International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Graph Neural Networks for Anomaly Detection in Encrypted Network Traffic Flows

Omowunmi Folashayo Makinde

Independent Researcher, Department of Information Systems Security, University of the Cumberlands, U.S.A
omakinde74865@ucumberlands.edu

Abstract

The proliferation of encrypted network traffic has created significant challenges for traditional anomaly detection systems that rely on deep packet inspection and payload analysis. As organizations increasingly adopt encryption protocols to protect data privacy and security, the ability to identify malicious activities within encrypted traffic flows has become a critical concern for network security professionals. This research explores the application of Graph Neural Networks as a novel approach to detecting anomalies in encrypted network traffic without compromising the confidentiality of the encrypted data. The study demonstrates how GNN architectures can effectively model the complex relationships and patterns inherent in network traffic flows by representing them as graph structures. Through extensive experimentation on real-world encrypted traffic datasets, the proposed methodology achieves detection accuracy rates exceeding 94 percent while maintaining low false positive rates below 3 percent. The research findings indicate that graph-based representations of network flows, combined with deep learning techniques, offer a promising solution to the growing challenge of securing encrypted communications. This work contributes to the field by providing a comprehensive framework for implementing GNN-based anomaly detection systems that respect privacy requirements while maintaining robust security monitoring capabilities.

Keywords: Graph Neural Networks, Anomaly Detection, Encrypted Traffic Analysis, Network Security, Deep Learning, Traffic Flow Patterns

1. Introduction

The landscape of network security has undergone a fundamental transformation over the past decade. With the widespread adoption of encryption protocols such as Transport Layer Security and its predecessor Secure Sockets Layer, an estimated 85 to 90 percent of internet traffic now travels through encrypted channels. While this shift represents a significant victory for data privacy and protection against eavesdropping, it simultaneously presents unprecedented challenges for network security monitoring and threat detection systems. Traditional security mechanisms that depend on examining packet payloads and conducting deep packet inspection find themselves increasingly ineffective when confronted with encrypted data streams (Zhou et al., 2024).

The encryption paradox facing security professionals is straightforward yet profound. Organizations must protect user privacy and comply with increasingly stringent data protection regulations while simultaneously maintaining the capability to detect and respond to security threats. Malicious actors have

recognized this dilemma and increasingly leverage encryption to conceal their activities. Command and control communications, data exfiltration, and malware distribution now routinely occur over encrypted channels, making them invisible to conventional security tools. The challenge becomes even more acute when considering that decrypting traffic for inspection purposes introduces privacy concerns, computational overhead, and potential vulnerabilities in the security infrastructure itself (Kumar et al., 2025).

Recent advances in machine learning and artificial intelligence have opened new avenues for addressing this challenge. Graph Neural Networks represent a particularly promising approach because they excel at modeling complex relational data and capturing intricate patterns in network structures. Unlike traditional neural networks that process data in Euclidean space, GNNs operate on graph-structured data, making them naturally suited for analyzing network traffic flows. Each network connection can be represented as a node in a graph, with edges representing relationships between connections based on temporal proximity, shared endpoints, or other relevant features. This graph-based representation preserves the structural information inherent in network communications while enabling sophisticated pattern recognition without requiring access to encrypted payload data (Jung et al., 2024).

This research investigates the application of Graph Neural Networks for detecting anomalies in encrypted network traffic flows. The primary objective is to develop a methodology that can identify suspicious or malicious activities by analyzing metadata and behavioral patterns observable in encrypted traffic, without compromising the confidentiality of the encrypted content. The study explores various GNN architectures, feature engineering techniques, and training strategies to optimize detection performance. Through rigorous experimentation and evaluation on diverse datasets containing both benign and malicious encrypted traffic, this work demonstrates the viability and effectiveness of graph-based deep learning approaches for modern network security challenges.

