Leveraging Multilayer Threat Graph Detection Techniques for Correlation and Risk Assessment

1st YuCheng Lin
Department of Information and Finance Management
National Taipei University of Technology
Taipei, Taiwan
t109ab0752@ntut.org.tw

2nd PoTing Lu
Computer Science and Information Engineering
Fu Jen Catholic University
Taipei, Taiwan
amos040425@outlook.com

3rd YuJie Wang
Computer Science and Information Engineering
Ming Chuan University
Taipei, Taiwan
a844536170@gmail.com

4th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

Falcon Wang
ATD
WNC
Hsinchu, Taiwan
falcon.wang@wnc.com.tw

Eric Mao
ATD
WNC
Hsinchu, Taiwan
eric.mao@wnc.com.tw

***Abstract*—As cyber threats grow in complexity and scope, traditional security measures prove increasingly inadequate. This paper presents an advanced intelligent detection tool tailored to address these evolving threats through a sophisticated multi-layer network threat graph. This innovative tool amalgamates data from network traffic, intrusion detection systems, and system logs to provide a comprehensive view of network security dynamics. Leveraging state-of-the-art artificial intelligence technologies, including machine learning and deep learning, the tool excels in identifying both known and emerging security threats. It achieves this by analyzing extensive datasets to detect abnormal behaviors and anomalous network patterns. The resulting multi-layer threat graph not only depicts network connections and anomalies visually but also significantly augments the ability of security teams to rapidly comprehend and respond to security threats. This abstract details the design, development, and practical application of the intelligent detection tool, emphasizing its efficacy in converting raw data into actionable security insights via sophisticated AI-driven analysis and visualization techniques. The proposed approach enhances immediate threat detection and facilitates strategic security planning and risk assessment.**

Keywords: Cybersecurity, Network Threat Analysis, Artificial Intelligence, Machine Learning, Deep Learning, Data Visualization, Threat Detection.

***Index Terms*—Threat Detection, Graph Theory, Risk Assessment, Multilayer Analysis**

I. Introduction

As network attacks grow increasingly sophisticated and diverse, traditional security measures are struggling to keep pace, highlighting a pressing need for more advanced solutions. This paper introduces an innovative intelligent detection tool designed to address these evolving challenges through the creation of a multi-layer network threat graph. The tool analyzes network traffic, event logs from Network Intrusion Detection Systems (NIDS), and system logs from monitoring devices to offer a comprehensive view of network security status. This holistic approach enables security analysts to assess network conditions from multiple dimensions, thus enhancing their ability to identify and respond to potential security threats effectively.

The primary challenge addressed by this tool involves the application of advanced artificial intelligence technologies to perform deep analyses of extensive network data. By implementing machine learning algorithms, the tool can distinguish abnormal network packets, pinpoint hosts exhibiting anomalous behaviors, and analyze behavioral clusters. This capability allows for the detection of both known and unknown security threats, including covert threats that might elude traditional security solutions.

Additionally, the intelligent detection tool visualizes complex analysis results in a multi-layered graph. This multi-layer threat graph not only illustrates the connections and interactions between network nodes but also accentuates abnormal events and the distribution of anomalous behaviors. Such visualizations provide an intuitive, easily comprehensible format for security teams to quickly assess the overall security situation of the network, recognize patterns of vulnerabilities, and identify attack behaviors. The graph offers various analytical entry points, facilitating a multifaceted approach to security analysiswhether tracking specific security incidents, studying general network communication patterns, or investigating the propagation paths of malicious activities.

This paper details the design, development, and implemen-

tation of the intelligent detection tool, aimed at equipping organizations with a sophisticated, multi-layered perspective on network security. Incorporating cutting-edge artificial intelligence techniques, including machine learning, deep learning, and big data analytics, the tool conducts an in-depth analysis of data from diverse sources. Key topics such as data preprocessing, AI analysis techniques, and the creation and visualization of the multi-layer network threat graph are discussed, illustrating the tool's development process, implementation strategies, and practical advantages. This overview provides a comprehensive framework for leveraging multi-layer threat graph detection to analyze and assess the correlation and risk of heterogeneous data.

II. Related Work

A. Emerging Research Themes in Cybersecurity Applications

The cybersecurity landscape is continuously reshaped by advancements in web technologies, mobile platforms, and the Internet of Things (IoT). Primary research efforts focus on detecting and analyzing vulnerabilities in online social networks (OSNs), enhancing browser security, and assessing the security frameworks of mobile applications. Recent studies highlight a pronounced emphasis on analytical methodologies over data collection, pinpointing significant concerns about the evolution of browser threats through extensions and fingerprinting techniques [7]. Additionally, the mobile app ecosystem is subjected to rigorous scrutiny, particularly in terms of how apps interact with operating systems and utilize third-party libraries to ensure security [7]. IoT devices, noted for their diversity and pervasive integration, present formidable security challenges. Research in this field employs techniques such as Internet scanning, honeypots, and malware analysis to identify and mitigate vulnerabilities. These efforts underscore the necessity for adaptive security strategies to counter the rapidly evolving digital threats in the IoT landscape [7].

