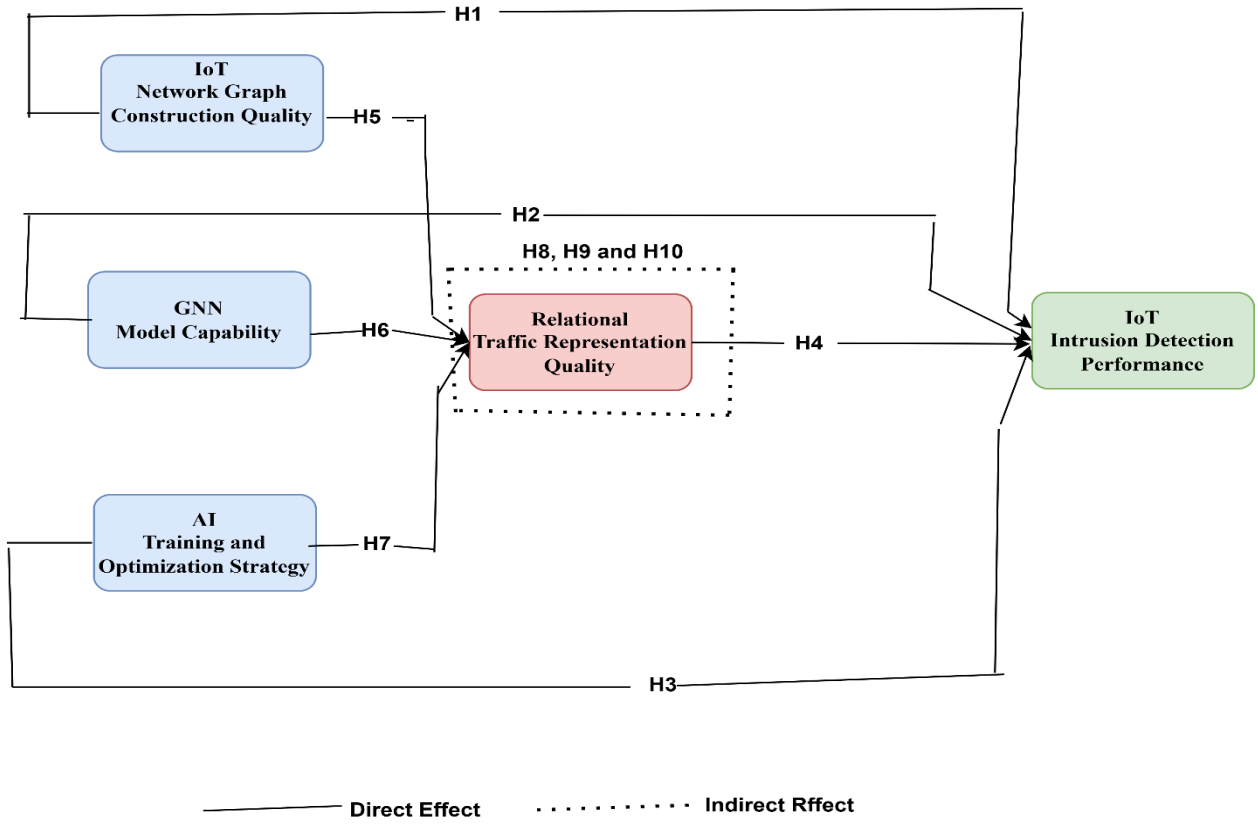

Figure 1: Proposed Research Model

3. Research Methodology

3.1 Research Design

In this research, the research design is used is quantitative, explanatory and cross-sectional which is intended to study the relationship between quality of the IoT network graph construction, the capability of the GNN model, the strategy for training and optimizing an AI model, the quality of the representation of the traffic relation, and the performance of IoT intrusion detection. Data will be collected through a structured questionnaire, including all the respondents who have a relevant knowledge regarding IoT networks, cyber security, artificial intelligence, network security management and intrusion detection systems. The partial least squares structural equation modelling (PLS-SEM) will be used because the study is a complex predictive model that involves several independent variables, a mediating variable, and a dependent variable, so that PLS-SEM is able to test the direct and indirect relationship between the variables. This analysis will be conducted using the SmartPLS software and then the measurement model test is carried out using indicator reliability, internal consistency reliability, convergent validity and discriminant validity. After that, the test of the structural model will be carried out through the path coefficient and coefficient of determination test, effect size test, predictive relevance test, and bootstrapping test for hypothesis testing. The selected method (PLS-SEM) can be used in this study as it is a technique used to predict research, it is suitable to handle complex models, and also widely used in technology and technology research (Ogenyi et al., 2025) and cybersecurity studies involving mediation analysis. This research design will enable the empirical verification of the proposed framework and explore the influence of graph construction quality, GNN capabilities and training strategy of AI on the performance of IoT intrusion detection system (IDS) based on relational traffic representation quality.

3.2 Measurement Instruments

The survey instrument was a structured questionnaire using the scale strongly disagrees to strongly agree that had 5-point scale. All constructs will be treated as reflection measured constructs in PLS-SEM. The quality of the IoT network graph construction, performance of the GNN model, and performance of the IoT intrusion detection will be each selected 7 items; the AI training strategy, optimization strategy will be selected 6 each; the quality of the representation of the relational traffic will be selected 6. The items take advantage on cutting-edge studies from the following areas: GNN application to IDS based IoT, graph representation learning, AI optimization and IDS performance. To test the reliability and validity of indicators, PLS-SEM standards will be followed, such as reliability test (Cronbach's alpha, composite reliability, AVE), and Fornell-Larcker and HTMT, bootstrapping will be conducted to test the validity and reliability of the indicators (Madalieva et al., 2025).

Table 1. Instruments

Variable	Code	Measurement Items	Sources
IoT Network Graph Construction Quality	GQ1	The IoT network traffic is represented through clear and meaningful graph structures.	Sun, Teixeira, & Toor (2024); Termos (2026); Dasarla (2026); Kanca & Türker (2026)
	GQ2	The graph construction process accurately represents IoT devices as nodes.	
	GQ3	The graph construction process accurately represents communication links among IoT devices as edges.	
	GQ4	The graph structure captures important temporal patterns in IoT network traffic.	
	GQ5	The graph construction process includes relevant node and edge features for intrusion detection.	
	GQ6	The graph structure preserves important IoT network topology and communication dependencies.	
	GQ7	The graph construction process reduces irrelevant or noisy relationships in IoT traffic data.	
GNN Model Capability	GMC1	The GNN model can effectively learn relationships among IoT devices and traffic flows.	Alnazzawi et al. (2025); Jiang et al. (2025); Ares-Robledo, Rifà-Pous, & Clarisó (2026); Sharma et al. (2026)
	GMC2	The GNN model can aggregate useful information from neighboring nodes in the IoT network graph.	
	GMC3	The GNN model can identify important traffic relationships through attention or weighting mechanisms.	
	GMC4	The GNN model can capture both local and global communication patterns in IoT networks.	
	GMC5	The GNN model can handle heterogeneous and dynamic IoT traffic conditions.	
	GMC6	The GNN model is scalable for analyzing large IoT network structures.	
	GMC7	The GNN model provides explainable or interpretable support for intrusion detection decisions.	
AI Training and Optimization Strategy	ATO1	The model training process uses appropriate hyperparameter tuning to improve detection performance.	Zhou et al. (2024); Tanvir et al. (2026); Diao et al.
	ATO2	The training strategy includes effective feature selection or feature optimization techniques.	

Variable	Code	Measurement Items	Sources
	ATO3	The training strategy addresses class imbalance in IoT intrusion detection data.	(2026); Mwiga et al. (2026)
	ATO4	The model uses advanced learning strategies such as semi-supervised, self-supervised, or federated learning.	
	ATO5	The training process improves the model's ability to detect unseen or zero-day attacks.	
	ATO6	The optimization strategy supports lightweight and efficient deployment in IoT environments.	
Relational Traffic Representation Quality	RTRQ1	The learned traffic representations clearly capture relationships among IoT devices and flows.	Mananayaka & Chung (2026); Ares-Robledo et al. (2026); Dey (2026); Gupta et al. (2026)
	RTRQ2	The learned representations effectively distinguish normal traffic from malicious traffic.	
	RTRQ3	The learned representations reduce noise and irrelevant traffic features.	
	RTRQ4	The learned representations capture temporal changes in IoT network behavior.	
	RTRQ5	The learned representations improve the separation of different attack classes.	
	RTRQ6	The learned representations generalize well across different IoT traffic conditions.	
IoT Intrusion Detection Performance	IDP1	The intrusion detection system accurately detects malicious activities in IoT networks.	Komal & Li (2026); Sanjalawe et al. (2026); Ahmed & Askar (2026); Sallam, El Barachi, & Li (2026)
	IDP2	The intrusion detection system achieves high precision in identifying actual attacks.	
	IDP3	The intrusion detection system achieves high recall in detecting different types of intrusions.	
	IDP4	The intrusion detection system maintains a strong F1-score across normal and attack traffic.	
	IDP5	The intrusion detection system reduces false positive alerts in IoT network monitoring.	
	IDP6	The intrusion detection system detects attacks with low latency.	
	IDP7	The intrusion detection system remains effective against dynamic, unknown, or zero-day attacks.	

