International Journal of Intelligent Computing Systems

June-2026 | IJICS | Volume-2 Issue-1 | ISSN: 3107-7218

A Cybersecurity Knowledge Graph for Advanced Persistent Threat Organization Attribution

B.Swathi[1], Dr.N.Sujatha[2]

Student[1], Professor[2]

Priyadarshini Institute of Technology & Science for Women, Chintalapudi, Andhra Pradesh, india

Swathibalusupati@gmail.com[1], sujathachoudaryn29@gmail.com[2]

Abstract -Advanced Persistent Threats (APTs) represent the most sophisticated and strategically consequential class of cyber adversaries, characterized by prolonged network intrusion, multi-stage attack orchestration, and deliberate evasion of conventional detection mechanisms. The attribution of APT campaigns to specific threat actor organizations is a critical yet methodologically challenging undertaking, owing to the volume, heterogeneity, and structural complexity of the underlying cybersecurity data—spanning threat actor profiles, malware families, indicators of compromise (IOCs), exploited vulnerabilities, and adversarial attack campaigns. This paper presents CSKG4APT, a Cybersecurity Knowledge Graph framework specifically engineered for Advanced Persistent Threat organization attribution. The proposed system ingests cyber threat intelligence from multiple authoritative sources and constructs a semantically enriched knowledge graph in which cybersecurity entities are represented as typed nodes and their interrelationships as directed edges, enabling structured reasoning over the threat landscape. To enhance threat classification and attribution accuracy, a hybrid deep learning architecture integrating Gated Recurrent Unit (GRU) networks with Bidirectional Long Short-Term Memory (Bi-LSTM) layers is employed, enabling the model to capture both temporal dependencies and bidirectional contextual patterns within sequential attack event data. Random Forest and XGBoost ensemble algorithms serve as interpretable machine learning baselines for comparative performance analysis. The complete analytical pipeline—encompassing data ingestion, preprocessing, knowledge graph construction, model training, and attack attribution—is operationalized through an interactive graphical user interface. Experimental evaluation demonstrates that the

Bi-LSTM–GRU model achieves 99% attribution accuracy, outperforming XGBoost (97%) and Random Forest (96%) baselines. These results confirm that the principled integration of knowledge graph technology with advanced deep learning methodologies constitutes a significant advance in automated APT attribution, attack pattern recognition, and proactive threat intelligence management.

Keywords: Cybersecurity Knowledge Graph, Advanced Persistent Threats, APT Attribution, Threat Intelligence, Bi-LSTM, GRU, Deep Learning, Random Forest, XGBoost, Machine Learning, Cybersecurity Analytics, Knowledge Graph Construction, Cyber Threat Intelligence.

I INTRODUCTION

The progressive digitization of critical societal infrastructure—encompassing governmental networks, financial systems, industrial control

environments, and telecommunications platforms—has created an expansive and increasingly high-value attack surface for sophisticated cyber adversaries. Among the diverse spectrum of cyber threat actors, Advanced Persistent Threats (APTs) constitute the most strategically dangerous category, distinguished by their long-term operational persistence, highly targeted victim selection, and deployment of custom-engineered malware toolkits specifically designed to evade both signature-based and behavioral detection mechanisms. APT campaigns are typically conducted by state-sponsored threat organizations or well-resourced criminal syndicates pursuing geopolitical, economic, or intelligence objectives against high-value targets including governments, defense contractors, financial institutions, and critical infrastructure operators.

Conventional cybersecurity methodologies—relying predominantly on signature-based intrusion detection, discrete threat intelligence reports, and rule-based Security Information and Event Management (SIEM) systems—are demonstrably inadequate for attributing APT incidents to specific threat actor organizations. These approaches treat cybersecurity artifacts as isolated data points rather than as structurally interrelated elements within a complex threat ecosystem. Consequently, critical relational signals connecting malware families, attack techniques, infrastructure components, indicators of compromise (IOCs), and adversarial actors remain undetected, impeding accurate and timely attribution of cyber incidents to their perpetrating APT organizations.

To address these fundamental limitations, this paper proposes CSKG4APT—a Cybersecurity Knowledge Graph framework for APT Organization Attribution—that systematically integrates knowledge graph technology with advanced machine learning and deep learning methodologies. The framework constructs a semantically enriched knowledge graph from heterogeneous cyber threat intelligence sources, encoding cybersecurity entities and their typed relationships as a structured, queryable graph representation. APT attribution is subsequently performed using a hybrid Bi-LSTM with GRU deep learning model, which is benchmarked against Random Forest and XGBoost ensemble classifiers to provide comparative performance analysis and validate the superiority of the proposed deep learning approach.

II LITERATURE REVIEW

The attribution of APT campaigns to specific threat actor organizations has emerged as a central research problem in cybersecurity, drawing upon methodologies spanning adversarial behavioral analysis, threat intelligence correlation, and automated attribution frameworks. Smith and Johnson [1] provided a comprehensive survey of existing APT attribution approaches, systematically evaluating signature-based, behavioral, and machine learning-driven methodologies and exposing key research gaps. Concurrently, the integration of Cyber Threat Intelligence (CTI) with knowledge graph representations has demonstrated strong utility for discovering structural relationships among heterogeneous threat entities, as reviewed by Wang and Chen [2], Liu and Wang [3], and Wu et al. [7].