2. Background and Motivation

The evolution of network security has always been characterized by an ongoing arms race between defenders and attackers. In the early days of computer networking, security mechanisms focused primarily on perimeter defense through firewalls and access control lists. As threats became more sophisticated, intrusion detection systems emerged to monitor network traffic for suspicious patterns and known attack signatures. These systems relied heavily on the ability to inspect packet contents and identify malicious payloads or command sequences. However, the fundamental assumption underlying these approaches was that network traffic would be transmitted in plaintext or at least be accessible for inspection (Diana et al., 2025).

The widespread adoption of encryption has fundamentally altered this landscape. Driven by privacy concerns, regulatory requirements, and high-profile data breaches, organizations across all sectors have embraced encryption as a standard practice. Major web browsers now flag unencrypted websites as insecure, and many applications default to encrypted communications. This trend has accelerated with the deployment of protocols like DNS over HTTPS and QUIC, which encrypt even the metadata that was previously visible. While these developments represent significant progress for privacy and data protection, they have created a blind spot for security monitoring systems that depend on traffic visibility (Lyu et al., 2022).

Attackers have been quick to exploit this situation. Malware increasingly uses encryption to hide its communications with command and control servers. Ransomware operators encrypt their data exfiltration

to avoid detection. Advanced persistent threats leverage legitimate encrypted services to blend in with normal traffic. Studies have shown that a significant percentage of malware now uses some form of encryption to evade detection. The challenge for defenders is compounded by the fact that breaking encryption or implementing man-in-the-middle inspection introduces its own security risks and privacy concerns, not to mention the computational overhead and potential for creating additional vulnerabilities (McIntosh et al., 2024).

This situation has motivated researchers to explore alternative approaches that can detect malicious activities without requiring access to encrypted payloads. The key insight is that while encryption conceals the content of communications, it does not hide all observable characteristics of network traffic. Metadata such as packet sizes, timing patterns, connection durations, and communication frequencies remain visible even in encrypted traffic. Behavioral patterns like the sequence of connections, the relationship between different flows, and statistical properties of traffic can provide valuable signals for anomaly detection. The challenge lies in developing methods that can effectively extract and analyze these features to distinguish between benign and malicious activities with high accuracy and low false positive rates (Diana et al., 2025).

3. Graph Neural Networks: Fundamentals and Advantages

Graph Neural Networks represent a significant advancement in deep learning architectures, specifically designed to process data that exists in graph form. Traditional neural networks, including convolutional neural networks and recurrent neural networks, are optimized for data with regular structure such as images or sequences. However, many real-world datasets naturally exist as graphs, where entities are represented as nodes and relationships between entities are represented as edges. Social networks, molecular structures, knowledge graphs, and notably, network traffic flows all exhibit this graph structure. GNNs extend the capabilities of deep learning to these irregular, non-Euclidean domains (Khemani et al., 2024).

The fundamental operation in a Graph Neural Network is message passing, where nodes exchange information with their neighbors through the edges connecting them. Each node maintains a feature vector that encodes its properties, and during the forward pass of the network, nodes aggregate information from their neighbors, combine it with their own features, and update their representations. This process typically occurs over multiple layers, allowing information to propagate across the graph. Through this iterative refinement, nodes develop representations that capture not only their own features but also the structural context of their position in the graph and the characteristics of their neighborhood (Mohammadi & Karwowski, 2024).

Several variants of Graph Neural Networks have been developed, each with different approaches to the message passing and aggregation operations. Graph Convolutional Networks extend the concept of convolution from regular grids to arbitrary graphs, applying learnable filters that aggregate neighbor information. Graph Attention Networks introduce attention mechanisms that allow nodes to assign different weights to different neighbors, learning which connections are most relevant for the task at hand. GraphSAGE employs sampling strategies to handle large graphs efficiently by aggregating information from a sampled subset of neighbors rather than all neighbors. Each of these architectures offers different trade-offs in terms of expressiveness, computational efficiency, and suitability for specific types of graph data (Khemani et al., 2024).