All items were measured using a five-point Likert scale ranging from 1 = strongly disagree to 5 = strongly agree.

3.3 Population and Sampling

The population of this study will be professionals and experts with hands-on experience of IoT networks, cybersecurity, artificial intelligence, network monitoring, intrusion detection systems, cloud-edge computing or IT security management in companies whereIoT-infrastructures are used. The population of the respondents will be selected by purposive sampling as it is a specialized and technical knowledge based study which involves individuals who are directly involved in the implementation of IoT security and knowledge about intrusion detection practice using AI. This total sample size of 510 is judged to be sufficient for PLS-SEM since it has multiple independent variables, a mediating variable, and a dependent variable and larger population size would lead to higher statistical

power and parameter stability, better predictive ability and the reliability of the bootstrapping results (Shkarupylo et al., 2024). Cyber security analysts, engineers working in the field of IoT or other related areas, network administrators, AI or machine learning specialists, IT managers, system security officers and researchers in IoT security-related areas may be included on the list of selected respondents. Thus, the selection of 510 subjects is appropriate for conducting empirical verification of the proposed hypotheses in this study, which connects the construction quality of the graph of the IoT network, the ability of the GNN model, the training and optimization process for the AI model, the quality of the representation of the traffic flow, and the performance of the IoT intrusion detection.

3.4 Data Collection

The data for this study will be obtained via a structured questionnaire survey of the respondents who have experience of knowledge regarding the IoT network, cyber security, AI, intrusion detection systems or IT security management. The questionnaire will primarily be made available on online platforms like email, Google Forms, LinkedIn, professional cybersecurity networks and contacts within the organizations themselves – to efficiently reach the targeted respondents. The instrument will be pre-taken for content validity by academic experts, industrial experts before main data collection and for the pilot test to check the clarity, reliability, and suitability of content items to the context of the study. Respondents will be provided with an explanation of the purpose of the study, that responses will be confidential and that they can withdraw from the study at any time. In this study, structured survey is appropriate as it is structured to be a quantitative, cross-sectional type of research which tests the possibilities of relationships by applying PLS-SEM, and using purposive sampling, as widely applied in cybersecurity, IoT and information systems research, where the research object involves survey data collection (Alohali et al., 2025).

3.5 Respondents Profile

The demographic profile of the respondents will be briefly described in order to give a clear picture of the characteristics of the background of the 510 respondents who participated in the study. The demographic area includes things like genders, age groups, levels of education, involvements in IoT networks, levels of monitoring networks, intrusion detection systems, cyber security, or professional position. The stakeholders include cybersecurity analysts, IoT engineers, network administrators, AI and machine learning specialists, IT managers and system and cloud-edge computing experts, and academics or industry experts who are currently studying AI for intrusion detection in IoT networks. Education level would be represented by having bachelor's or other post-graduate degree and work experience would be represented as less than 3 years, 3–5 years, 6–10 years and more than 10 years. This demographic information is important because the technical background, role and experience of the respondents can likely impact their opinion of the quality of graph construction, the ability of the GNN model, their optimization of the GNN model, their perception of the quality of relationship traffic, and their detection ability of the IoT intrusion detection system. Demographic profiling is commonly used in characterizing samples, evaluating the respondents' suitability, and confirming the results of quantitative survey and PLS-SEM studies particularly in the field of cybersecurity, IoT and information systems studied (Haldorai, 2023).

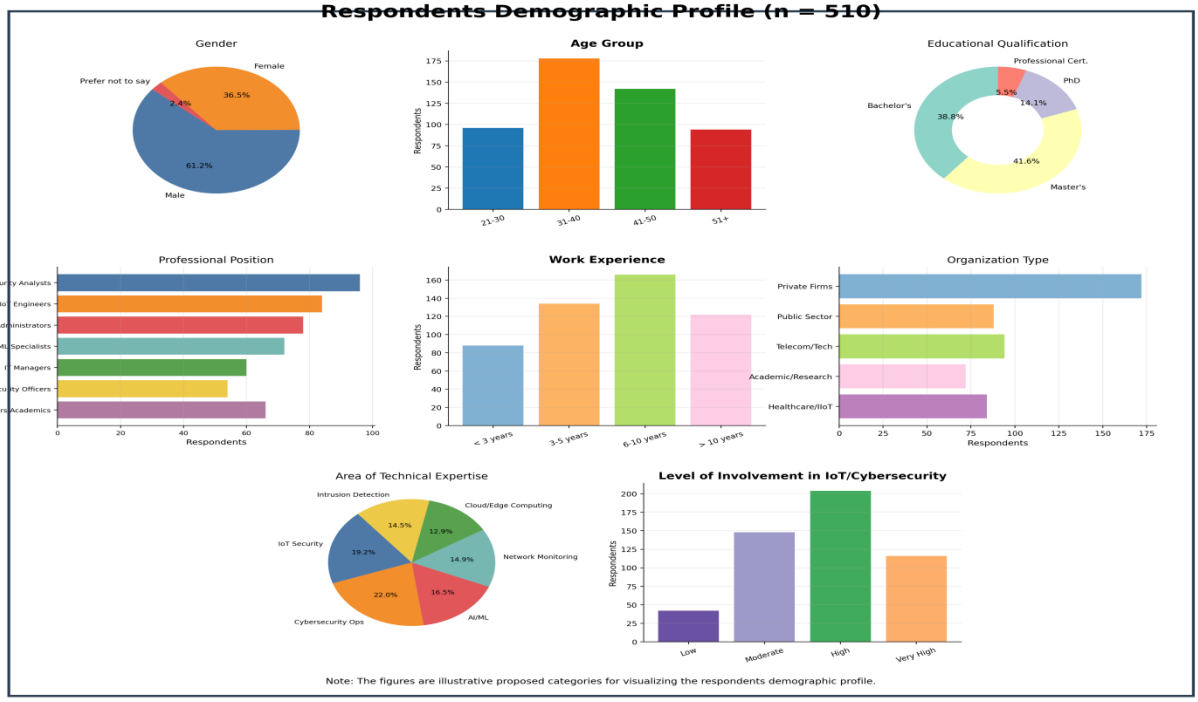

Figure 2: Respondents Profile

3.6 Data Analysis Technique

The data technique used in this study is Partial Least Squares Structural Equation Modeling (PLS-SEM) because the number of independent variables, one independent variable which is the mediator, and one dependent variable in this study. Data screening procedures of the data will be conducted in the analysis, which will include the check of missing values, normality, outliers, common method bias and descriptive statistics. Next, the measurement model is examined in relation to indicator loadings, Cronbach's alpha coefficient, composite reliability and average variance extracted, Fornell-Larcker criterion and HTMT ratio to ensure the reliability, convergent validity and discriminant validity of the measurement model. Then, this model will be examined in terms of variance inflation factor, path coefficient, coefficient of determination, effect size and bootstrapping for the direct and mediating effects, and for the predictive relevance. The technique is suitable due to PLS-SEM being prediction-oriented, the fact that there are many variables involved particularly in the research on information systems and technology adoption, and the widespread use of such models for mediation analysis (Prince et al., 2024).

3.7 Assessment of Measurement Model

Measurement model will be evaluated first to ensure reliability and validity of construct and then will be tested structural relationship to ensure reliability and validity of structural relationship. The first analysis will focus on the reliability of all variables used in this study, the outer loading needs to be checked, if the outer loading is 0.70 or above, it is deemed to be acceptable, the outer loading below 0.50 may be deleted as it is weak, and the deletion will increase the reliability and validity of the current study. The internal consistency reliability test will be evaluated by Cronbach alpha and composite reliability and rho A will be in the range of 0.70–0.95. Convergent validity will be assessed using average variance extracted in which a construct threshold of 0.50 will be met, meaning that the variance in the indicators would exceed 50% for each construct. Fornell–Larcker criterion and heterotrait-monotrait ratio will assess the discriminant validity, which means that the square root of AVE is greater than the inter-construct correlation and the HTMT is less than the recommended limit of 0.85 or 0.90. Moreover, variance inflation parameters will be used to check for possible multicollinearity in the indicators, to see whether the measurement model is affected by multicollinearity. These procedures can be appropriate in order to check whether the quality of the graph construction is consistent for the IoT network, the ability of the GNN, the training and optimization of the AI model and the quality of relation representation in traffic can be measured correctly and consistently, prior to engaging in the structural model assessment process in the SmartPLS (Thavasimani & Srinath, 2022).

