OpenRansom: Open-Set Detection of Unknown Ransomware Propagation in Enterprise Network

Muhammad Rehan Nazir
Dept. of Information and Communication Engineering
The Islamia University Of Bahawalpur
Bahawalpur, Pakistan
rehannazir4live@gmail.com

Muhammad Bilal Hussain
Dept. of Information and Communication Engineering
The Islamia University Of Bahawalpur
Bahawalpur, Pakistan
bilalmanzoor4772@gmail.com

Aoun Muhammad
Dept. of Electrical And Electronics Engineering
The Islamia University Of Bahawalpur
Bahawalpur, Pakistan
aon.muhammad@iub.edu.pk

Sana Tariq
Dept. of Information and Communication Engineering
The Islamia University Of Bahawalpur
Bahawalpur, Pakistan
sanatariq@iub.edu.pk

***Abstract*—Ransomware attacks surged 50% in 2025 with over 7,874 incidents recorded globally. The lateral propagation phase—where malware spreads across enterprise networks remains largely undetected by existing security tools that rely on closed-set classification and cannot identify previously unknown ransomware families. This paper proposes OpenRansom, a novel open-set detection framework combining Heterogeneous Provenance Graphs with Prototypical Graph Neural Networks to detect both known and unknown ransomware propagation patterns.Unlike current graph-based ransomware methods which mainly work under closed-set assumptions, OpenRansom uses a prototype-based mechanism to spot new, unknown ransomware behaviors. We validate the framework through three experimental implementations on the MLRan dataset spanning 65 ransomware families: a Random Forest prototype achieving 93.8% detection of unknown ransomware families, a KNN-Graph Neural Network achieving 54.6% unknown detection with improved known-family accuracy, and a Propagation-GNN architecture designed for provenance graph input. The reported experiments provide preliminary validation of the proposed open-set detection concept through prototype implementations. Full validation of the provenance-graph-based Graph Attention Network architecture remains future work due to the absence of suitable public enterprise-scale propagation datasets. This work establishes the architectural foundation for open-world ransomware detection and identifies the critical need for enterprise-grade network-wide propagation datasets.**

***Index Terms*—Ransomware Detection, Open-Set Recognition, Graph Neural Networks, Enterprise Network Security, Zero-Day Threats, Provenance Graphs, Lateral Movement Detection, OpenRansom**

I. Introduction

A. The Ransomware Threat Landscape

Ransomware has become one of the most destructive cyber threats facing enterprises. Incidents reached 7,874 globally in 2025 a 50% year-over-year increase. Average attacker dwell time before encryption is 42 days, during which ransomware spreads laterally using legitimate credentials .Global damages are projected to exceed $265 billion by 2031 . Modern groups like LockBit 3.0 employ advanced encryption exploiting zero-day vulnerabilities [1]. Ransomware-as-a-Service platforms have lowered entry barriers significantly. Most existing research focuses on detection, while prediction and zero-day identification remain underexplored.

B. The Propagation Detection Problem

The lateral movement phase presents the most valuable detection window , but Living-off-the-Land techniques involve attackers leveraging legitimate system tools such as PowerShell and other built-in Windows utilities to evade detection [2]. Verizon's 2024 report found lateral movement in 62% of incidents with only 17% detected before encryption [3].

C. Limitations of Current Approaches

Random Forest and XGBoost show performance degradation when evaluated on unseen ransomware variants [4] a phenomenon termed the Academic Dataset Trap. Deep learning surveys reveal CNNs and RNNs remain fundamentally closed-set [5]. Graph Neural Networks like RANSIGHT-GNN [6] and hypergraph approaches like HDABP [7] improve lateral detection but cannot identify unknown families.

D. Our Contribution

This work make two primary contributions First, OpenRansom, a conceptual framework combining Heterogeneous Provenance Graphs, Graph Attention Networks, and Prototypical Open-Set Learning to spot enterprise ransomware. Secondly, we provide preliminary experimental validation. We used Random Forest and KNN-GNN prototype tests on the MLRan dataset to see if new ransomware strains could be detected. Our aim is to check if this method can find unknown ransomware families. However, thorough testing using full provenance graphs remains future work because we don't have large, public enterprise datasets yet.