B. Multilayer and Multidimensional Security Analysis

The escalating sophistication of network threats has spurred the development of advanced security frameworks, notably multilayer and multidimensional architectures. These frameworks integrate multiple levels of protection, forging a resilient defense against cyber threats [1]. Such architectures feature overlapping defense layers throughout IT systems, ensuring comprehensive protection even in the event of breaches [2]. A prime example of this strategy is the use of Network Intrusion Detection Systems (NIDS), which monitor network traffic to detect anomalies and mitigate intrusionsthereby safeguarding against data breaches and financial losses [3]. Further enhancing these security measures, the integration of machine learning and big data analytics has revolutionized threat detection. Tools like IBMs QRadar and Splunk leverage these technologies to detect subtle threats and expedite incident response times [4]. Recent innovations in this domain include a novel multi-stage IDS that utilizes a simplified Cyber Kill Chain model along with Graph Neural Network (GNN) algorithms. This approach has been particularly effective in detecting complex, evolving attacks, significantly enhancing detection capabilities and reducing false positives in critical sectors such as finance and government [5], [6].

C. Artificial Intelligence in Network Security

As network environments grow increasingly complex with the proliferation of 5G and Internet of Things (IoT) technologies, traditional security measures are becoming inadequate. This research explores the application of machine learning (ML) techniques in developing an Intrusion Detection System (IDS) that effectively counters sophisticated cyber threats, such as Krack and Kr00k attacks targeting IEEE 802.11 protocols. Leveraging the AWID3 dataset, our ML models have demonstrated remarkable effectiveness, achieving a 99This study highlights the pivotal role of advanced computational techniques in addressing the challenges posed by emerging cybersecurity threats. By incorporating ML into our security frameworks, the developed models not only increase detection accuracy but also offer scalable solutions adaptable to complex network infrastructures. Future research will aim at refining these models to further improve the effectiveness of IDS, contributing towards more secure and resilient network systems [10], [11].

D. Multisource Data Integration and Analysis Techniques

The rapid expansion of the internet and online platforms has significantly heightened exposure to cyber threats, necessitating advanced detection mechanisms. This research introduces a cutting-edge method that combines large language models with a synchronized attention mechanism, significantly enhancing the detection of cyberattack behaviors. Our extensive experiments across various datasetsincluding server logs, financial transactions, and social media commentsdemonstrate this method's superiority over traditional models like the Transformer and BERT in terms of precision, recall, and accuracy. Notably, our approach achieved a precision of 93% on the server log dataset, markedly outperforming existing methods [12]–[14]. In conclusion, this innovative integration of large language models with synchronized attention mechanisms has proven to be highly effective in enhancing the accuracy and efficiency of cyberattack behavior detection. Comprehensive testing on diverse datasets has confirmed the method's effectiveness, consistently showing superior performance metrics compared to established models. This approach not only deepens our understanding of complex attack patterns but also facilitates robust multisource data integration, marking a significant advancement in cybersecurity technologies [15]–[17].

E. Dynamic Threat Graphs and Visualization Techniques

Cybersecurity knowledge graphs (CKGs) leverage graph-based models to enhance cyber situational awareness and enable comprehensive cyber threat analysis. These CKGs integrate vast volumes of heterogeneous system data using advanced graph data models, which facilitate automated reasoning and the visualization of complex network dynamics and