The test–reliability scores for the measurement model in Table 3 show that it has good internal consistency, reliability and convergent validity. The item factor loading for all the items in this study revealed that they are in the acceptable range of 0.7 to 0.8 and above, signifying that all items are satisfactory representations of their constructs. The item factor loading range is from 0.851 to 0.927. The means of the Outer VIF values (2.643 to 4.867) are in the lower end of the range compared with the general cutoff of 5.0 meaning that the general problem of multicollinearity is not a significant problem in the measurement items. The internal consistency reliability of the AI training and optimization strategy is 0.942 - 0.965 for Cronbach's α and 0.942 - 0.966 for composite reliability, which denotes high internal consistency reliability for the AI training and optimization strategy. The values of AVE range from 0.775 to 0.850, which represents a convergent validity because all constructs explain more than 50% of the variance in their indicators. The reliability values of all constructs for the AI training and optimization strategy are very high and can be examined for any item similarities, but the results indicate the constructs are all reliable and valid to further assess the structural model for PLS-SEM (Li et al., 2024).

From the results shown in Table 4 there are no multi-collinearity problems among the constructs of predictors in the structural model. All of the inner VIF values are under 1.004, and much less than the threshold values of 5.0 and 3.3. This means that while there is a correlation between each variable, AI training and optimization strategy, GNN model capability and quality of IoT network graph construction, these three variables are not meaningfully highly correlated when predicting the quality of relational traffic representation and IoT intrusion detection performance. Thus, the independent variables can be incorporated in the model without inducing a collinearity problem and the path coefficients are not over- or underestimated. These results suggest that the structural model could be suitable for future hypothesis testing and that a path-coefficient and effect size analysis and a mediation analysis in PLS-SEM were performed (Ramzan et al., 2023).

Table 5 shows that the results did support discriminant validity based on Heterotrait-Monotrait ratio. The values for HTMT are lower than the recommended value (0.85 or 0.90); range from 0.026 – 0.763. The best correlation (0.763) exists between performance of intrusion detection for the IoT and the quality of traffic representation for the relational DB, whereas all the other correlations do not reach the acceptable level. This implies that constructs are uncorrelated and represent different aspects of the model. Therefore, the discriminant validity of AI training and optimization strategy, capability of GNN model, quality of IoT network graph construction, IoT intrusion detection performance, and quality of relational traffic representation are sufficiently developed, and the measurement model is suitable for evaluating and testing the model presented in this study, which is based on PLS-SEM (Vurubindi et al., 2025).

Table 6 shows that all the predictor variables have meaningful (ES) effect on each endogenous construct. From the common understanding of s^2 (Zakariah et al., 2025), values around 0.02 indicate small effects, around 0.15 indicate medium effects and above 0.35 indicate large effects. For IoT IDS the performance of the training and optimization strategy is medium (0.321) while the effectiveness of the representation of the relational traffic is large (0.370). The GNN model capability is one of the most prominent for both the IoT intrusion detection and the relational traffic representation, with f square value of 0.587 and 0.394 for these two, respectively. The quality of IoT network graph construction also has a significant influence on the performance of IoT intrusion detection (value 0.401), and a medium impact on representing relational traffic (value 0.345). In general, the results demonstrate that both capability of the GNN model and the quality of the graph construction used as well as the approach for training and optimizing the model using AI greatly improve the IoT IDS, and the representation of relational traffic.

The structural model can be seen in the results presented in the table 7, the model is acceptable in terms of explanatory power, its predictive relevance and model fit. The R-square value for performance of IoT intrusion detection is 0.582 and adjusted R-square value is 0.579 which means that the performance of IoT intrusion detection can be explained by the predictors with moderate explanatory power of 58.2%. Similarly, the R-squared value to represent the traffic in relations is 0.542 and the adjusted R-square value is 0.539 indicating that 54.2% of the variance of the mediating variable is explained by the predictors (Bensaid et al., 2024). The IoT intrusion detection performance value of Q^2 is above 0, which shows the predictive relevance is strong positive; the same applies for the value of the relational traffic representation quality Q^2, which is 0.536. The values of RMSE and MAE are acceptable as they are within reasonable limit, and relatively low. In terms of model fit, the values of the SRMR for both of the models – the saturated model (0.026) and the estimated model (0.044) – were both lower than the recommended value of 0.08, and the NFI for both models was 0.961, which exceeds the recommended value of >0.90. Therefore, the model has a good fitting of 81%, a moderate explanation of 81% and a reasonable prediction of 80%, which is enough to test the proposed model with PLS-SEM.

Table 2: Measurement Model Assessment Criteria

Assessment Criteria	Recommended Threshold	References
Indicator Reliability (Outer Loading)	≥ 0.70	Hair et al. (2022; 2024)
Cronbach's Alpha (α)	≥ 0.70	Hair et al. (2022)
Composite Reliability (CR)	≥ 0.70	Hair et al. (2022)
rho_A	≥ 0.70	Dijkstra & Henseler (2015); Hair et al. (2022)
Average Variance Extracted (AVE)	≥ 0.50	Fornell & Larcker (1981)
HTMT Ratio	< 0.85 (strict) or < 0.90 (acceptable)	Henseler et al. (2015)
Variance Inflation Factor (VIF)	< 3.3 (preferred) or < 5.0	Hair et al. (2022; 2024)

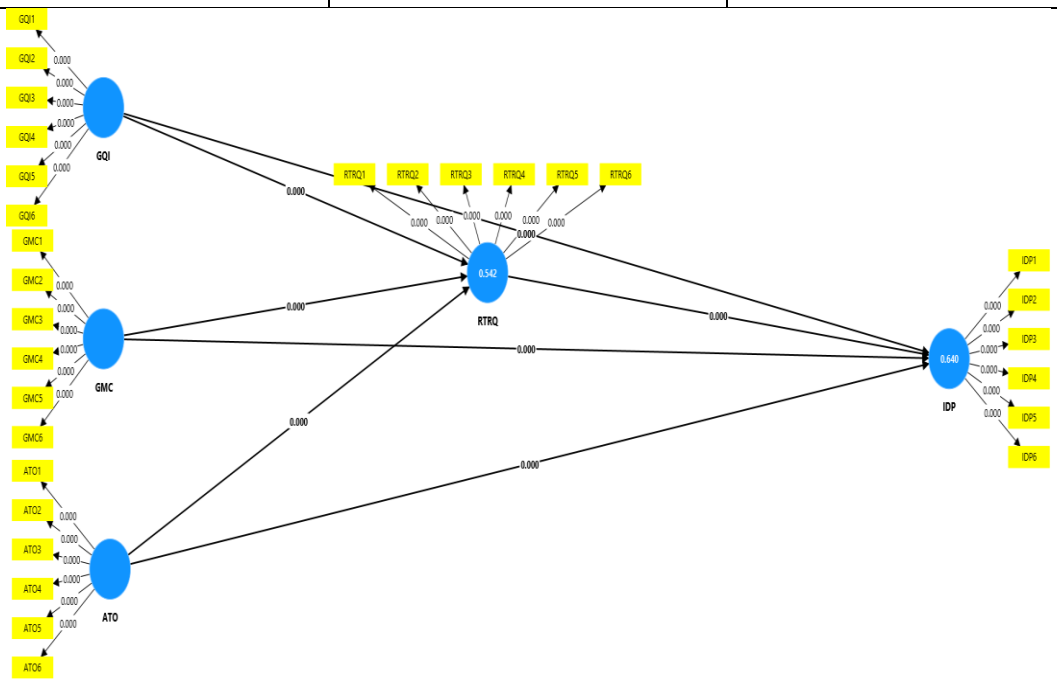

Table 3: Internal Consistency, Reliability and Convergent Validity

Construct/Items	OuterVIF values	Factor Loadings	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
AI Training and Optimization Strategy			0.965	0.966	0.850
ATO1	4.568	0.919			
ATO2	4.867	0.927			
ATO3	4.792	0.923			
ATO4	4.553	0.922			

ATO5	4.594	0.919			
ATO6	4.778	0.923			
GNN Model Capability			0.958	0.959	0.827
GMC1	4.519	0.921			
GMC2	3.887	0.905			
GMC3	3.949	0.906			
GMC4	3.905	0.905			
GMC5	4.333	0.916			
GMC6	3.918	0.903			
IoT Network Graph Construction Quality			0.948	0.949	0.793
GQI1	3.593	0.894			
GQI2	2.809	0.858			
GQI3	4.292	0.916			
GQI4	3.386	0.889			
GQI5	3.736	0.900			
GQI6	3.305	0.885			
IoT Intrusion Detection Performance			0.949	0.949	0.796
IDP1	3.873	0.903			
IDP2	3.131	0.878			
IDP3	3.207	0.883			
IDP4	3.421	0.890			
IDP5	3.973	0.907			
IDP6	3.410	0.892			
Relational Traffic Representation Quality			0.942	0.942	0.775
RTRQ1	2.643	0.851			
RTRQ2	3.311	0.888			
RTRQ3	3.118	0.878			
RTRQ4	3.519	0.895			
RTRQ5	3.024	0.875			
RTRQ6	3.486	0.893			