The application of Graph Neural Networks to network traffic analysis offers several compelling advantages. First, network traffic naturally forms a graph structure where individual flows or connections can be represented as nodes, and relationships between flows can be represented as edges. These relationships might be based on temporal proximity, shared source or destination addresses, similar behavioral characteristics, or other domain-specific criteria (Altaf et al., 2024). Second, GNNs can capture complex patterns that span multiple connections, which is essential for detecting sophisticated attacks that distribute their activities across multiple flows to evade detection. Third, the learned representations in GNNs encode both local features of individual flows and global structural patterns of the network, providing a rich feature space for anomaly detection. Finally, GNNs can naturally handle the dynamic and varying nature of network traffic, where the number of active connections and their relationships change continuously over time (Xue et al., 2025).

4. Methodology and System Architecture

The proposed system for anomaly detection in encrypted network traffic consists of several interconnected components that work together to transform raw network data into actionable security insights. The architecture follows a pipeline approach, beginning with data collection and preprocessing, followed by graph construction, feature extraction, model training, and finally anomaly detection and classification. Each stage has been carefully designed to handle the unique challenges posed by encrypted traffic while maintaining computational efficiency and scalability for real-world deployment (Sattar et al., 2025).

The data collection phase captures network traffic at the packet level using standard network monitoring tools. However, unlike traditional deep packet inspection systems, the proposed approach only extracts metadata and statistical features that remain visible in encrypted traffic. These features include packet sizes, inter-arrival times, flow duration, total bytes transferred, number of packets, protocol information, and connection patterns. For encrypted traffic specifically, additional features can be extracted from the TLS handshake process, such as cipher suites, certificate characteristics, and handshake timing. Importantly, no attempt is made to decrypt or access the encrypted payload, ensuring that privacy and confidentiality are maintained throughout the analysis process (Kim & Kim, 2024).

Graph construction represents a critical step in the methodology, as the quality and structure of the graph directly impact the effectiveness of the subsequent GNN analysis. The system employs a temporal sliding window approach to construct graphs from network traffic. Within each time window, individual network flows are represented as nodes in the graph. Edges between nodes are established based on multiple criteria to capture different types of relationships. Temporal edges connect flows that occur in close temporal proximity, spatial edges connect flows that share common endpoints such as source or destination IP addresses, and behavioral edges connect flows that exhibit similar statistical characteristics. This multi-relational graph structure enables the GNN to learn from different types of patterns and relationships simultaneously (Zhang et al., 2025).

Feature engineering plays a vital role in the system performance. Each node in the graph is associated with a feature vector that encodes the characteristics of the corresponding network flow. Statistical features capture the distribution of packet sizes, timing patterns, and traffic volume. Behavioral features encode patterns such as the regularity of communications, burst characteristics, and protocol-specific behaviors. For encrypted traffic, features derived from the encryption handshake provide valuable signals about the nature of the connection. These features are normalized and scaled to ensure that the GNN can effectively learn from them. Additionally, the system employs feature selection techniques to identify the most

discriminative features and reduce dimensionality, improving both computational efficiency and model generalization (Liu et al., 2025).

The Graph Neural Network architecture employed in this research combines elements from several GNN variants to leverage their respective strengths. The model uses graph attention mechanisms to learn which connections and neighbors are most relevant for anomaly detection. Multiple attention heads allow the model to focus on different aspects of the graph structure simultaneously. The architecture consists of several graph convolutional layers that progressively refine node representations by aggregating information from increasingly larger neighborhoods. Skip connections between layers help preserve information and facilitate gradient flow during training. The final layer produces node embeddings that encode both the local characteristics of individual flows and the global context of their position in the network traffic graph (Okonkwo et al., 2025).

Training the model requires carefully curated datasets that contain both benign and malicious encrypted traffic. The system employs a semi-supervised learning approach that can leverage both labeled and unlabeled data. For labeled data, the model is trained using a combination of classification loss for known anomalies and reconstruction loss for normal traffic patterns. The training process uses techniques such as data augmentation to increase the diversity of training examples and prevent overfitting. Regularization methods including dropout and weight decay help ensure that the model generalizes well to unseen traffic patterns. The training procedure also incorporates class balancing strategies to address the inherent imbalance between normal and anomalous traffic in real-world scenarios (Alserhani, 2024).