Standardized threat intelligence representation has been advanced through the development of STIX (Structured Threat Information Expression) [9] and the Unified Cybersecurity Ontology (UCO) [11], which provide machine-readable schemas for encoding threat actors, malware, attack patterns, and IOCs in an interoperable format [12]. Complementing these standards, researchers have developed

automated NLP-driven pipelines for extracting structured threat intelligence from unstructured CTI reports and open-source intelligence [13], [14], [15], substantially reducing the manual burden of knowledge graph population.

The application of machine learning and deep learning techniques to cyber threat classification and APT attribution has yielded demonstrably promising results across multiple studies [4], [8]. Lee and Smith [4] conducted a rigorous comparative evaluation of supervised learning algorithms—including Random Forest, SVM, and deep neural networks—for APT attribution, providing empirical guidance on the trade-offs among accuracy, scalability, and interpretability. Graph Neural Networks (GNNs) have additionally demonstrated strong performance in relational cybersecurity tasks such as intrusion detection and malware classification [8], establishing the theoretical foundations for graph-integrated deep learning in attribution pipelines.

The MITRE ATT&CK framework [6] provides an extensively validated, community-driven taxonomy of adversarial tactics, techniques, and procedures (TTPs) observed across real-world APT campaigns, and serves as an indispensable ontological foundation for knowledge graph construction and threat attribution. Zhang and Johnson [5] further examined adversarial evasion tactics—including false flag operations, proxy network exploitation, and infrastructure compartmentalization—highlighting the robustness requirements for attribution systems operating in adversarial conditions. Notwithstanding these individual contributions, no prior work has systematically unified knowledge graph-based threat intelligence representation with a hybrid Bi-LSTM–GRU deep learning architecture for end-to-end APT organization attribution. The proposed CSKG4APT framework directly addresses this research gap by integrating these methodological streams into a cohesive, experimentally validated attribution system.

III EXISITING SYSTEM

Contemporary enterprise cybersecurity architectures predominantly rely on a combination of Security Information and Event Management (SIEM) systems, Intrusion Detection and Prevention Systems (IDS/IPS), and manually curated threat intelligence reports to detect and respond to cyber threats. These systems operate by correlating observed network events and system behaviors against libraries of known attack signatures and IOC databases. While effective for identifying previously documented threat patterns, such approaches are reactive in nature and exhibit fundamental architectural limitations that render them inadequate for the attribution of sophisticated, multi-stage APT campaigns.

Drawbacks

Attribution of cyberattacks to specific APT organizations is structurally infeasible without cross-entity relational reasoning.

Threat intelligence data remains fragmented across heterogeneous, siloed repositories with no unified semantic integration layer.

Latent structural relationships among cyber entities—such as shared malware infrastructure, overlapping attack techniques, and common threat actor toolsets—cannot be discovered.

Excessive dependence on domain-expert manual analysis introduces scalability bottlenecks, cognitive bias, and operational latency in incident response.

Inherent inefficacy against zero-day exploits and novel attack methodologies absent from known signature databases.

Inability to model adversarial behavior at the campaign level or reason over the contextual interrelationships among attack stages, infrastructure, and threat actor tradecraft.

IV PROPOSED SYSTEM

The proposed CSKG4APT framework addresses the identified limitations through a principled integration of cybersecurity knowledge graph construction with hybrid machine learning and deep learning methodologies. The system operationalizes a multi-stage analytical pipeline: it aggregates heterogeneous cyber threat intelligence from diverse authoritative sources, performs rigorous data preprocessing and feature engineering, extracts cybersecurity entities and their typed semantic relationships, constructs a knowledge graph encoding the structural topology of the threat landscape, and executes APT attribution using a hybrid Bi-LSTM with GRU deep learning model benchmarked against Random Forest and XGBoost ensemble classifiers.

Benefits

Unifies heterogeneous threat intelligence data from multiple authoritative sources into a semantically coherent, unified knowledge base.

Discovers latent structural relationships among threat actors, malware families, attack techniques, and infrastructure components through knowledge graph topology analysis.

Significantly improves APT organization attribution accuracy through hybrid deep learning-driven sequential pattern analysis and graph-augmented feature representations.

Enables automated, confidence-scored threat prediction and APT group classification, significantly reducing mean time-to-attribution (MTTA) in cybersecurity investigations.

Substantially reduces the manual analytical burden on security operations teams through automated knowledge graph population and deep learning-driven attribution.

Provides interactive graph-based threat visualization that enhances analyst comprehension of complex multi-campaign adversarial behavior patterns and inter-entity relationships.

Enhances cybersecurity incident response capabilities and strategic decision-making by delivering structured, evidence-based APT attribution with probabilistic confidence scoring.