Table 4: Collinearity Statistics (Inner VIF)

Relationship	**VIF**	**Decision**
ATO -> IDP	1.004	No multicollinearity issue
ATO -> RTRQ	1.004	No multicollinearity issue
GMC -> IDP	1.003	No multicollinearity issue
GMC -> RTRQ	1.003	No multicollinearity issue
GQI -> IDP	1.001	No multicollinearity issue
GQI -> RTRQ	1.001	No multicollinearity issue

Table 5: Discriminate Validity Heterotrait-Monotrait (HTMT) Ratio

	ATO	**GMC**	**GQI**	**IDP**	**RTRQ**

ATO					
GMC	0.058				
GQI	0.034	0.026			
IDP	0.423	0.546	0.447		
RTRQ	0.468	0.476	0.437	0.763	

Table 6: Effect Size of Latent Variables

Path	f-square	Effect Size
ATO -> IDP	0.321	Medium
ATO -> RTRQ	0.370	Large
GMC -> IDP	0.587	Large
GMC -> RTRQ	0.394	Large
GQI -> IDP	0.401	Large
GQI -> RTRQ	0.345	Medium

Table 7: Model Fit

	R-sq	Adj R-sq	Q²predict	RMSE	MAE	Saturated Model	Estimated Model
IDP	0.582	0.579	0.576	0.654	0.529		
RTRQ	0.542	0.539	0.536	0.685	0.533		
SRMR						0.026	0.044
NFI						0.961	0.961

3.8 Hypothesis Testing:

H1: IoT network graph construction quality has a positive and significant effect on IoT intrusion detection performance.

The result shows that for the hypothesis H1, the path coefficient is 0.410, standard deviation is 0.028, t value is 14.515 and p value is 0.000, which allows the hypothesis to be accepted. It means that the quality of constructing IoT networks' graph has a positive and statistically significant impact on the performance of IoT intrusion detection. Therefore, if the graph construction is improved, the knowledge base of the communication pattern, the pattern of the attack, and the knowledge base of the IoT devices that the intrusion detection system can be constructed upon will be increased as well (Chaudhari et al., 2023).

H2: GNN model capability has a positive and significant effect on IoT intrusion detection performance.

Based on the obtained result shows that the relationship between the two constructs showed the path coefficient value of H2 (0.496), the standard deviation value of (0.026), the t value of (18.792) and the p value of (0.000). This indicates that out of the direct paths, the contribution of GNN model capability to the IoT intrusion detection performance is the highest. The finding shows that GNNs with improved abilities to collect information, attract attention and grow and to resist attacks are capable of dissecting intrusions in IoT networks better (Xu et al., 2023).

H3: AI training and optimization strategy has a positive and significant effect on IoT intrusion detection performance.

Based on this study the result shows the path coefficient of 0.367, standard deviation of 0.028, t value is 13.309 and p value is 0.000 which supports the hypothesis (H3). This means that this training and optimization process of AI has a positive and significant impact on the performance of the IoT intrusion detection system (IDS). There are various effective optimization techniques, like hyperparameter tuning, dealing with address class imbalance, feature

optimization, and lightweight training of the model, that help in achieving attack detection accuracy and efficiency (Liu, 2024).

H4: Relational traffic representation quality has a positive and significant effect on IoT intrusion detection performance.

From the result, the value of path coefficient for model H4 is 0.357 with standard deviation (SD) 0.033; this shows that the model has been confirmed at p-value < 0.05 with the t value of 10.692. It demonstrates that a relational, high-quality traffic representation will greatly improve the IoT intrusion detection (ID) detection. The result showed that the detection mechanism was more effective in detecting a normal traffic and abnormal traffic if the learned traffic representation is clearly based on the relationships between the devices in the network, the dependencies between the traffic and abnormal pattern (Zhang et al., 2024).

H5: IoT network graph construction quality has a positive and significant effect on relational traffic representation quality.

Based on the hypothesis test that the result achieved is path coefficient is 0.398, standard deviation of 0.028, t value of 14.297, and a p value of 0.000 concluded that the hypothesis was accepted. This confirms the effectiveness of the relational traffic representation quality that can be obtained through the creation of high quality graphs. By virtue of designing a well-structured IoT graph, meaningful relationships between the nodes, edges, flows and attack paths are learned, as well as better traffic embeddings for intrusion detection (Abdel-Basset et al., 2022).

H6: GNN model capability has a positive and significant effect on relational traffic representation quality.

H6 is supported by the result, which is path coefficient = 0.426; SD = 0.029; t-value = 14.735; p-value = 0.000. This indicates that the quality of relational traffic representation positively and significantly affects its capability of the GNN model. Based on the results, it is evident that deep GNN models can capture richer and more discriminative graph representations based on the data of an IoT network (Shoukat et al., 2025).

H7: AI training and optimization strategy has a positive and significant effect on relational traffic representation quality.

From the above results, it can be concluded that the result values of path coefficient, standard deviation, t-value and p-value support the research of H7 with values of 0.412, 0.028, 14.886 and 0.000 respectively. These suggest that the way in which the AI is trained and optimized could have a significant effect on performance of relational traffic representation. The traffic model will be enhanced by learning a stable, generalizable and meaningful traffic representation from complex IoT network data by properly training and optimizing the model (Zareh Farkhady et al., 2025).

H8: Relational traffic representation quality mediates the relationship between IoT network graph construction quality and IoT intrusion detection performance.

The result showed that the coefficient of determining H8 with the indirect path was 0.142, with SD (standard deviation) value as 0.016, t-value as 8.684 and p-value as 0.000. This indicates that the quality of the graph construction in the IoT network is an important QoR to bridge the gap between the quality of the traffic in the relational network and the intrusions detected from the IoT network. It is also a partial mediation where the direct effect of graph construction quality on intrusion detection performance is also considered, and the indirect effect of graph construction quality on intrusion detection performance is mediated by the relational traffic representation of graph construction (Binthiya & Ravindran, 2025).

H9: Relational traffic representation quality mediates the relationship between GNN model capability and IoT intrusion detection performance.

The path coefficient of the result is supporting H9 is 0.152, the standard deviation is 0.017, t value is 8.766 and p value is 0.000. The results demonstrate the important mediation role of the quality of relational traffic representation between the capability of the GNN model and the performance of IoT intrusion detection. The result here suggests a partial mediation as another pathway for GNN model capability to influence intrusion detection performance is a complementary pathway. By improving learnable relational traffic representations, this not only improves the GNN capability but has a direct positive impact on intrusion detection performance as well (Rajasekaran et al., 2025).

H10: Relational traffic representation quality mediates the relationship between AI training and optimization strategy and IoT intrusion detection performance.

It is obtained with an indirect path coefficient of 0.147, a standard deviation of 0.0175 and a t value of 8.478, the p value is 0.000. This validates that the quality of relational traffic representation, as a result of AI training, significantly acts as a mediator between AI training and optimization strategy and the performance of IoT intrusion detection. The mediation is complementary partial mediation since the mediation process of the increase in intrusion detection performance due to the direct effect of the AI training and optimization strategy is also significant (Zhukabayeva et al., 2025). This introduces direct and indirect ways of improving intrusion detection via training and optimization methods to improve the representations of relational traffic.

Table 8: Hypotheses Testing (Bootstrapping)

Hypothesis	Relationship	Path Coefficient	Standard deviation	t- Value	P - values	Result
H1	GQI → IDP	0.410	0.028	14.515	0.000	Supported
H2	GMC → IDP	0.496	0.026	18.792	0.000	Supported
H3	ATQ → IDP	0.367	0.028	13.309	0.000	Supported
H4	RTRQ → IDP	0.357	0.033	10.692	0.000	Supported
H5	GQI → RTRQ	0.398	0.028	14.297	0.000	Supported
H6	GMC → RTRQ	0.426	0.029	14.735	0.000	Supported
H7	ATQ → RTRQ	0.412	0.028	14.886	0.000	Supported
H8	GQI → RTRQ →IDP	0.142	0.016	8.684	0.000	Complementary Partial Mediation
H9	GMC → RTRQ→IDP	0.152	0.017	8.766	0.000	Complementary Partial Mediation
H10	ATQ →RTRQ →IDP	0.147	0.017	8.478	0.000	Complementary Partial Mediation

4. Discussion

This study shows that the quality of constructing a graph for IoT network, capability of GNN model, strategy of AI training and optimization and traffic representation quality of the network in the form of a relation positively and significantly affect the IoT intrusion detection performance. All three direct predictors had a significant impact on intrusion detection performance: GNN model capability, quality of IoT network graph construction, and the strategy for training or optimizing the AI. This indicates that the enhancement of the attack detection in IoT depends on the improvement of the GNN architecture, graph construction and training techniques. These results align with the recent research that proves learning relationships between the devices, flows, services, and attack paths is the key to successfully improve performance of the intrusion detection system model based on GNN – without having the packet records as independent entities (Wahab et al., 2025). Previous studies in the area of using GNNs for IoT and edge security confirmed that the application of specialized graph learning, attention mechanisms, multi-channel architectures and effective optimization strategies can improve the accuracy of detection, resilience and explainability of GNNs models (Mishra et al., 2023).