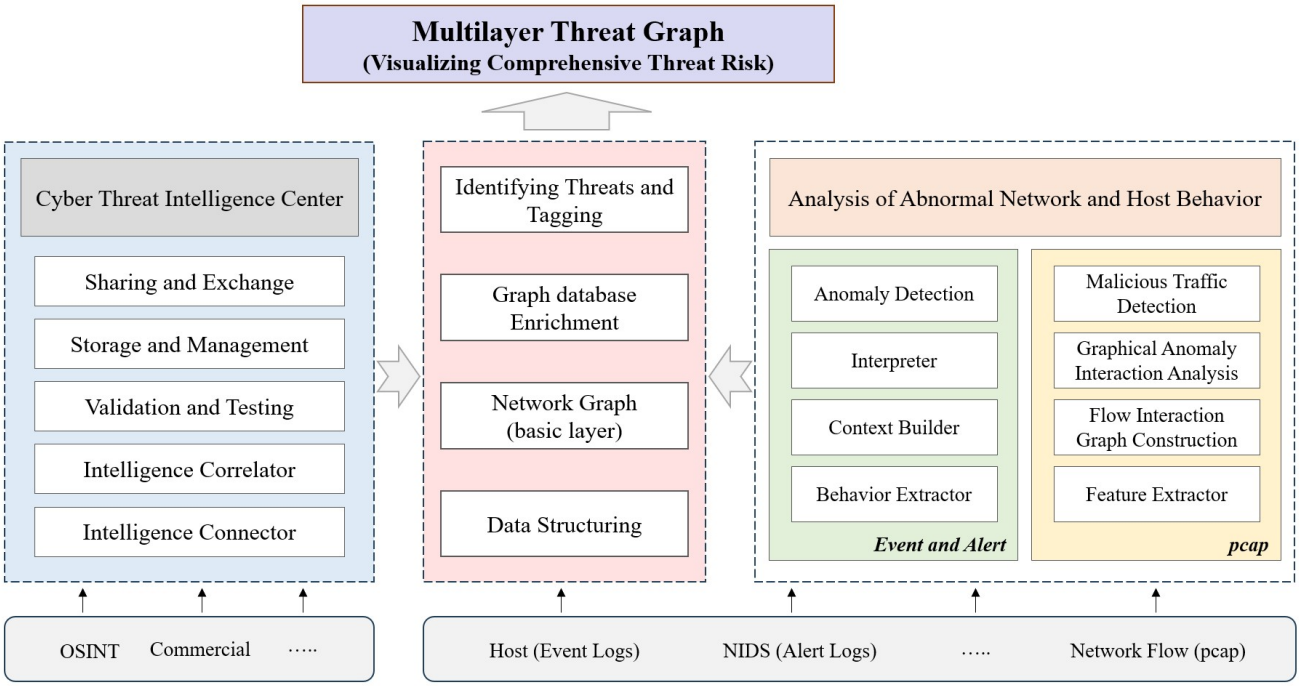

Fig. 1. Overview of the Overall System Architecture

attack paths. The adoption of RDF graphs, labeled property graphs, and other sophisticated models allows for the effective organization and manipulation of cybersecurity data, significantly enhancing detection and analytical capabilities [18]–[20]. The formalization of cybersecurity data into CKGs not only promotes standardization in terminology and reasoning but also supports advanced data integration and visualization techniques. This synthesis is essential for constructing robust defenses against increasingly sophisticated cyber threats, proving invaluable in domains such as cybersecurity and digital forensics. The strategic use of CKGs enhances our ability to anticipate, visualize, and mitigate potential threats in real-time, providing a critical edge in the ongoing battle against cybercrime [21]–[23].

III. System Architecture

A. The Cyber Threat Intelligence Center (CTIC)

The Cyber Threat Intelligence Center (CTIC) collects threat intelligence from various sources, including attack events, malware reports, vulnerability disclosures, and more. These threat intelligence data typically contain entities associated with specific attacks, such as attackers, victims, tools used, attack vectors, and so forth. When presenting information relationships, the Threat Graph can visualize these entities in a graphical manner, enabling users to clearly see their interconnections. CTIC's analysis of threat intelligence can also be utilized to identify attack behaviors and patterns, which can be represented in the Threat Graph as specific types of nodes or edges. Additionally, threat intelligence can be rated and prioritized to assist organizations in more effectively responding to threats. In the Threat Graph, different colors or sizes can be used to indicate the severity and priority of threats, enabling users to quickly identify and respond to the most critical threats. The CTIC's integration with the Threat Graph helps organizations gain a clearer understanding of the threat landscape and more effectively respond to various threats. Through presenting information relationships, the Threat Graph can become a powerful tool for visualizing threat intelligence and supporting organizational security decision-making. The Cyber Threat Intelligence Center comprises several key modules designed to enhance cyber defense capabilities by processing and managing threat intelligence efficiently. Below is a detailed overview of each module:

1) **Intelligence Connector:** This module collects threat intelligence from a variety of sources, including public databases, private intelligence feeds, and partner-shared data. It aggregates this information and prepares it for analysis, ensuring a comprehensive data pool is available for threat assessment.
2) **Intelligence Correlator:** It analyzes and correlates the collected intelligence to identify potential attack patterns, threat behaviors, and underlying security risks. This module compares new data with historical threat information to detect emerging attack trends and vulnerabilities.
3) **Validation and Testing:** This module assesses the credibility and accuracy of the threat intelligence gathered. Tasks include source verification, authenticity validation of the reported threats, and testing how the applied in-