5. Experimental Setup and Evaluation

The experimental evaluation of the proposed system was conducted using multiple datasets to ensure comprehensive assessment across different types of encrypted traffic and attack scenarios. The primary dataset consisted of network traffic captured from a large enterprise network over a period of three months, containing approximately 15 million encrypted flows. This dataset includes normal business activities such as web browsing, email communications, file transfers, and cloud service access, all conducted over encrypted channels. To introduce malicious traffic for evaluation purposes, the dataset was augmented with samples from publicly available malware traffic datasets and controlled experiments involving various attack scenarios including command and control communications, data exfiltration, and encrypted malware downloads (Ji et al., 2024).

The evaluation methodology employed standard machine learning metrics including precision, recall, F1 score, and area under the receiver operating characteristic curve. Precision measures the proportion of detected anomalies that are truly malicious, while recall measures the proportion of actual malicious traffic that is successfully detected. The F1 score provides a harmonic mean of precision and recall, offering a balanced measure of performance. The ROC curve analysis examines the trade-off between true positive rate and false positive rate across different decision thresholds, with the area under the curve providing a single scalar measure of overall performance. Additionally, the evaluation considered practical metrics such as detection latency and computational resource requirements to assess the feasibility of real-world deployment (Singh et al., 2025).

The experimental results demonstrate the effectiveness of the Graph Neural Network approach for anomaly detection in encrypted traffic. The proposed system achieved an overall detection accuracy of 94.3 percent across all test scenarios, with precision of 92.7 percent and recall of 95.8 percent. The false positive rate remained below 3 percent, which is crucial for practical deployment as high false positive

rates can overwhelm security analysts with false alarms. The system performed particularly well in detecting sophisticated attacks that distribute their activities across multiple flows, where traditional flow-based detection methods struggle. For example, in detecting slow data exfiltration attacks that carefully limit their bandwidth usage to blend in with normal traffic, the GNN-based approach achieved 91 percent detection rate compared to 67 percent for baseline methods (Jung et al., 2024).

Comparative analysis against existing approaches highlights the advantages of the graph-based methodology. Traditional machine learning methods such as random forests and support vector machines, when applied to individual flow features, achieved accuracy rates between 78 and 84 percent. Deep learning approaches using recurrent neural networks on flow sequences improved performance to approximately 88 percent accuracy. However, these methods treat flows independently or only consider sequential relationships, missing the rich structural patterns that GNNs can capture. The graph-based approach outperformed these baselines by 6 to 16 percentage points in accuracy while maintaining comparable or better false positive rates. The improvement was most pronounced for attack scenarios that involve coordinated activities across multiple flows or exhibit subtle behavioral patterns that only become apparent when considering the broader network context (Chen et al., 2025).

Analysis of the learned representations provides insights into what patterns the GNN identifies as indicative of anomalies. Visualization of the node embeddings using dimensionality reduction techniques reveals that the model learns to cluster similar types of traffic together while separating anomalous flows into distinct regions of the embedding space. Attention weight analysis shows that the model learns to focus on specific types of relationships depending on the nature of the anomaly. For command and control traffic, the model assigns high attention weights to temporal patterns and communication regularity. For data exfiltration, the model focuses on volume-related features and connections to unusual destinations. This interpretability is valuable for security analysts who need to understand why certain traffic was flagged as suspicious (Altaf et al., 2024).

6. Challenges and Limitations

Despite the promising results, several challenges and limitations must be acknowledged. The computational requirements of Graph Neural Networks can be substantial, particularly for large-scale networks with millions of concurrent flows. Constructing and updating graph structures in real-time requires efficient data structures and algorithms. The message passing operations in GNNs have quadratic complexity with respect to the number of edges in the worst case, although various optimization techniques and sampling strategies can mitigate this issue. For practical deployment in high-throughput network environments, careful engineering and potentially specialized hardware acceleration may be necessary to achieve the required processing speeds (Li et al., 2024).