The quality of the IoT network graph construction's impact on both relational traffic representation quality and intrusion detection performance verifies the crucial role that design quality of the graph plays in GNN-based cyber security systems. Properly structured graph gives the ability to represent an IoT device as graph node, communication as graph edges and attack behavior as patterns, enhancing the ability of the model to detect subtle attack patterns. Temporal behavior and communication dependency have been highlighted in recent research (El Gadal & Ganti, 2025) as well as the modelling of network topology for the use of graph-based intrusion detection systems. However, as this example shows, there are other studies that offer another viewpoint: The graph might also add noise to the system, add something to the computational load, and not work out in the real world as well if it didn't accurately represent real world traffic. To cite just a few examples, recent literature on GNN anomaly detection and AI applications for IoT-edge cybersecurity has pointed out several un-addressed issues such as dynamic graph modeling (Jiang et al., 2024), data imbalance (Gill & Dhillon, 2024), scalability, and deployment readiness. This contradictive evidence does not challenge the significance of constructions of graphs but it reinforces the need for a careful design of the graph, choice of its features, and validation for heterogeneous IoT settings.

The results also confirm that the performance of GNN can greatly improve the relational traffic representation and its intrusion detection capability as well. Advanced GNN functions such as neighbourhood aggregation, attention based weighting, spatio-temporal learning, multi-Graph processing and explainability, allow it to learn more complex representations of both normal and malicious traffic. The results corroborate those of other researchers, who have shown that graph attention networks (GAT) and multi-graph neural networks (MGN) as well as hybrid GNN-transformer models are able to successfully capture the structural and temporal properties of IoT and edge networks to improve the problem of intrusion detection (Khadam et al., 2024). In large-scale IoT environments, however, the complex models, such as GNNs, pose challenges on computation cost, low deployability in real-time, vulnerability to adversarial attacks, and interpretability issues are reported in the literature (Ayyadurai et al., 2025). This is the reason it is necessary to perform the balance of heavy model capability with light design, and clear outputs and deployment constraints.

The improvement in relational traffic representation quality achieved by the AI training and optimization strategy, as well as the improvement in ID performance for IoT traffic, indicate that the optimisation strategy plays a crucial role in model performance, in addition to the model architecture used. Representations are learned with effective strategies like hyperparameter tuning, handling class imbalance, autoencoder pretraining, semi supervised learning, self supervised learning, federated learning and knowledge distillation, etc., which can lead to good generalization to other attacks. Optimized GNNs models, autoencoder-pretrained spatio-temporal GNNs and self-supervised graph learning approaches have also improved the performance of intrusion detection systems in IoT, healthcare-IoT and cloud-edge environment as revealed by the recent studies (Al-Jabbar et al., 2023). However, some studies caution that optimization methods may not always be suitable for a range of datasets and real-life IoT environment because of the variety of attacks and attack pattern, the different behaviors of devices, and network traffic distribution (Paliwal et al., 2025). An opposite evidence points out that future models must be tested using other datasets of IoT and deployment environments in order to guarantee the robustness and generalization of models.

The results of the mediation analysis show that mediation by the quality of representation in relational traffic is complementary-partially mediating between the three independent variables and intrusion detection performance in IoT. Quality of intrusion detection is improved both directly and indirectly through quality of the constructed graph, and the ability of the GNN model, and through improvements to the way the graph is trained and optimized for the AI. The results indicated that the GNN model capability with relational traffic representation quality, AI training optimization strategy and graph construction quality were the top three indirect correlations. This is a theoretical significance because it provides the insight on how and why the usage of GNN-based intrusion detection enhances the security of the IoT network: With the help of graph structures, model architectures and training methods that generate meaningful embeddings to differentiate between normal and malicious traffic, the system becomes effective. The outcome aligns with previous graphs representation learning research which confirms that high-quality embeddings are found to be effective for anomaly detection, attack classification and cybersecurity decision-making (Joshi et al., 2025). On the contrary, other works suggest that the quality of the representation might be degraded when the data are imbalanced, the graphs are noisy, the labels are too short, or the traffic pattern changes from time to time (Lin et al., 2025). This study offers valuable insights into the literature by proving that the quality of traffic representation in the relational graph is an important explanatory mechanism between the relational graph, its learning capacity and the optimization method, and its impact on the ability to detect IoT attacks.

4.1 Theoretical implications

From a theoretical perspective, this study helps advance the literature of cybersecurity for AI-supported IoT by establishing the key relationships among the quality of the constructed graph of the IoT network, the ability of the GNN, AI training and optimization strategies, the quality of the representation of the traffic, and the performance of IoT intrusion detection. Therefore, the focus of the previous studies has been on the accuracy, robustness or explainability of the GNN-based intrusion detection system (IDS) or on the degree of computational efficiency; in this work, an attempt is made to give an explanation to the improved detection outcomes by using graphs and graph-based learning techniques. The empirical result that the quality of relational traffic representation is a complementary partial mediator is a confirmation of the representation learning theory, suggesting that the importance of graph construction, model capability and optimization strategy is carried through in detection performance by significant relational embeddings. This is in line with the most recent research, which has indicated that GNNs can be utilized for intrusion detection, as they have the ability to learn structural, temporal, and relational patterns in the traffic of IoT networks (Alqahtany et al., 2025) , (Xia & Zhou, 2024). The study also represents the stepping forward from the graph theory to the information processing theory and further reinforces the notion that recent Internet of Things attacks need to be

seen as the relationships of devices, flows, services and attack paths rather than the view as a list of unrelated traffic records.

4.2 Practical implications

The study results are applicable in practice to cybersecurity managers, network security experts, IoT system designers, and AI developers who are interested in improving intrusion detection systems for IoT. It was observed that the capability of GNNs most significantly influenced the performance of an IoT ID system, and thus, the researchers recommend that organizations consider GNN architectures with the following properties: explainability, robustness, scalability, attention, and spatio-temporal learning, as well as graph aggregation. Moreover, the quality of the graph construction is crucial in IoT networks, and organizations can greatly benefit from correct graph design; they need to properly define nodes, edges, traffic characteristics, communication dependencies, and attack paths, before implementing GNN models. Additionally, the effectiveness of the method of introducing AI training and optimizing its parameters suggests that cybersecurity professionals can benefit from hyperparameter tuning, handling class imbalance, self-supervised learning, autoencoder pretraining, federated learning and lightweight optimization to improve the effectiveness of real-time detection and readiness for deployment. The implications are noted in accordance to the latest research on the requirements of optimized EXPLAINED ADAPTIVE LIGHTWEIGHT intrusion detection systems in IoT/edge network, health-care IoT, Industrial IoT, and Critical Infrastructure scenarios (Basri, 2025). The study thus pushes the practices to focus towards the improvement of the quality of graph, the ability to use graph, training strategy and quality of graph representation as the key bases for improving the performance of IoT cybersec, rather than towards the imminent adoption of an IDS tool based on AI.

5. Conclusion

They determined that IDS systems had to be more sophisticated and capable of detecting more dynamic, relational and hidden patterns of attacks between the devices, flows, services and messages sometimes passed between the devices to combat increasingly complex IoT networks. To solve this issue, the study investigated the mediating effects of relational traffic representation quality between the quality of IoT network graph construction, the capability of GNN and the strategy of AI training and optimization on IoT intrusion detection performance. The results showed all positive and significant direct relationships, where high quality constructing graphs correlated with a high capability of graphs, the optimized use of AI, and meaningful representation of relational traffic helps to improve the performance of intrusion detection for IoT. As regards predictors, the GNN model capability proved to be the best direct predictor, with graph aggregation and attention learning, spatio-temporal modeling, scalability and robustness/explainability playing a crucial role in effective IoT cyber security. The quality of the relational traffic representation is the other partial mediator it is found in the mediation results, as the construction of the graph, the GNN capability, and the optimization of the AI based system have a direct and indirect impact on the ID performance through providing better learned traffic embedding. The findings have theoretical importance as they extend the scope of graph theory, information processing theory and representation learning theory for IoT Cyber Security, and practical importance for designing AI-based IDS solutions as they suggest focusing on the quality of the graph, model, training procedure and representation. The study has limitations in that it has a cross sectional design and quantitative approach, confined to self reported responses to questionnaires, relies on purposive sampling and engages only selected set of professionals with angles of security in IoT, failing to generalize to other areas of IoT and real time operations. In the future, the model should be validated with experimental implementation of a GNN, real datasets of network traffic, comparing IoT system and smart city systems with edge-cloud systems and industrial IoT systems. Enhancing the explainability and lightweight nature of IDS models developed using GNNs, while also considering federated and privacy-preserving models and adversarially robust models, as suggested in recent research, would also be valuable for future investigations to increase their suitability for deployment and scalability and to ensure trust in AI-based IoT cybersecurity systems.