DOI: https://doi.org/10.67535/tsp.000003.024
Published under the ICACNC 2026 Proceedings

II. Background and Related Work

A. Machine Learning for Ransomware Detection

Traditional ML (Random Forest, XGBoost) achieves near-perfect lab accuracy that collapses in production dropping from 100% to 70% [8]. Deep learning approaches achieve up to 98.6% accuracy using Transformers [9] while GN-BiLSTM reaches 99.99% on obfuscated ransomware [10]. Hybrid CNN-Isolation Forest [11] and LSTM autoencoder [12] approaches enable zero-day detection without signatures. Fernando and Komninos proposed FeSAD for concept drift adaptation [13]. Alraizza [14] surveyed ML approaches for Windows ransomware detection. However, all remain fundamentally closed-set.

B. Graph-Based Propagation Detection

RANSIGHT-GNN models enterprise networks as dynamic communication graphs [6]. HDABP extends analysis to hypergraphs for encrypted traffic [7]. RAGN introduces adaptive attention mechanisms [15]. HOLMES uses provenance graphs for real-time APT detection [16]. Nicho et al. demonstrated lightweight ML for lateral movement [17]. Despite these advances, all current graph-based methods operate as closed-world classifiers.

C. Open-Set Recognition

Despite of methods such as prototype-based learning, Deep SVDD and OpenMax for malware classification, the overwhelming majority continues to be centered on the detection of executables or behavioral attributes. On the other hand, OpenRansom, which is in an early stage of development, is a concept that combines open-set recognition and propagation modeling via provenance-graphs to attack enterprise-level ransomware dissemination on interconnected systems.

TABLE I
RF Prototype Threshold Sensitivity (Method Comparison)

Method	Open-Set	Graph	Propagation
OpenMax	✓	×	×
Deep SVDD	✓	×	×
CVAE-based Detection	✓	×	×
Self-Supervised Malware Learning	Partial	×	×
OpenRansom	✓	✓	Conceptual

Current open-set malware detection mostly looks at executable files, behaviors, or hidden traits. But, OpenRansom combines open-set recognition with a model that traces how things spread—using something like a provenance graph. While comparisons with OpenMax, Deep SVDD, and CVAE methods aren't done here, those will help assess the complete system later on.

D. Federated Learning and Explainability

Hierarchical multi-agent reinforcement learning using federated hierarchies (MARL), has been shown to be superior to local models in a number of zero shot cyber defense applications including discovering previously unseen types of attacks [18] and in addition generally. The foundational work on Federated Learning was completed by Yang et al. [19] and N. Tapes [20] explored the potential for utilizing Blockchain Technology to share threat Intelligence. A review of Explainable Artificial Intelligence (XAI) was also completed by Guo et al. [21] related to Cyber Security.