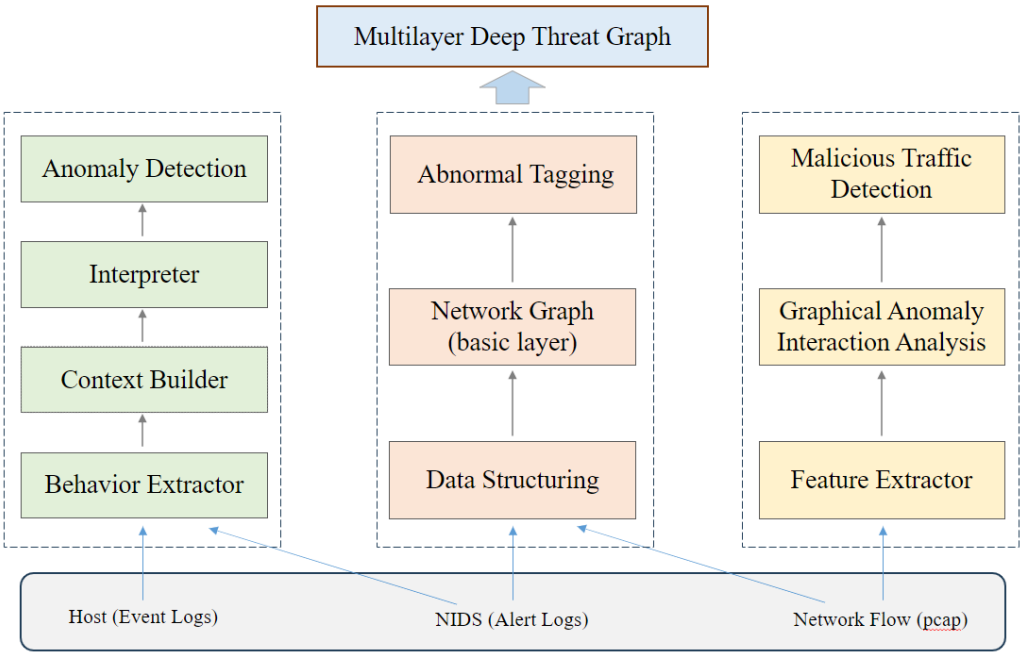

Fig. 2. Detailed Overview of the System Components

telligence holds up in simulated environments to ensure its efficacy.

4) **Storage and Management:** Responsible for the secure storage and management of threat intelligence. It ensures the integrity, confidentiality, and availability of data, and manages access controls to prevent unauthorized access to sensitive information.
5) **Sharing and Exchange:** Facilitates the sharing and exchange of threat intelligence with external entities, such as other organizations and security communities. This exchange broadens the reach and effectiveness of the intelligence gathered, enhancing collective awareness and response capabilities against cyber threats.

B. Anomaly Detection and Interpretation

This model primarily focuses on the analysis of event logs and NIDS (Network Intrusion Detection System) alert logs using advanced tools such as DeepLog or DeepCase. The core objective is to predict subsequent events and determine whether they constitute anomalous behavior, thereby aiming to reduce false alarm rates and enhance anomaly detection. Both event logs and alert logs are analyzed by extracting their respective identifiersEvent IDs for event logs and Signature IDs for alert logs. The model then examines the sequential relationships of these identifiers to identify potential irregularities and ascertain anomalies.

1) Behavioral Pattern Extraction: This component is crucial for extracting behavioral patterns from the data supplied by hosts, particularly focusing on event logs and alert logs to identify deviations from normal operations that may indicate potential security threats.

a) Event Logs:: For event logs, the process begins by converting log files (typically in .evtx format) into a more manageable JSON format. Subsequently, a specialized module extracts the time series data, which is then saved in a text file (.txt). This transformation is critical for isolating and analyzing behavior patterns over time, allowing for the identification of anomalies that deviate from established norms.

b) Alert Logs:: Similarly, for alert logs, network traffic data stored in .pcap format is processed using the Suricata engine to generate alerts. These alerts are then converted by the module into a time series format and saved as text files (.txt). This process is designed to capture and evaluate the sequence of events that may signal unauthorized or malicious activities within the network.

By systematically transforming and analyzing these logs, the component enhances the capability to detect and respond to potential security threats efficiently, ensuring that only the most relevant data is considered in the ongoing security assessment.

2) Context Builder: The Context Builder is designed to enhance the accuracy and relevance of anomaly detection by integrating contextual information into the data interpretation process. This component encompasses both preprocessing and analysis steps:

The preprocessing stage involves transforming input files into a structured format necessary for model input. This includes a mapping process where each event in the input file is replaced with a specific coderanging from 0 to the number of events, with the final code, -1337, representing a blank space. It also constructs context by converting the sequence into a list composed of the previous ‘n‘ sequences, which can

be customized based on the model's needs.