Limitations

There are a number of limitations that need to be taken into account in the interpretation of the findings of this study. This study adopted a cross-sectional quantitative design, where the observations were performed at a single point in time, thus cannot completely account for the performance changes of IoT intrusion detection techniques with respect to changing cyber attack, IoT traffic characteristics, and IoT GNN models over time. Secondly, the study was based on survey questionnaires from 510 respondents, resulting in the responses being based on perceptions as opposed to direct experimental testing on real IoT traffic sets. Third, because of the limitations of the study, the study sample consisted of individuals who were knowledgeable in the fields of IoT networks, Cyber security, AI and IoT

intrusion detection systems, which may limit the ability to generalize the results to other industry areas related to IoT. Fourth, the study didn't explicitly include all the other factors which are considered as important to the study such as Data Privacy, Adversarial attacks, Computational cost, Explainability, Real-time deployment readiness and Organizational Cyber-security maturity. These factors are expected to play almost the same important role as the study. Furthermore, recent research also has identified some remaining challenges with GNN intruder detection systems as mentioned below: dataset imbalance (Albattah et al., 2022); scalability (Alippi & Ozawa, 2024); explainability, generalization and deployability in resource-limited environments (Geetha et al., 2023).

Future Research Directions

Research efforts should be carried out to study such relationships in longitudinal designs, in experiments and with real IoT traffic data to verify stability of the proposed relationships in time and under attack scenarios. Evaluation of the model should be done to make the model more generalizable in any specific domain such as, Industrial IoT, Healthcare IoT, Smart cities, Smart energy, Transportation system and Edge-Cloud environments, etc. In future, other GNN models such as GCN, GAT, GraphSAGE, spatio-temporal GNNs, multi-graph GNNs and hybrid models can be compared to identify the best GNN model that performs well in different scenarios of IoT security. Moreover, future efforts are needed to explore privacy-preserving and federated GNN-based IDS, explainable GNN models, lightweight deployment of GNNs, countermeasure against adversarial robustness, IDS for zero-day attacks, and scalability for real-time detection. Future work should be undertaken to gain deeper insights into quality of representation learning of real-world embeddings of graphs with benchmark datasets, performance metrics (e.g., accuracy, precision, recall, F1-score, false-positive rate, latency, and robustness), and representation quality of relational traffic by examining the complementary partial mediating role in this research. The results are consistent with the recent works which advocate for explainable and adaptive intrusion detection models for IoT and edge devices that are lightweight, privacy-preserving and generalizable (Huang et al., 2024). Due to a temporary access problem it was not possible to conduct a new scholarly search and these citations are based on the studies identified in the draft proposal.

References

1. Abdel-Basset, M., Hawash, H., Sallam, K. M., Elgendi, I., Munasinghe, K., & Jamalipour, A. (2022). Efficient and lightweight convolutional networks for IoT malware detection: A federated learning approach. IEEE Internet of Things Journal, 10(8), 7164-7173.
2. Abirami, A., & Palanikumar, S. (2023). An Artificial Intelligence-based Proactive Network Forensic Framework. Iraqi Journal of Science, 5896-5911.
3. Akanksha, P., & Naik, S. M. (2025). TCSO-KD: a novel technique for optimal feature selection and knowledge distillation for efficient IoT intrusion detection systems. Cluster Computing, 28(10), 684.
4. Al-Amiedy, T. A., Anbar, M., Belaton, B., Kabla, A. H. H., Hasbullah, I. H., & Alashhab, Z. R. (2022). A systematic literature review on machine and deep learning approaches for detecting attacks in RPL-based 6LoWPAN of internet of things. Sensors, 22(9), 3400.
5. Al-Jabbar, M., Al-Mansor, E., Abdel-Khalek, S., & Alkhalaf, S. (2023). Ebola optimization with modified DarkNet-53 model for scene classification and security on Internet of Things in smart cities. Alexandria Engineering Journal, 75, 29-40.
6. Albattah, W., Javed, A., Nawaz, M., Masood, M., & Albahli, S. (2022). Artificial intelligence-based drone system for multiclass plant disease detection using an improved efficient convolutional neural network. Frontiers in Plant Science, 13, 808380.
7. Alghamdi, R. (2022). Intrusion Detection System for Internet of Things with Deep Learning. Ecole Polytechnique, Montreal (Canada).
8. Alippi, C., & Ozawa, S. (2024). Computational intelligence in cyber-physical systems and the Internet of Things. In Artificial Intelligence in the Age of Neural Networks and Brain Computing (pp. 251-267). Elsevier.
9. Alkhafaji, N., Viana, T., & Al-Sherbaz, A. (2025). Integrated genetic algorithm and deep learning approach for effective Cyber-Attack detection and classification in industrial Internet of things (IIoT) environments. Arabian Journal for Science and Engineering, 50(15), 12071-12095.
10. Almehdhar, M., Albaseer, A., Khan, M. A., Abdallah, M., Menouar, H., Al-Kuwari, S., & Al-Fuqaha, A. (2024). Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks. IEEE Open Journal of Vehicular Technology, 5, 869-906.
11. Alohali, M. A., Alamgeer, M., Al-Sharafi, A. M., Asklany, S. A., Aljabri, J., Alotaibi, F. A., Alajmani, S. H., & Issaoui, I. (2025). Improving internet of health things security through anomaly detection framework using artificial intelligence driven ensemble approaches. Scientific Reports, 15(1), 33962.
12. Alqahtany, S. S., Shaikh, A., & Alqazzaz, A. (2025). Enhanced Grey Wolf Optimization (EGWO) and random forest based mechanism for intrusion detection in IoT networks. Scientific Reports, 15(1), 1916.
13. Alrayes, F. S., Zakariah, M., Driss, M., & Boulila, W. (2023). Deep neural decision forest (DNDF): A novel approach for enhancing intrusion detection systems in network traffic analysis. Sensors, 23(20), 8362.