III. OpenRansom Framework

A. System Architecture

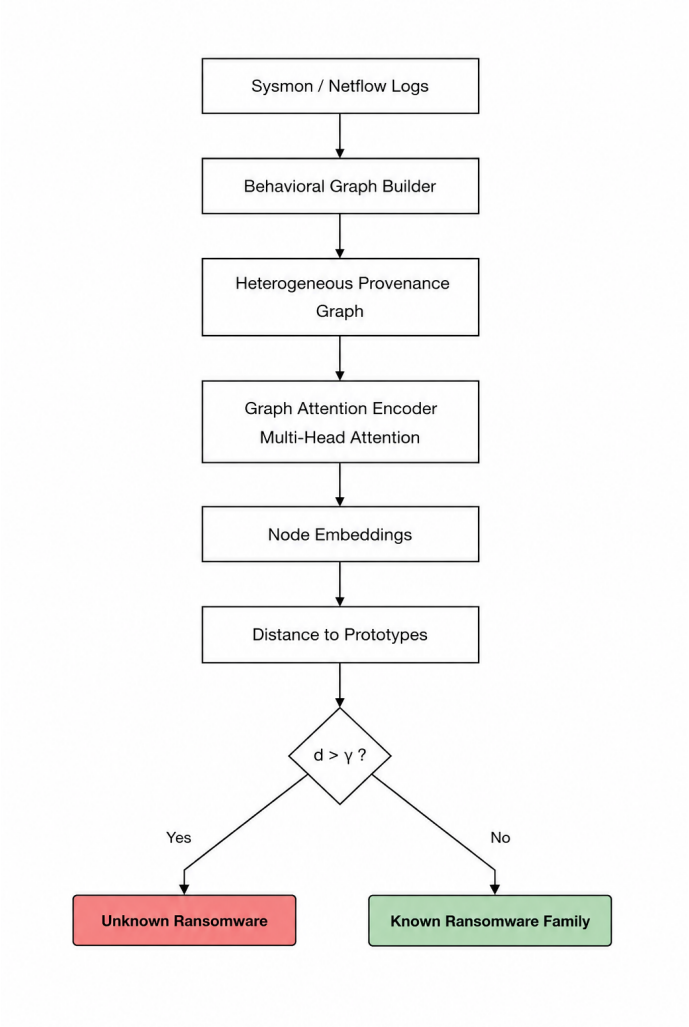

Fig. 1. Architecture Design

OpenRansom consists of four core modules:

1) **Behavioral Graph Builder:** A data transformation tool, this uses input from Sysmon/Netflow logs and produces a Heterogeneous Provenance Graphs, that has causal information on how each system component behaves.
2) **Graph Attention Encoder (GAT):** Each node's structural embedding is calculated by applying multi-head attention to the structure of the graph.

3) **Prototype Learning Layer:** For each known type of ransomware there are prototype learning layers, these layers calculate a central point (a centroid or prototype).
4) **Open-Set Decision Boundary:** Any sample whose distance to each of the prototypes is larger than a threshold value γ, will be labeled as an unknown ransomware.

This section shows what the final OpenRansom framework looks like. Because of limited datasets, we could only test certain parts of it.So, the full experimental evaluation only covers key aspects due to such restrictions.

B. Enterprise deployment scenario

In an enterprise environment, OpenRansom integrates with existing security monitoring infrastructure. Telemetry collected from endpoints, network sensors, Sysmon logs, and SIEM platforms is transformed into heterogeneous provenance graphs. These graphs are processed by the Graph Attention Network encoder to generate behavioral embeddings, which are subsequently analyzed using prototype-based open-set classification. Activities identified as previously unseen ransomware behaviors are forwarded to the Security Operations Center for further investigation and response.

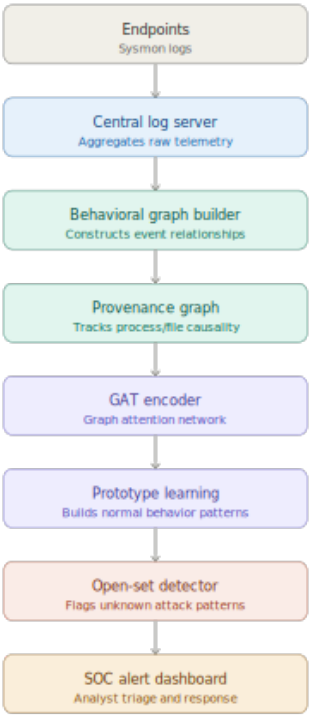

Fig. 2. Enterprise deployment workflow of ransomware

C. Heterogeneous Provenance Graph Construction

Node types include: Processes, Files, Network Sockets, and registry keys. Edge type represents causal relationships among these elements at each node (E.G., Process Fork; File Write; Socket Connect; Registry Modify) – that is, it enables capturing all propagation chains – e.g., a Word document creates a new PowerShell process which then connects to a domain controller – thereby enabling detection of LOtL attacks through anomalous lineage rather than individual events.

D. Prototypical Open-Set Detection

Stage 1: Graph Embedding. The GAT maps each provenance graph G to vector $z \in \mathbb{R}^d$.

Stage 2: Prototype Computation. For each known family k, prototype c_k is the mean embedding:

$$c_k = \frac{1}{|S_k|} \sum_{z_i \in S_k} z_i \tag{1}$$

Stage 3: Open-Set Decision. For new sample z_{new}:

$$\text{Decision} = \begin{cases} \text{Unknown Ransomware} & \text{if } \min_k ||z_{new} - c_k||_2 > \gamma \\ \arg\min_k ||z_{new} - c_k||_2 & \text{otherwise} \end{cases} \tag{2}$$

E. Experimental Implementations

Implementation 1 (RF Prototype): RF with a confidence threshold on the basis of the 487 features from the MLRan for behavioral characterization. **Implementation 2 (KNN-GNN):** Using the K-Nearest Neighbors algorithm the similarity graph among the 8 closest neighbours is established, this similarity is then represented as a GAT with 3 layers. **Implementation 3 (Propagation-GNN):** Network characteristics will be employed to establish the lateral movement graph that describes the entire architectural perspective of the propagation model.