Following preprocessing, the Context Builder employs a Deep LSTM network that uses the structured input to train the model and generate confidence values. It selects the top 'k' predictions based on these values to ensure precise anomaly detection. This advanced model excels at identifying contextually relevant events and distinguishing those triggered by malicious attacks from those inadvertently triggered by benign applications or user behaviors. This capability is vital for building an attention vector that accurately reflects security threats, as highlighted in the relevant literature.

3) Interpreter: The Interpreter component is essential for transforming incoming data from unstructured or semi-structured forms into a structured format suitable for further anomaly analysis. This transformation is crucial for accurately identifying deviations from typical patterns.

The subsystem also includes an "Attention Query" mechanism, which plays a critical role in evaluating the effectiveness of the predictions made. If an incorrect event is predicted, leading to erroneous conclusions, a manual review is initiated to ensure accuracy. This step highlights the model's capability to revert to manual checks when automated predictions fail, thus maintaining the integrity of the analysis.

Additionally, the Attention Query considers actual security incidents to determine which type of attention distribution results in correct predictions. This analysis helps in refining the predictive model to improve its accuracy and reliability in real-world scenarios.

4) Anomaly Detection: This model focuses on predicting anomalies in specific hosts over determined periods by calculating and scoring deviations from normal activity sequences. The anomaly scores help in assessing the severity and potential impact of disruptions, enabling prioritized responses and better resource allocation for threat mitigation. This method enhances both immediate and long-term security measures by allowing ongoing monitoring and trend analysis.

C. Tagging and Network Analysis

This model rigorously analyzes NIDS (Network Intrusion Detection System) alert logs alongside network flow pcap (Packet Capture) files. It effectively structures these data sources and leverages this structured data to construct an intricate network graph. This graph is instrumental in visualizing complex network interactions and pinpointing potential security threats with enhanced accuracy.

1) Data Structuring: This phase involves the meticulous organization of raw data into a structured format, integrating heterogeneous data sources, notably NIDS alert logs and pcap files. Such integration is crucial for the preliminary identification and characterization of anomalies in network traffic, serving as a foundational step for subsequent analytical processes.

2) Abnormal Tagging: Post data structuring, this critical process involves the systematic classification and labeling of data instances that exhibit anomalous behaviors. By applying advanced tagging algorithms, this step significantly enhances the targeted analysis of potential threats, streamlining the detection and response mechanisms.

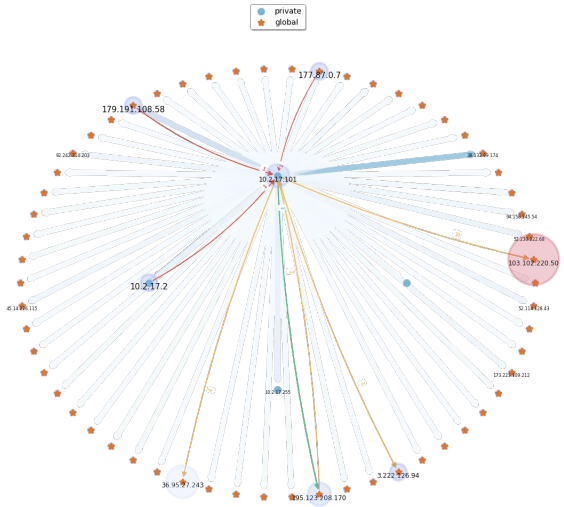

Fig. 3. Multilayer Network Threat Graph Example

3) Network Graph Construction: This stage entails the creation of a dynamic network graph that provides a visual framework for the analysis of network interactions. This graph is pivotal in tracing the pathways of threat dispersion and understanding the interconnectivity within the network, thereby facilitating a comprehensive threat assessment.

4) Multilayer Network Threat Visualization: Figure 6 exemplifies a sophisticated multilayer network threat map. This visualization allows users to intuitively comprehend the security posture within the network environment, facilitating the identification of key nodes, the severity of incidents, and the intricacies of network connectivity. The diagram elaborately represents node interactions, using color and shape variations to convey detailed security insights.

Nodes in Figure 6 are highlighted with halos, indicating a high incidence of security alerts. These halos emphasize nodes that require heightened scrutiny. Nodes are distinctly categorized by their IP address characteristics into internal, private IPs and public, internet-facing IPs. Internal IPs are denoted by light blue dots, while external IPs are marked with yellow stars, enabling swift identification of node types by users.

Inter-node connections are illustrated with lines colored to indicate the severity of alerts: red for critical severity (level 3), yellow for moderate severity (level 2), and green for low severity (level 1). Hosts with extensive network connections are depicted with bold blue lines, which vary in intensity with the connection frequency. This feature assists users in identifying potential high-risk connections even without specific event triggers.

The innovative design of this multilayer network threat map not only offers a panoramic view of the network's security

landscape but also empowers users to rapidly pinpoint and respond to potential security vulnerabilities. By transforming complex security data into a visually intuitive format, this tool significantly enhances the efficacy of security monitoring, analysis, and decision-making processes.