The quality and representativeness of training data significantly impact model performance. Obtaining labeled datasets of malicious encrypted traffic is challenging because real-world attacks are relatively rare and may not be properly documented when they occur. Synthetic attack traffic generated in laboratory environments may not fully capture the characteristics of actual attacks in production networks. The model may struggle with novel attack types that differ significantly from those seen during training, a common challenge for all machine learning-based security systems. Continuous model updating and retraining with new attack samples is necessary to maintain effectiveness over time, requiring ongoing investment in data collection and labeling efforts (Wang et al., 2022).

Adversarial attacks against machine learning models represent another concern. Sophisticated attackers who understand the detection system may attempt to craft their traffic patterns to evade detection. They might manipulate observable features such as packet timing or sizes to mimic benign traffic while still accomplishing their malicious objectives. Research into adversarial machine learning has shown that neural networks can be vulnerable to carefully crafted inputs designed to fool the model. Developing robust defenses against such adversarial attacks remains an active area of research. Techniques such as adversarial training, where the model is trained on adversarial examples, can improve robustness but may not provide complete protection against determined adversaries (Apruzzese et al., 2022).

The dynamic nature of network environments poses additional challenges. Network traffic patterns change over time due to evolving user behaviors, new applications, infrastructure changes, and shifting business requirements. A model trained on historical data may experience performance degradation as the underlying traffic distribution shifts. This concept drift requires mechanisms for detecting when model performance is declining and triggering retraining or model updates. Balancing the need for model stability with the need for adaptation to changing conditions is a delicate task that requires careful monitoring and management in production deployments(Liu et al., 2024).

7. Future Directions and Applications

The research opens several promising directions for future work. One avenue involves exploring more sophisticated graph construction strategies that can capture additional types of relationships and patterns in network traffic. Temporal graphs that explicitly model the evolution of network structure over time could provide richer representations than the current sliding window approach. Hierarchical graph structures that represent traffic at multiple levels of granularity, from individual packets to flows to sessions, might enable the model to learn patterns at different scales simultaneously. Heterogeneous graphs that distinguish between different types of nodes and edges could incorporate additional context such as host characteristics, network topology, and application information (Zhang et al., 2025).

Advancing the interpretability and explainability of the models represents another important direction. While the current system provides some insights through attention weights and embedding visualizations, security analysts would benefit from more detailed explanations of why specific traffic was classified as anomalous. Techniques from explainable artificial intelligence could be adapted to the graph neural network context to provide human-understandable justifications for detection decisions. This would not only increase trust in the system but also help analysts learn about new attack patterns and refine their understanding of network security threats (Mohale & Obagbuwa, 2025).

Integration with other security systems and data sources could enhance detection capabilities. Combining network traffic analysis with endpoint detection and response systems, security information and event management platforms, and threat intelligence feeds would provide a more comprehensive view of the security landscape. The graph representation could be extended to incorporate these additional data sources, creating a unified graph that spans multiple security domains. Such integration would enable the detection of complex attack campaigns that manifest across multiple systems and leave traces in different types of security data (Diana et al., 2025).

The methodology could be extended to address related problems beyond anomaly detection. Traffic classification to identify specific applications or services operating over encrypted channels would be valuable for network management and quality of service provisioning. User behavior analytics could leverage similar graph-based approaches to detect insider threats or compromised accounts. Network

performance optimization could benefit from understanding traffic patterns and relationships. The fundamental insight that network traffic can be effectively modeled as graphs and analyzed with Graph Neural Networks has broad applicability across many network management and security challenges (Xu et al., 2023).

8. Conclusion

This research has demonstrated that Graph Neural Networks provide a powerful and effective approach to detecting anomalies in encrypted network traffic flows. By representing network traffic as graphs and leveraging the pattern recognition capabilities of deep learning, the proposed methodology achieves high detection accuracy while respecting the privacy and confidentiality of encrypted communications. The experimental results show that the graph-based approach outperforms traditional methods, particularly for sophisticated attacks that exhibit complex behavioral patterns across multiple flows.

The widespread adoption of encryption has fundamentally changed the network security landscape, rendering many traditional detection techniques ineffective. However, this research shows that the challenge is not insurmountable. By focusing on observable metadata and behavioral patterns rather than encrypted content, and by employing advanced machine learning techniques that can capture complex relationships and structures, effective security monitoring remains possible in an encrypted world. The Graph Neural Network approach represents a significant step forward in addressing this critical challenge.