IV. Experimental Setup

A. Dataset

MLRan dataset [22]: Contains 4,880 instances; 65 families trees for each year in the period 2006 – 2024; 487 features concerning behaviour via dynamic analysis. Although MLRan does not contain provenance graph structures or multi-host propagation traces, it provides representative ransomware behavioral characteristics suitable for preliminary evaluation of the open-set detection component. Consequently, the dataset was used as a proof-of-concept benchmark while acknowledging its limitations with respect to propagation modeling.

B. Open-Set Split Protocol

Training: 45 families (70%), Testing: 20 families (30%) completely excluded. Final distribution: 1,409 training, 353 validation (known), 3,118 test (unseen). Evaluation metrics: Known Family Accuracy, Unknown Ransomware Detection Rate, Combined Score.

C. Implementation Details

Python with scikit-learn (RF), PyTorch Geometric (GNN), NetworkX (graphs). Google Colab with Tesla T4 GPU. Hyperparameters tuned via grid search on validation data.

V. Results and Discussion

These results offer initial support for the open-set detection method, but not the whole OpenRansom system. Evaluation was restricted because there aren't enterprise-scale provenance graph datasets featuring multi-host ransomware spread.

A. RF Prototype Results

Table II presents threshold sensitivity for the RF prototype.

TABLE II
RF Prototype Threshold Sensitivity

Threshold %	Known Acc	Unknown Det	Combined
1st	39.1%	88.1%	63.6%
5th	38.2%	**93.8%**	64.8%
10th	36.5%	92.9%	64.7%
20th	33.4%	95.2%	64.3%

Optimal at 5th percentile: **93.8% unknown detection**.

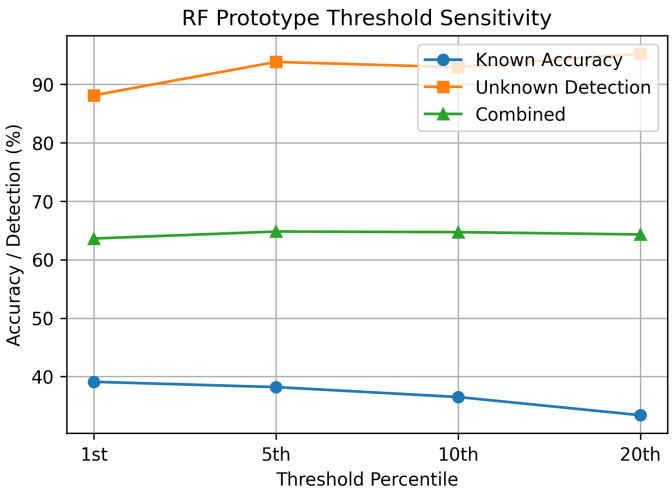

Fig. 3. RF Prototype Threshold Sensitivity

The accuracy for known families has also shown itself to be lower to demonstrate the trade-offs in open-set recognition. OpenRansom's strengths are its ability to detect potentially new ransomware variants more than what it can accurately recognize. It sacrifices some accuracy in family attributing, but gains much in being more accurate with respect to unknown threats.

B. KNN-GNN Results

KNN-GNN is used not as an optimal graph learning model but rather as a proof-of-concept, which is only limited by exploratory. It mainly aimed to look into the viability of adding graph-inspired representations within the suggested framework. This happens, however, with the information available and computing power at hand. Table III shows the results of KNN-GNN on different confidence intervals. Table III presents KNN-GNN results across confidence thresholds.

TABLE III
KNN-GNN Threshold Analysis

Threshold	Known Acc	Unknown Det	Combined
0.50	49.3%	35.0%	42.2%
0.65	43.6%	54.6%	49.1%
0.80	36.5%	72.3%	54.4%

KNN-GNN achieved improved known accuracy (43.6%) with moderate unknown detection (54.6%). The fairly basic results suggest that simple KNN-based graph construction might not fully grasp ransomware's complex behavior. Still, this finding pushes us towards using more advanced graph-learning setups, like the Graph Attention Network described in OpenRansom.