D. Traffic and Feature Analysis

This model, inspired by the advanced methodologies outlined in recent studies, focuses on the evaluation of pcap files for detecting malicious traffic within encrypted flows and extracting significant features for in-depth anomaly analysis [24], [26].

1) Malicious Traffic Detection: Following approaches similar to those in recent works [24], [26], the Enhanced Traffic Graph Analysis Model (ETGAM) categorizes network traffic into short and long flows based on their flow size distribution [25]. This classification is critical for managing the complexity of the network graph and enhancing analysis efficiency. Each flow is evaluated based on a sophisticated loss score that integrates metrics such as the Euclidean distance to the cluster center, the time range, and the flow count, crucial for identifying potential security threats in real-time.

2) Graphical Anomaly Interaction Analysis: Using depth-first search (DFS), similar to the method employed in other advanced systems [26], the network traffic graph is segmented into connected components. Critical nodes identified during this process are analyzed with the Z3 SMT solver to pre-cluster edges for further detailed analysis. The DBSCAN algorithm clusters these components based on their traffic patterns, and subsequent K-Means clustering assesses the structural and flow features connected to critical vertices [24], [26].

3) Feature Extractor: Consistent with the approaches described in [24], [25], feature extraction involves analyzing pcap data to isolate crucial features such as source and destination IPs, ports, connection duration, timestamps, and protocols. These features are fundamental for the classification of network anomalies and ensure that the data is prepared for comprehensive analysis and real-time detection of security threats.

IV. Experiments

A. Introduction

In this section, we present the experimental validation of our proposed intelligent detection tool, comparing its performance against established baseline methods. Our tool focuses on accurately identifying and tracking sophisticated attack patterns by analyzing a variety of network data sources, including both encrypted traffic and interactions from untrusted services. We evaluate the tool's effectiveness in both short-term and extended attack campaigns, highlighting its practical implications for enhancing network security.

B. Experimental Setup

Our experiments are conducted on a virtual machine environment configured on Ubuntu 22.04 LTS, using OpenStack Nova (version 18.2.2). This setup runs on dual Intel Xeon Processors (Skylake, IBRS), each with 4 cores at 2 GHz, and includes 64GiB of ECC RAM to ensure stable and efficient processing.

1) Hardware and Virtual Machine Configuration: The system configuration comprises:

- **CPUs:** Dual 2 GHz Intel Xeon with hyper-threading and virtualization support, essential for simulating complex network scenarios.
- **Memory:** 64GiB of ECC RAM, providing robust error correction capabilities critical for handling large-scale data processing.
- **Storage:** 2TB of disk space across multiple virtual storage devices, facilitating extensive data logging and analysis.
- **Networking:** High-speed Virtio network device optimized for low overhead and high throughput, vital for network traffic analysis.

This VMWare-hosted environment supports our deep learning models and Python-integrated tools, finely tuned for high-volume network traffic simulation and analysis. The setup ensures minimal detection latency and maximizes system responsiveness and accuracy.

C. Dataset and Evaluation Metrics

To ensure a comprehensive evaluation, our methodology incorporates a mix of synthetic, real-world, and third-party datasets, enabling a robust assessment of our detection tool under various conditions:

- The **CICIDS2017 dataset** and **CICIDS2018 dataset** simulate realistic network traffic and attack scenarios, serving as benchmarks for testing intrusion detection systems.
- **Real-world data** from over a hundred computers at The Philippines Office, collected over eight months, adds operational realism and depth to our evaluation.
- We further include datasets from the study by Hublikar and Shet [24], which feature specific attack scenarios such as:
  - Traditional brute force attacks testing the capability of our tool to detect persistent login attempts.
  - Encrypted flooding traffic assessing the effectiveness in recognizing DoS attacks disguised under encryption.
  - Encrypted web malicious traffic evaluating detection of malicious activities conducted through secure web protocols.
  - Malware generated encrypted traffic examining the tools ability to identify malware communication over encrypted channels.

These datasets collectively facilitate a detailed analysis of the tool's performance, with metrics including accuracy, precision, recall, and the F1 score to quantitatively assess its effectiveness across different types of network threats.

D. Testbed Configuration

Our testbed leverages an integrated suite of technologies including Suricata for intrusion detection, OpenCTI for threat intelligence management, and the ELK stack for data processing and visualization, all running on a system that mirrors network traffic to ensure comprehensive monitoring without disrupting actual data flows. This setup enhances our ability to simulate, monitor, and analyze both encrypted and unencrypted network traffic efficiently. Using these tools in conjunction, we achieve real-time threat detection and analysis, with Elasticsearch indexing the vast amounts of data generated, Logstash processing and structuring this data, and Kibana providing immediate visual insights, which collectively support an agile response to emerging security threats.