14. Araújo, G., Gomes, L., Neto, A., & Vale, Z. (2025). Intelligent IoT Device Powered by AI-Based Models for Forecast and Classification. Energy Informatics Academy Conference,
15. Asim, M., Junhong, C., Wenyin, L., & Abd El-Latif, A. A. (2023). Artificial Intelligence-Based Secure Edge Computing Systems for IoTDs and Smart Cities: A Survey. Secure Edge and Fog Computing Enabled AI for IoT and Smart Cities: Includes selected Papers from International Conference on Advanced Computing & Next-Generation Communication (ICACNGC 2022),
16. Ayyadurai, R., Bobba, J., Parthasarathy, K., & Panga, N. K. R. (2025). An IoT-Powered Surgical Monitoring System Using Graph Convolutional Networks (GCNs) and Hybrid Neural Networks for Enhanced Medical Image Analysis. 2025 Third International Conference on Networks, Multimedia and Information Technology (NMITCON),
17. Bajpayi, P., Mathur, S., & Gaur, M. S. (2025). Performance Comparison of ANN and CNN for Intrusion Detection System in IoMT Networks. 2025 1st IEEE Uttar Pradesh Section Women in Engineering International Conference on Electrical Electronics and Computer Engineering (UPWIECON),
18. Basri, T. (2025). Securing VANETs for Internet of Things (IoT): AI-Driven Solutions for Privacy and Intrusion Detection. In AI-Driven Transportation Systems: Real-Time Applications and Related Technologies (pp. 105-122). Springer.
19. Bensaid, R., Labraoui, N., Ari, A. A. A., Saidi, H., Emati, J. H. M., & Maglaras, L. (2024). SA-FLIDS: secure and authenticated federated learning-based intelligent network intrusion detection system for smart healthcare. PeerJ Computer Science, 10, e2414.
20. Binthiya, A., & Ravindran, S. (2025). An effective classification using enhanced flame seeker optimization with convolution neural network for intrusion detection. Wireless Networks, 31(5), 3873-3891.
21. Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In Artificial intelligence for societal issues (pp. 3-25). Springer.
22. Chaudhari, S. A., Ahire, N. B., Jagtap, V. J., Shinde, P. S., & William, P. (2023). Design of Blockchain Models for the Identifications of Harmful Attack Activities in Industrial Internet of Things (IIOT). 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM),
23. Cheng, N., Wu, S., Wang, X., Yin, Z., Li, C., Chen, W., & Chen, F. (2023). AI for UAV-assisted IoT applications: A comprehensive review. IEEE Internet of Things Journal, 10(16), 14438-14461.
24. Cherukuri, A. K., Ikram, S. T., Li, G., & Liu, X. (2024). Artificial intelligence-based approaches for anomaly detection. In Encrypted Network Traffic Analysis (pp. 73-99). Springer.
25. Čisar, S. M., Čisar, P., & Pinter, R. (2022). Fuzzy-based intrusion detection systems. In Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach (pp. 205-215). Springer.
26. Dapel, M. E., Asante, M., Uba, C. D., & Agyeman, M. O. (2023). Artificial intelligence techniques in cybersecurity management. Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022,
27. Darla, S., & Naveena, C. (2024). Improved adaptive spiral seagull optimizer for intrusion detection and mitigation in wireless sensor network. SN Computer Science, 5(4), 394.
28. Dubey, G. P., Bhujade, R. K., Asthana, S., & Arockiam, D. (2025). 5 AI and Fuzzy Logic for Threat Detection in Healthcare Networks. Healthcare 5.0 with Fuzzy Logic: Artificial Intelligence, Cyber-Physical Systems, and Medical Internet of Things, 111.
29. El Gadal, W., & Ganti, S. (2025). Federated Secure Intelligent Intrusion Detection and Mitigation Framework for SD-IoT Networks using ViT-GraphSAGE and Automated Attack Reporting. 2025 12th IFIP International Conference on New Technologies, Mobility and Security (NTMS),
30. Gan, C., Lin, J., Huang, D.-W., Zhu, Q., & Tian, L. (2023). Advanced persistent threats and their defense methods in industrial internet of things: A survey. Mathematics, 11(14), 3115.
31. Geetha, C., Gilda, A. J., & Neelakandan, S. (2023). Deep Belief Network Algorithm-Based Intrusion Detection System in Internet of Things Environments. International Conference on Information Technology,
32. Gill, K. S., & Dhillon, A. (2024). A hybrid machine learning framework for intrusion detection system in smart cities. Evolving Systems, 15(6), 2005-2019.
33. Gummadi, A. N., Napier, J. C., & Abdallah, M. (2024). XAI-IoT: an explainable AI framework for enhancing anomaly detection in IoT systems. IEEE Access, 12, 71024-71054.
34. Haldorai, A. (2023). A review on artificial intelligence in internet of things and cyber physical systems. Journal of Computing and Natural Science, 3(1), 012-023.
35. Huang, J., Chen, Z., Liu, S.-Z., Zhang, H., & Long, H.-X. (2024). Improved intrusion detection based on hybrid deep learning models and federated learning. Sensors, 24(12), 4002.
36. Huo, Y., Chen, J., Guo, Y., Liang, W., & Sun, J. (2025). LG-BiTCN: A Lightweight Malicious Traffic Detection Model Based on Federated Learning for Internet of Things. Electronics, 14(8), 1560.
37. Jiang, W., Han, H., Zhang, Y., Wang, J. a., He, M., Gu, W., Mu, J., & Cheng, X. (2024). Graph neural networks for routing optimization: Challenges and opportunities. Sustainability, 16(21), 9239.
38. Joshi, V. R., Assa-Agyei, K., Al-Hadhrami, T., & Qasem, S. N. (2025). Hybrid AI Intrusion Detection: Balancing Accuracy and Efficiency. Sensors, 25(24), 7564.
39. JS, S. M., Thirunavukkarasu, M., Kumaran, N., & Thamaraiselvi, D. (2024). Deep learning with blockchain based cyber security threat intelligence and situational awareness system for intrusion alert prediction. Sustainable Computing: Informatics and Systems, 42, 100955.

40. Kamruzzaman, M., Bhuyan, M. K., Hasan, R., Farabi, S. F., Nilima, S. I., & Hossain, M. A. (2024). Exploring the landscape: a systematic review of artificial intelligence techniques in cybersecurity. 2024 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI),
41. Karim, F. K., Varela-Aldás, J., Ishak, M. K., Aljarbouh, A., & Mostafa, S. M. (2024). Modeling of Bayesian machine learning with sparrow search algorithm for cyberattack detection in IIoT environment. Scientific Reports, 14(1), 29285.
42. Kavitha, M. (2025). Secure IOT Framework: Blockchain Authentication and Intrusion Detection.
43. Khadam, U., Davidsson, P., & Spalazzese, R. (2024). Exploring the role of artificial intelligence in internet of things systems: a systematic mapping study. Sensors, 24(20), 6511.
44. Khuwuthyakorn, P., Thinnukool, O., & Lakhan, A. (2025). A Federated Flower Learning-Empowered Intrusion Detection System for Vehicle 6G Fog Networks. 2025 IEEE Conference on Communications and Network Security (CNS),
45. Koshkin, D., Sadovoy, O., Rudenko, A., & Sokolik, V. (2025). Optimising energy distribution and detecting vulnerabilities in networks using artificial intelligence. Machinery & Energetics, 16(2).
46. Kunaparaju, C. (2025). AI-Driven Cyber Defense Systems: Strengthening National Security through Intelligent Threat Prediction and Response. Algora, 2(1), 1-30.
47. Kushwaha, A. K., & Tiwari, P. K. (2025). Enhancing the Network Intrusion Detection Using CNN–BiLSTM: A Comparative Study with CNN–Stacked LSTM and MLP–GRU Architectures. International Conference on Next-Generation Networks and Deployable Artificial Intelligence,
48. Li, Y., Liu, Y., Xia, Y., Zhang, W., Quan, W., Kang, J., & Zhang, H. (2024). A collaborative programmable LFA defense using temporal graph learning in AIoT. IEEE Internet of Things Journal, 12(3), 2514-2529.
49. Lin, X., Yao, Y., Fang, Y., Song, B., & Yang, W. (2025). A Real-Time Hacker Group Identification Method for Industrial Control Systems Based on Gaussian Self-Organising Incremental Neural Network. IEEE Internet of Things Journal.
50. Liu, B. (2024). The analysis of art design under improved convolutional neural network based on the Internet of Things technology. Scientific Reports, 14(1), 21113.
51. López Delgado, J. L., & López Ramos, J. A. (2024). A comprehensive survey on generative AI solutions in IoT security. Electronics, 13(24), 4965.
52. Ma, P., Zhu, L., & Zhang, C. (2024). Research on Vulnerability Mining Method Based on Artificial Intelligence in Internet of Things. 2024 IEEE 2nd International Conference on Image Processing and Computer Applications (ICIPCA),
53. Madalieva, D., Ugli, J. N. K., Tuychiyeva, S., Gurudiwan, P., & Mahmood, N. T. (2025). Artificial Immune System Approach to Intrusion Detection in IOT Sensor Networks. 2025 International Conference on AI-Driven STEM Education and Learning Technologies (AISTEMEDU),
54. Makhmudov, F., Kilichev, D., Giyosov, U., & Akhmedov, F. (2025). Online machine learning for intrusion detection in electric vehicle charging systems. Mathematics, 13(5), 712.
55. Mehta, H. (2025). An Autonomous Self-Recovery Framework for Network Systems Using Reinforced Causal Decision Intelligence During Cyber Attacks. 2025 IEEE International Conference on Communication Networks and Computing (CNC),
56. Menon, S., Anand, D., Kavita, Verma, S., Kaur, M., Jhanjhi, N., Ghoniem, R. M., & Ray, S. K. (2023). Blockchain and machine learning inspired secure smart home communication network. Sensors, 23(13), 6132.
57. Mishra, A. K., Tripathi, N., Vaqur, M., & Sharma, S. (2023). Artificial intelligence based security solution for data encryption using aes algorithm. 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS),
58. Moghaddasi, K., Rajabi, S., & Hosseinzadeh, M. (2025). Intrusion Detection Systems for Enhanced Security in Mobile Edge Computing: A Systematic Review and Survey of the Applications, Challenges, and Future Directions. Wireless Personal Communications, 1-63.
59. Mohan, R. J., Raju, B. R. K., Sekhar, V. C., & Prasad, T. (2025). Algorithms in advanced artificial intelligence. CRC Press.
60. Ogenyi, F. C., Ugwu, C. N., & Ugwu, O. P.-C. (2025). Securing the future: AI-driven cybersecurity in the age of autonomous IoT. Frontiers in the Internet of Things, 4, 1658273.
61. Paliwal, G., Sharma, K. P., Sharma, P., Shrimal, V. M., & Kaur, G. (2025). AI-Based Effective Intrusion Detection System. 2025 International Conference on Digital Innovations for Sustainable Solutions (ICDISS),
62. Perumal, G., Subburayalu, G., Abbas, Q., Naqi, S. M., & Qureshi, I. (2023). VBQ-Net: a novel vectorization-based boost quantized network model for maximizing the security level of IoT system to prevent intrusions. Systems, 11(8), 436.
63. Prince, N. U., Al Mamun, M. A., Olajide, A. O., Khan, O. U., Akeem, A. B., & Sani, A. I. (2024). IEEE Standards and Deep Learning Techniques for Securing Internet of Things (IoT) Devices Against Cyber Attacks. Journal of Computational Analysis & Applications, 33(7).
64. Rahmani, P., Arefi, M., Shojae, S. M. S., & Mirzaee, A. (2024). The Random Neural Network–Based Approach and Evolutionary Intelligence Are Essential Elements of IOT–RNNEI, an Attack Detection System for IOT Networks.
65. Rajasekaran, S., Arun Kumar, A., Thangavel, C., & Arunachalam, K. P. (2025). Artificial intelligence enabled internet of things for modeling a smart power distribution system. Journal of the Chinese Institute of Engineers, 1-19.
66. Rampone, G., Ivaniv, T., & Rampone, S. (2025). A hybrid federated learning framework for privacy-preserving near-real-time intrusion detection in IoT environments. Electronics, 14(7), 1430.
67. Ramzan, M., Shoaib, M., Altaf, A., Arshad, S., Iqbal, F., Castilla, Á. K., & Ashraf, I. (2023). Distributed denial of service attack detection in network traffic using deep learning algorithm. Sensors, 23(20), 8642.