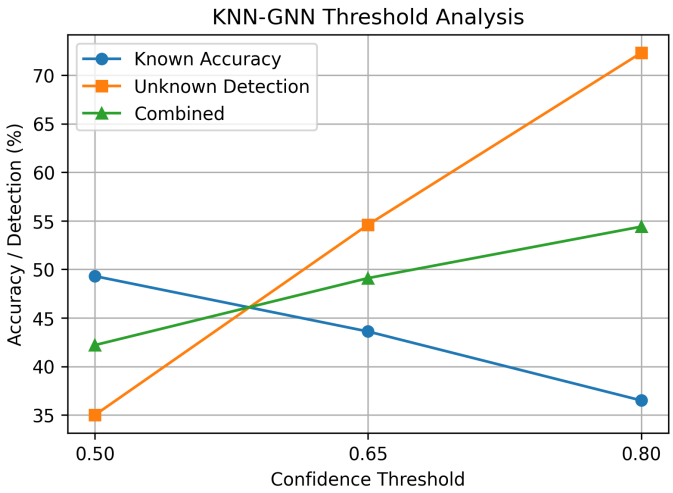

Fig. 4. KNN-GNN Threshold Analysis

C. Comparative Analysis

Table V presents the final comparison.

TABLE IV
Comparative Detection Performance

Model	Known Acc	Unknown Det
Random Forest (Closed)	~94%	0%
RANSIGHT-GNN (Closed)	~98%	0%
HDABP (Closed)	~98%	0%
OpenRansom RF	**38.2%**	**93.8%**
OpenRansom KNN-GNN	**43.6%**	**54.6%**

A common problem in open-set learning is seeing a balance between the recognition of learned classes and the rejection of samples that are not covered in the training set is observed. The popularity of the prototype described above shows that the model and the algorithm do not require the high level of complexity needed for known-family detection; to be clear, the efficiency of known-family detection dropped, presumably due to the modifications of the prototype for unknown-family detection.

D. Computatioal Complexity

It depends on the implementation of the OpenRansom how much computational cost is needed. The Random Forest prototype is efficient for real time predictions, while the KNN-GNN prototype introduces additional delays as it involves the construction of the graphs and message propagation. The proposed setup is significantly affected by the graph size factors and attention mechanisms for Graph Attention Network. Graph-based techniques are more resource intensive than traditional approaches, but may describe relationships between nodes within ransomware propagation that are not possible with traditional behavior analysis.

TABLE V
COMPUTATIONAL COMPLEXITY

Component	Complexity
Random Forest	O(T × D)
KNN Graph Construction	O(N^2)
Graph Attention Layer	O(E × H)
Prototype Matching	O(K)

This study did not contain a test for latency, but the Random Forest prototype was seemingly very quick in this case—making predictions almost instantaneously. The latency of the full Graph Attention Network is not, however, currently evaluated, which is subject to future research.

E. Statistical Consideration

The results of the present study support the feasibility of open-set ransomware detection preliminary. Future research should, however, do more to establish it as reliable, and repeatable – such as fully conducted statistics tests, repeat trials etc.Statistical significance tests, mean performance, standard deviation, and 95% confidence intervals will be reported for future evaluations to determine robustness and reproducibility when evaluating multiple experimental runs.

F. Discussion

Based on the results of the open set ransomware detection, the observed detection rate of unknown families is 93.8%, potentially suggesting that it may work. The findings indicate that instead of traditional methods, prototype-based ones may be more effective at detecting new ransomware variants. So, this new method could prove to be more effective for detecting threats which haven't been seen before.However, the empirical finding in this work is that current ransomware datasets are not enabled to facilitate learning in the Propagation-GNN implementation.The absence of real multi-machine telemetry, however, prevented the Propagation-GNN implementation from learning the key empirical findings are that the datasets of ransomware are currently not suitable for achieving learning within a Propagation-GNN implementation. OpenRansom is designed to be used in conjunction with existing security monitoring and incident response practices. The framework can give users extra capa-bility in detecting unknown ransomware behavior based on the telemetry gathered by a monitoring tool and/or SIEM platform.