E. Results

Our experimental results underscore the robustness of our detection system:

- We observed a significant increase in the precision of detecting encrypted malicious trafficup 15%and a 20% increase in recall compared to traditional baseline methods.
- DeepLog's anomaly detection capabilities flagged 20 out of 320 monitored hosts as compromised, significantly enhancing our security posture by identifying vulnerabilities that were previously undetected.

F. Effectiveness Analysis

Our comprehensive evaluation spans multiple attack vectors, yielding insightful results:

- Detailed analysis of network behavior anomalies categorized into 8 distinct types, notably within RDP and P2P traffic, revealing specific patterns.
- Sensitivity analysis to determine optimal parameter settings for maximizing detection accuracy.

G. Deep Threat Analysis

A qualitative assessment conducted by domain experts utilizing our multi-layer threat graph methodology has provided deeper insights into the progression and root causes of attacks, improving our understanding of attack vectors and informing mitigation strategies.

H. Efficiency Analysis and Case Studies

In-depth case studies of Advanced Persistent Threats, specifically APT29 and APT41, demonstrate the practical applicability and efficiency of our detection methodology in real-world scenarios.

I. Discussion

This section synthesizes our experimental findings and discusses their broader implications for advancing cybersecurity measures and shaping future threat hunting strategies. We also explore the potential integration of additional AI-driven analytical tools to expand our security coverage.

V. Conclusion

This paper has presented a comprehensive intelligent detection tool that leverages advanced artificial intelligence techniques to enhance network security through a multi-layer threat graph approach. Our experiments demonstrate that this tool significantly improves the detection of sophisticated and multi-stage cyber threats, outperforming traditional security systems in both synthetic and real-world environments.

A. Key Findings

The key findings from our research include:

- The integration of machine learning and deep learning algorithms enables our tool to effectively identify both known and novel threats by analyzing patterns in network traffic, system logs, and intrusion detection outputs.
- Our experimental results highlight the tool's enhanced capability in precision and recall, particularly in detecting encrypted and anomalous traffic, which are common vectors for advanced persistent threats (APTs).
- The visualization capabilities of the multi-layer threat graph provide intuitive and actionable insights, allowing security teams to swiftly respond to potential threats and understand the broader security landscape.

B. Implications for Cybersecurity

The development of this tool signifies a substantial advancement in cybersecurity practices. By providing a deeper and more nuanced understanding of threat dynamics, our tool supports a proactive security posture, enabling organizations to preemptively address vulnerabilities and mitigate potential attacks more effectively.

C. Future Research Directions

Future research will focus on several key areas to further enhance the detection tool's capabilities:

- **Real-Time Data Processing:** Improving the tool's ability to process and analyze data in real-time will help in quicker threat identification and response.
- **Integration of More Data Sources:** Expanding the types of data inputs to include more varied network and endpoint data will enhance the depth and accuracy of threat detection.
- **Automated Response Mechanisms:** Developing automated response features that can not only detect but also respond to security threats in an automated fashion will be a significant step forward.
- **Cross-Platform Compatibility:** Ensuring the tool is compatible across different platforms and environments will broaden its applicability and utility.

In conclusion, the intelligent detection tool introduced in this paper provides a vital asset in the field of cybersecurity, offering enhanced detection capabilities and a robust framework for future enhancements. As cyber threats continue to evolve, so too must our approaches to detecting and combating them. Our future work will continue to build on this foundation with

the aim of developing a universally applicable, highly adaptive security solution.

REFERENCES

[1] J. Lan, Y. Li, B. Li, and X. Liu, "Matter: A Multi-Level Attention-Enhanced Representation Learning Model for Network Intrusion Detection," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Los Alamitos, CA, USA, IEEE Computer Society, pp. 111–116, Dec. 2022.

[2] D. Mudzingwa et al., "A Study of Methodologies Used in Intrusion Detection and Prevention Systems (IDPS)," in *2012 Proceedings of IEEE Southeastcon*, pp. 1–6, Mar. 2012.

[3] S. Walling and S. Lodh, "A Survey on Intrusion Detection Systems: Types, Datasets, Machine Learning Methods for NIDS and Challenges," in *13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–7, Oct. 2022.

[4] P. V. Pandit et al., "Implementation of Intrusion Detection System Using Various Machine Learning Approaches with Ensemble learning," in *2023 International Conference on Advancement in Computation and Computer Technologies (InCACCT)*, pp. 468–472, May 2023.

[5] J. Straub, "Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATTI&CK and STRIDE Frameworks as Blackboard Architecture Networks," in *2020 IEEE International Conference on Smart Cloud (SmartCloud)*, pp. 148–153, Nov. 2020.