68. Razaque, A., Khan, M. J., Hassan, D. S., Kassymova, A., Rizvi, S., Ali, A., & Serbin, V. V. (2025). Optimizing Internet-of-Things Energy Management: Integrating Theory of Inventive Problem Solving with Transfer Learning and Advanced Optimization Algorithms. IEEE Access.
69. Saba, T., Rehman, A., Haseeb, K., Bahaj, S. A., & Damaševičius, R. (2022). Sustainable data-driven secured optimization using dynamic programming for green internet of things. Sensors, 22(20), 7876.
70. Sana, L., Nazir, M. M., Yang, J., Hussain, L., Chen, Y.-L., Ku, C. S., Alatiyyah, M., Alateyah, S. A., & Por, L. Y. (2024). Securing the IoT cyber environment: Enhancing intrusion anomaly detection with vision transformers. IEEE Access, 12, 82443-82468.
71. Sankaram, M., Roopesh, M., Rasetti, S., & Nishat, N. (2024). A comprehensive review of artificial intelligence applications in enhancing cybersecurity threat detection and response mechanisms. Management, 3(5).
72. Sayed, S. A., Abdel-Hamid, Y., & Hefny, H. A. (2023). Artificial intelligence-based traffic flow prediction: a comprehensive review. Journal of Electrical Systems and Information Technology, 10(1), 13.
73. Shen, Y., Shepherd, C., Ahmed, C. M., Shen, S., & Yu, S. (2024). SGD3QN: Joint stochastic games and dueling double deep Q-networks for defending malware propagation in edge intelligence-enabled Internet of Things. IEEE Transactions on Information Forensics and Security, 19, 6978-6990.
74. Shkarupylo, V., Alsayaydeh, J. A. J., Yusof, M. F. B., Oliinyk, A., Artemchuk, V., & Herawan, S. G. (2024). Exploring the potential network vulnerabilities in the smart manufacturing process of Industry 5.0 via the use of machine learning methods. IEEE Access, 12, 152262-152276.
75. Shoukat, S., Gao, T., Javeed, D., & Adil, M. (2025). SparsLIME: A Sparsity-Optimized and LIMELight-Illuminated Intrusion Detection Framework for Industrial IoT Networks. 2025 IEEE 25th International Conference on Communication Technology (ICCT),
76. Singh, S. P., Piras, G., Viriyasitavat, W., Kariri, E., Yadav, K., Dhiman, G., Vimal, S., & Khan, S. B. (2025). Cyber security and 5G-assisted industrial internet of things using novel artificial adaption based evolutionary algorithm. Mobile Networks and Applications, 30(1), 42-58.
77. Sokkalingam, S., & Ramakrishnan, R. (2022). An intelligent intrusion detection system for distributed denial of service attacks: A support vector machine with hybrid optimization algorithm based approach. Concurrency and Computation: Practice and Experience, 34(27), e7334.
78. Son, B. D., Hoa, N. T., Van Chien, T., Khalid, W., Ferrag, M. A., Choi, W., & Debbah, M. (2024). Adversarial attacks and defenses in 6G network-assisted IoT systems. IEEE Internet of Things Journal, 11(11), 19168-19187.
79. Sumathi, S., & Rajesh, R. (2023). A dynamic BPN-MLP neural network DDoS detection model using hybrid swarm intelligent framework. Indian J. Sci. Technol, 16(43), 3890-3904.
80. Swamy, K. K., & Sophia, S. (2025). Detecting Poisoning Attacks in UAVs via Spatio-Temporal Graph Neural Network and Walrus Optimizer. 2025 5th International Conference on Soft Computing for Security Applications (ICSCSA),
81. Taherdoost, H., Le, T.-V., & Slimani, K. (2025). Cryptographic techniques in artificial intelligence security: A bibliometric review. Cryptography, 9(1), 17.
82. Talukder, M. A., Islam, M. M., Uddin, M. A., Hasan, K. F., Sharmin, S., Alyami, S. A., & Moni, M. A. (2024). Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. Journal of big data, 11(1), 33.
83. Taneja, A., & Kumar, G. (2024). Attention-CNN-LSTM based intrusion detection system (ACL-IDS) for in-vehicle networks: A. Taneja, G. Kumary. Soft Computing, 28(23), 13429-13441.
84. Terumalasetti, S. (2025). Artificial intelligence-based approach to detect malicious users using deep learning and optimization techniques. Multimedia Tools and Applications, 84(8), 3979-4001.
85. Thavasimani, K., & Srinath, N. K. (2022). Hyperparameter optimization using custom genetic algorithm for classification of benign and malicious traffic on internet of things-23 dataset. International Journal of Electrical & Computer Engineering (2088-8708), 12(4).
86. Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the internet of things. Electronics, 13(16), 3343.
87. Vurubindi, P., Frnda, J., Sujatha, C. N., Divakarachari, P. B., Nijaguna, G., & Mahendar, A. (2025). Optimizing feature selection with random reversal and adaptive Gaussian based Dung beetle optimizer for intrusion detection system in IoT. Scientific Reports.
88. Wahab, S. A., Sultana, S., Tariq, N., Mujahid, M., Khan, J. A., & Mylonas, A. (2025). A multi-class intrusion detection system for DDoS attacks in IoT networks using deep learning and transformers. Sensors, 25(15), 4845.
89. Xia, F., & Zhou, Z. (2024). Methods for Computer Network Security Management Assisted by Artificial Intelligence Models. 2024 2nd International Conference on Mechatronics, IoT and Industrial Informatics (ICMIII),
90. Xu, H., Wu, J., Pan, Q., Guan, X., & Guizani, M. (2023). A survey on digital twin for industrial internet of things: Applications, technologies and tools. IEEE Communications Surveys & Tutorials, 25(4), 2569-2598.
91. Yang, J., Govindarajan, V., Arif, S., Xu, X., Kallel, M., Shaikh, Z. A., Liu, Z., Yuan, C., & Por, L. Y. (2025). SwarmSense-DNN: A Trustworthy and Decentralized Neural Framework for Proactive Anomaly Defense in Consumer IoT. IEEE Transactions on Consumer Electronics.
92. Zakariah, M., Amin, S. U., Alrayes, F. S., Helal, M., & Khan, Z. I. (2025). SCADA intrusion detection using deep factorization machines. Scientific Reports, 15(1), 39753.

93. Zareh Farkhady, R., Majidzadeh, K., Masdari, M., & Ghaffari, A. (2025). 3DLBS-BCHO: A three-dimensional deep learning approach based on branch splitter and binary chimp optimization for intrusion detection in IoT. Cluster Computing, 28(2), 83.
94. Zhang, J., Zhang, K., & Ma, L. (2024). GAN-Based Intrusion Detection System for IoT Services. 2024 2nd International Conference on Computer Network Technology and Electronic and Information Engineering (CNTEIE),
95. Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. Sensors, 25(1), 213.
96. Zivkovic, M., Bacanin, N., Arandjelovic, J., Strumberger, I., & Venkatachalam, K. (2022). Firefly algorithm and deep neural network approach for intrusion detection. In Applications of artificial intelligence and machine learning: Select proceedings of ICAAAIML 2021 (pp. 1-12). Springer.