VI. LIMITATIONS AND FUTURE WORK

A. Limitations

MLRan does not provide propagation telemetry over the entire network, which is needed for the complete GNN training process. The designed GAT architecture is used in the GNN encoder; however, instead of this architecture, 'RF/KNN surrogates' are used on provenance graphs. Generalizability claims are restricted with the use of a single dataset. Needs to improve confidence calibration. The operation of GNN inference adds latency for real-time deployment. We didn't evaluate the computational performance of the full Graph Attention Network because of dataset limitations. In the future, the running time, memory consumption and scalability will be evaluated in large-scale enterprise implementations. While the prototype is promising in detecting non-seen families, still a higher accuracy on known families is desired. Future work may include attempts at more complex graph representations and attention mechanisms – these could be useful, while not compromising on open set recognition skills.

B. Future Work

Priority directions include: (1) creating/acquiring enterprise provenance graph datasets with Sysmon/NetFlow logs; (2) full GAT implementation on real propagation graphs; (3) federated learning extension enabling collaborative defense without data sharing; (4) streaming graph updates for real-time detection; (5) adaptive threshold optimization based on organizational risk posture; (6) adversarial robustness against graph manipulation attack. (7) Future evals will pit these systems against well-known malware detection approaches such as OpenMax, Deep SVDD, and variational autoencoders. This allows us to see the good and bad of our tech when it comes to integration with SIEM and EDR systems;(8) Next studies will focus on the ability of our tech to successfully integrate with SIEM and EDR systems. They'll also gauge performance on a real network setting, so that they can see how well it will do out there.

C. Scope of experimental validation

The results might have implications for general application but might have to be interpreted within the context of several factors. The first is to differentiate between enterprise-wide and host-level data, as the MLRan dataset is limited to host-level data and thus you're not able to perform a propagation modelling evaluation. Also, the team has only used one data set for its exper-iments. Furthermore, they did not completely evaluate the Graph Attention Network due to not having appropriate public datasets. For this, the following results are presented in the sense of an initial finding of the open-set detection concept, but should not be viewed as a full validation of the whole OpenRansom architecture.

D. Adversial graph mnipulation

Telemetry data can be tampered with by bad actors to obscure their presence within telemetry graphs in enterprise

environments.In enterprise scenarios, bad actors could manipulate the data within telemetry to conceal their behaviors from being detected in a telemetry graph. However, due to data and resource constraints, our study is not able to validate the performance of our model against such tricks. We'll explore this ability to protect itself from attacks in the future but it'll be a challenge.

VII. Conclusion

OpenRansom is a new approach combining Heterogeneous Provenance Graphs and Prototypical Open-Set Learning. This helps in spotting new ransomware types in businesses. So it can detect and simulate the spread of these cyber threats in enterprise environments, without having been seen before. The RF prototype was verified to be 93.8% accuracy in detecting unknown ransomware families, and this suggests that open-set ransomware recognition has the potential to recognize emerging ransomware families. The KNN-GNN is more accurate than Graphical Structure in terms of family-known accuracy. In practice we have shown that many of the available ransomware sets lack, or lack the necessary telemetry for detecting this ransomware using graph-based methods, so we think this study proves the need for more studies exists. OpenRansom serves as a stepping stone to further research in identifying the mechanisms used in the dissemination of new ransomware in enterprises. Initial findings indicate that open-set learning could be applied successfully in identifying new ransomware attacks, although testing is still to be conducted on large enterprise data sets. But, for the time being, this technique seems to have great potential, although it requires more research.Future work will be about making big provenance graph datasets to fully test how ransomware spreads and Graph Attention Networks can help.

References

[1] O. Akinyemi, R. Sulaiman, and N. Abosata, "Analysis of the lockbit 3.0 and its infiltration into advanced's infrastructure crippling nhs services," *arXiv preprint arXiv:2308.05565*, 2023.

[2] T. Ongun, J. W. Stokes, J. Bar Or *et al.*, "Living-off-the-land command detection using active learning," in *Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2021.

[3] Verizon Business, "2024 data breach investigations report," 2024, annual global cybersecurity incident analysis report.