[6] T. N. Kipf and M. Welling, "Semi-supervised Classification with Graph Convolutional Networks," *arXiv preprint arXiv:1609.02907*, Sept. 2017.

[7] M. Safaei Pour, C. Nader, K. Friday, and E. Bou-Harb, "A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security," *Computers & Security*, vol. 128, pp. 103123, 2023, doi: https://doi.org/10.1016/j.cose.2023.103123.

[8] Park J.H., Rathore S., Singh S.K., Salim M.M., Azzaoui A., Kim T.W., Pan Y., Park J.H., "A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions," *Human-Centric Computing and Information Sciences*, vol. 11, article 3, 2021.

[9] Gupta S., Parne B.L., Chaudhari N.S., "Security Vulnerabilities in Handover Authentication Mechanism of 5G Network," in *Proceedings of the 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, Jalandhar, India, pp. 369-374, Dec. 2018.

[10] Borgaonkar R., Tøndel I.A., Degefa M.Z., Jaatun M.G., "Improving Smart Grid Security Through 5G Enabled IoT and Edge Computing," *Concurrency and Computation: Practice and Experience*, vol. 33, e6466, 2021.

[11] Gonzalez A.J., Grønsund P., Dimitriadis A., Reshytnik D., "Information Security in a 5G Facility: An Implementation Experience," in *Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Porto, Portugal, pp. 425-430, June 2021.

[12] Nalendra, A. "Rapid Application Development (RAD) model method for creating an agricultural irrigation system based on internet of things," in *Proceedings of the IOP Conference Series: Materials Science and Engineering*, Sanya, China, IOP Publishing: Bristol, UK, vol. 1098, p. 022103, Nov. 2021.

[13] Chun, J.; Lee, J.; Kim, J.; Lee, S., "An international systematic review of cyberbullying measurements," *Comput. Hum. Behav.*, vol. 113, 106485, 2020.

[14] Wu, J.; Zhang, C.; Liu, Z.; Zhang, E.; Wilson, S.; Zhang, C., "Graphbert: Bridging graph and text for malicious behavior detection on social media," in *Proceedings of the 2022 IEEE International Conference on Data Mining (ICDM)*, Orlando, FL, USA, pp. 548557, Nov.-Dec. 2022.

[15] Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I., "Phishing attacks: A recent comprehensive study and a new anatomy," *Front. Comput. Sci.*, vol. 3, 563060, 2021.

[16] Liu, Q.; Hagenmeyer, V.; Keller, H.B., "A review of rule learning-based intrusion detection systems and their prospects in smart grids," *IEEE Access*, vol. 9, pp. 5754257564, 2021.

[17] Rezaimehr, F.; Dadkhah, C., "A survey of attack detection approaches in collaborative filtering recommender systems," *Artif. Intell. Rev.*, vol. 54, pp. 20112066, 2021.

[18] Zhang K, Liu J, "Review on the application of knowledge graph in cyber security assessment," in *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, vol. 768, p. 052103, 2020.

[19] Sikos LF, "AI-powered cybersecurity: from automated threat detection to adaptive defense," *CISO Mag*, vol. 4, no. 5, pp. 7487, 2020.

[20] Sikos LF, Philp D, Stumptner M, et al., "Visualization of conceptualized dynamic network knowledge for cyber-situational awareness," in *Proceedings of the 8th International Conference on Concept Mapping*, p. 396, 2018.

[21] Johnson JH, "Embracing n-ary relations in network science," in *Advances in Network Science*, Springer, Cham, pp. 147160, 2016.

[22] Sikos LF, Stumptner M, Mayer W, et al., "Representing network knowledge using provenance-aware formalisms for cyber-situational awareness," *Procedia Comput. Sci.*, vol. 126, pp. 2938, 2018.

[23] Garae J, Ko RKL, "Visualization and data provenance trends in decision support for cybersecurity," in *Data Analytics and Decision Support for Cybersecurity*, Springer, Cham, pp. 243270, 2017.

[24] Hublikar, Shivaraj and Shet, N. Shekar V., "Malicious encrypted network traffic flow detection using enhanced optimal deep feature selection with DLSTM," *International Journal of Modeling, Simulation, and Scientific Computing*, vol. 15, no. 01, pp. 2450011, 2024. DOI: 10.1142/S1793962324500119.

[25] Estan, C. and Varghese, G., "New directions in traffic measurement and accounting: Focusing on the elephants, ignoring the mice," *ACM Trans. Comput. Syst.*, vol. 21, no. 3, pp. 270313, 2003.

[26] Eshete, B. and Venkatakrishnan, V. N., "Dynaminer: Leveraging offline infection analytics for on-the-wire malware detection," in *DSN. IEEE*, 2017, pp. 463474.