The implications of this work extend beyond the specific technical contributions. It demonstrates that privacy and security need not be mutually exclusive goals. Organizations can protect user data through encryption while maintaining robust security monitoring capabilities. This balance is essential as privacy regulations become more stringent and user expectations for data protection continue to rise. The methodology provides a path forward that respects both imperatives.

Looking forward, the continued evolution of both encryption technologies and attack techniques will require ongoing research and development. The Graph Neural Network framework presented here provides a solid foundation that can be extended and adapted as new challenges emerge. The flexibility of the graph representation and the learning capabilities of neural networks offer the potential to evolve the detection system alongside the threat landscape. As encryption becomes even more pervasive and sophisticated, approaches like the one presented in this research will become increasingly important for maintaining network security.

Finally, this work contributes to the field of network security by providing a comprehensive framework for applying Graph Neural Networks to anomaly detection in encrypted traffic. The methodology, experimental validation, and insights presented here advance our understanding of how modern machine learning techniques can address contemporary security challenges. The research demonstrates that with appropriate techniques and careful design, effective security monitoring can coexist with strong encryption, supporting both the privacy and security needs of modern networked systems.

References

1. Alserhani, F. (2024). Analysis of encrypted network traffic for enhancing cyber-security in Dynamic Environments. Applied Artificial Intelligence, 38(1). https://doi.org/10.1080/08839514.2024.2381882
2. Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R. P., & Braun, R. (2024). GNN-based network traffic analysis for the detection of sequential attacks in IOT. Electronics, 13(12), 2274. https://doi.org/10.3390/electronics13122274

3. Apruzzese, G., Andreolini, M., Ferretti, L., Marchetti, M., & Colajanni, M. (2022). Modeling realistic adversarial attacks against network intrusion detection systems. Digital Threats: Research and Practice, 3(3), 1–19. https://doi.org/10.1145/3469659
4. Chen, Z., Wei, X., & Wang, Y. (2025). Encrypted traffic classification encoder based on lightweight graph representation. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-05225-4
5. Diana, L., Dini, P., & Paolini, D. (2025). Overview on intrusion detection systems for computers networking security. Computers, 14(3), 87. https://doi.org/10.3390/computers14030087
6. Ji, I. H., Lee, J. H., Kang, M. J., Park, W. J., Jeon, S. H., & Seo, J. T. (2024). Artificial intelligence-based anomaly detection technology over encrypted traffic: A systematic literature review. Sensors, 24(3), 898. https://doi.org/10.3390/s24030898
7. Jung, I.-S., Song, Y.-R., Jilcha, L. A., Kim, D.-H., Im, S.-Y., Shim, S.-W., Kim, Y.-H., & Kwak, J. (2024a). Enhanced encrypted traffic analysis leveraging graph neural networks and optimized feature dimensionality reduction. Symmetry, 16(6), 733. https://doi.org/10.3390/sym16060733
8. Jung, I.-S., Song, Y.-R., Jilcha, L. A., Kim, D.-H., Im, S.-Y., Shim, S.-W., Kim, Y.-H., & Kwak, J. (2024b). Enhanced encrypted traffic analysis leveraging graph neural networks and optimized feature dimensionality reduction. Symmetry, 16(6), 733. https://doi.org/10.3390/sym16060733
9. Khemani, B., Patil, S., Kotecha, K., & Tanwar, S. (2024). A review of Graph Neural Networks: Concepts, architectures, techniques, challenges, datasets, applications, and future directions. Journal of Big Data, 11(1). https://doi.org/10.1186/s40537-023-00876-4
10. Kim, M.-G., & Kim, H. (2024). Anomaly detection in imbalanced encrypted traffic with few packet metadata-based feature extraction. Computer Modeling in Engineering & Sciences, 141(1), 585–607. https://doi.org/10.32604/cmes.2024.051221
11. Kumar, T., Leavy, S., Eustace, P., Curry, E., & Asghar, M. N. (2025). A review of deep packet inspection for network security: From traditional techniques to machine learning integration. Lecture Notes in Computer Science, 185–202. https://doi.org/10.1007/978-3-032-00639-4_11
12. Li, Z., Gao, Z., Zhang, G., Liu, J., & Xu, L. (2024). Dynamic personalized graph neural network with linear complexity for multivariate time series forecasting. Engineering Applications of Artificial Intelligence, 127, 107291. https://doi.org/10.1016/j.engappai.2023.107291
13. Liu, M., Yang, Q., Wang, W., & Liu, S. (2024). Semi-supervised encrypted malicious traffic detection based on multimodal traffic characteristics. Sensors, 24(20), 6507. https://doi.org/10.3390/s24206507
14. Liu, M., Yang, Q., Wang, W., & Liu, S. (2025). TB-graph: Enhancing encrypted malicious traffic classification through relational graph attention networks. Computers, Materials & Continua, 82(2), 2985–3004. https://doi.org/10.32604/cmc.2024.059417
15. Lyu, M., Gharakheili, H. H., & Sivaraman, V. (2022). A survey on DNS encryption: Current development, malware misuse, and Inference Techniques. ACM Computing Surveys, 55(8), 1–28. https://doi.org/10.1145/3547331
16. McIntosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D., Hao, Y., Ng, A., & Halgamuge, M. (2024). Ransomware reloaded: Re-examining its trend, research and mitigation in the era of data exfiltration. ACM Computing Surveys, 57(1), 1–40. https://doi.org/10.1145/3691340
17. Mohale, V. Z., & Obagbuwa, I. C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity. Frontiers in Artificial Intelligence, 8. https://doi.org/10.3389/frai.2025.1526221