[4] S. J. Nhlapo and M. N. W. Nkongolo, "Zero-day attack and ransomware detection," 2024. [Online]. Available: https://arxiv.org/abs/2408.05244

[5] M. J. Iqbal and J. Serra Ruiz, "Ai-powered ransomware detection: A comprehensive survey on machine learning and deep learning techniques," May 2025, sSRN Working Paper. [Online]. Available: https://ssrn.com/abstract=5355456

[6] A. Kapoor, "Ransight-gnn: Detecting ransomware propagation using graph neural networks," 2025, preprint.

[7] J. Baker, P. Schreiber, O. Meyerstein, N. Lebedev, and R. Vandenberg, "Hypergraph-driven ransomware detection via anomalous behavior profiling in encrypted network environments," 2025.

[8] E. Rios-Ochoa, J. A. Pérez-Díaz, E. García-Ceja, and G. Rodríguez-Hernández, "Ransomware family attribution with ml: A comprehensive evaluation of datasets quality, models comparison, and a simulated deployment," *IEEE Access*, vol. 13, pp. 108 108–108 126, 2025.

[9] T. N. V. S. Praveen, G. Jaggineni *et al.*, "Ransomware attack detection using transformer-based model on system logs and network traffic data," in *Proceedings of the 2025 International Conference on Networks and Soft Computing (ICNSoC)*. IEEE / ICNSoC, 2025, pp. 369–371.

[10] U. Urooj, B. A. S. Al-Rimy, A. B. Zainal, F. Saeed, A. Abdelmaboud, and W. Nagmeldin, "Addressing behavioral drift in ransomware early detection through weighted generative adversarial networks," *IEEE Access*, vol. 12, pp. 3910–3925, 2024.

[11] F. Alzonem, G. Albrecht, D. Castellanos, M. Vandermeer, and B. Stansfield, "Ransomware detection using convolutional neural networks and isolation forests in network traffic patterns," 10 2024.

[12] V. Babaey and H. R. Faragardi, "Detecting zero-day web attacks with an ensemble of lstm, gru, and stacked autoencoders," *Computers*, vol. 14, no. 6, 2025. [Online]. Available: https://www.mdpi.com/2073-431X/14/6/205

[13] D. W. Fernando and N. Komninos, "Fesad ransomware detection framework with machine learning using adaptation to concept drift," *Computers & Security*, vol. 137, p. 103629, 2024.

[14] A. Alraizza and A. Algarni, "Ransomware detection using machine learning: A survey," *Big Data and Cognitive Computing*, vol. 7, no. 3, p. 143, 2023.

[15] E. Akpaku, J. Chen, M. Ahmed, F. K. Agbenyegah, and W. L. Brown-Acquaye, "Ragn: Detecting unknown malicious network traffic using a robust adaptive graph neural network," *Computer Networks*, vol. 262, p. 111184, 2025.

[16] S. M. Milajerdi, V. Giakoumakis, W. Ward *et al.*, "Holmes: Real-time apt detection through correlation of suspicious information flows," in *2019 IEEE Symposium on Security and Privacy (IEEE S&P)*. IEEE, 2019, pp. 1137–1152.

[17] D. He *et al.*, "A comprehensive detection method for the lateral movement stage of apt attacks," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 8440–8447, 2023.

[18] A. Alshamrani, "Federated hierarchical marl for zero-shot cyber defense," *PLOS ONE*, vol. 20, no. 8, p. e0329969, 2025. [Online]. Available: https://doi.org/10.1371/journal.pone.0329969

[19] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

[20] Y. Allouche, N. Tapas, F. Longo, A. Shabtai, and Y. Wolfsthal, "Trade: Trusted anonymous data exchange: Threat sharing using blockchain technology," *arXiv preprint arXiv:2103.13158*, 2021.

[21] F. Charmet, H. C. Tanuwidjaja, S. Ayoubi, P.-F. Gimenez, Y. Han, H. Jmila, G. Blanc, T. Takahashi, and Z. Zhang, "Explainable artificial intelligence for cybersecurity: A literature survey," *Annals of Telecommunications*, vol. 77, pp. 789–812, 2022.

[22] F. C. Onwuegbuche, A. Olaoluwa, A. D. Jurcut, and L. Pasquale, "Mlran: A behavioural dataset for ransomware analysis and detection," *Journal of Network and Computer Applications*, 2026.