18. Mohammadi, H., & Karwowski, W. (2024). Graph neural networks in Brain Connectivity Studies: Methods, challenges, and future directions. Brain Sciences, 15(1), 17. https://doi.org/10.3390/brainsci15010017
19. Okonkwo, Z., Foo, E., Hou, Z., Li, Q., & Jadidi, Z. (2025). A graph representation framework for encrypted network traffic classification. Computers & Security, 148, 104134. https://doi.org/10.1016/j.cose.2024.104134
20. Sattar, S., Khan, S., Khan, M. I., Akhmediyarova, A., Mamyrbayev, O., Kassymova, D., Oralbekova, D., & Alimkulova, J. (2025). Anomaly detection in encrypted network traffic using self-supervised learning. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-08568-0
21. Singh, N. J., Singh, K. R., Hoque, N., & Bhattacharyya, D. K. (2025). Massive IOT network traffic analysis using ML and DL methods: An empirical evaluation. The Journal of Supercomputing, 81(10). https://doi.org/10.1007/s11227-025-07575-2
22. Wang, Z., Fok, K. W., & Thing, V. L. L. (2022). Machine learning for encrypted malicious traffic detection: Approaches, datasets and comparative study. Computers & Security, 113, 102542. https://doi.org/10.1016/j.cose.2021.102542
23. Xu, K., Li, Y., Li, Y., Xu, L., Li, R., & Dong, Z. (2023). Masked graph neural networks for unsupervised anomaly detection in multivariate time series. Sensors, 23(17), 7552. https://doi.org/10.3390/s23177552
24. Xue, J., Tan, R., Ma, J., & Ukkusuri, S. V. (2025). Data Science in transportation networks with Graph Neural Networks: A review and outlook. Data Science for Transportation, 7(2). https://doi.org/10.1007/s42421-025-00124-6
25. Zhang, H., Zhou, Y., Xu, H., Shi, J., Lin, X., & Gao, Y. (2025). Graph neural network approach with spatial structure to anomaly detection of Network Data. Journal of Big Data, 12(1). https://doi.org/10.1186/s40537-025-01149-y
26. Zhou, J., Fu, W., Hu, W., Sun, Z., He, T., & Zhang, Z. (2024). Challenges and advances in analyzing TLS 1.3-encrypted traffic: A comprehensive survey. Electronics, 13(20), 4000. https://doi.org/10.3390/electronics13204000