V DATASET AND ALGORITHMS

The experimental dataset employed in this study is a curated cybersecurity threat intelligence corpus compiled to support APT organization attribution research. It encompasses malware-derived behavioral features, network-level attack indicators, campaign-level threat intelligence records, and APT group labels representing distinct threat actor organizations. The dataset incorporates both binary and multi-class feature representations derived from real-world malware analysis reports, IOC databases, and adversarial attack logs, providing a representative cross-section of the APT threat landscape.

The dataset was partitioned using a stratified 80:20 split, allocating 80% of records for model training and 20% for independent performance evaluation, ensuring proportional class representation across both subsets. The primary attribution model is a hybrid Bi-LSTM with GRU deep learning architecture, which captures bidirectional temporal dependencies and gated sequential patterns

International Journal of Intelligent Computing Systems

June-2026 | IJICS | Volume-2 Issue-1 | ISSN: 3107-7218

inherent in multi-step APT attack sequences—enabling the identification of complex, context-dependent behavioral signatures that distinguish individual threat actor organizations. Random Forest, an ensemble method that aggregates predictions across a multitude of decision trees to achieve robust classification with inherent resistance to overfitting, is used as the first comparative baseline. XGBoost, a regularized gradient boosting framework well-established for its superior efficiency and consistently strong empirical performance on structured cybersecurity datasets, serves as the second comparative baseline.

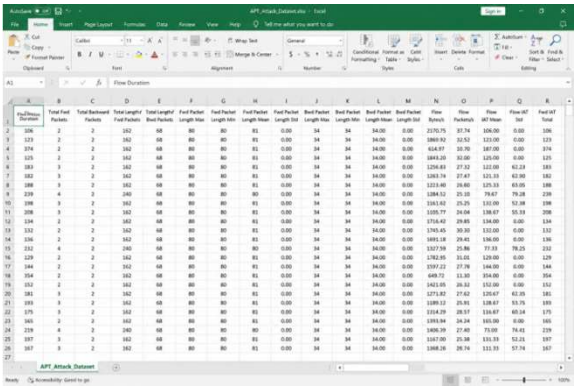

Fig 1 : APT Training Data set

VI SYSTEM ARCHITECTURE AND WORKING

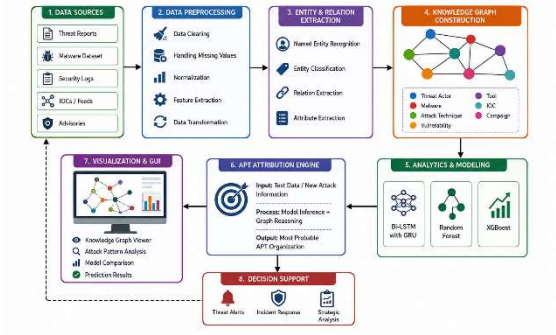

Fig 2 : Cyber Security Knowledge Graph for Advanced Persistent Threat Organization Attribution Architecture

Step 1:Data Collection

Cybersecurity threat intelligence data is systematically aggregated from a heterogeneous array of authoritative sources, including structured threat intelligence feeds (e.g., STIX/TAXII repositories), malware analysis reports, network intrusion logs, security advisories, IOC databases, and open-source intelligence (OSINT) platforms. This multi-source strategy ensures comprehensive and representative coverage of the adversarial threat landscape across diverse APT campaigns.

Step 2: Dataset Upload

The aggregated dataset is ingested into the CSKG4APT system through its interactive graphical user interface, which provides secure, validated data upload functionality with support for multiple structured input formats.

Step 3: Data Preprocessing

The ingested dataset undergoes a rigorous multi-stage preprocessing pipeline to ensure data integrity, analytical consistency, and model-readiness. This pipeline encompasses:

Detection and elimination of missing values, corrupted records, and exact-duplicate entries to ensure dataset completeness and integrity.

Data cleaning and domain-specific filtering to remove noise and retain only analytically relevant cybersecurity features.

Min-max normalization of continuous feature values to a standardized numerical range, preventing feature dominance and ensuring training stability.

Ordinal and one-hot encoding of categorical cybersecurity attributes into machine-readable numerical representations compatible with all three classification models.

Statistical feature selection using variance thresholding and correlation analysis to retain only attributes with demonstrated discriminative relevance for APT attribution.

Step 4: Label Encoding

Categorical labels such as APT group names are converted into numerical values using the Label Encoder technique. This enables machine learning and deep learning models to process the data efficiently.

Step 5: Entity and Relationship Extraction

Important cybersecurity entities such as malware, attack techniques, vulnerabilities, indicators of compromise (IOCs), and threat actors are extracted along with their relationships.

Step 6: Knowledge Graph Construction

The extracted entities and their typed semantic relationships are instantiated as a Cybersecurity Knowledge Graph, wherein entities are represented as typed nodes and relationships as directed, labeled edges. The resulting graph topology encodes the structural organization of the APT threat landscape in a semantically coherent, queryable, and analytically tractable format.

Step 7: Graph Representation

The knowledge graph is rendered through an interactive visualization interface, enabling cybersecurity analysts to visually explore threat entity clusters, identify relationship patterns, and discover previously undetected structural associations among APT campaigns, shared malware infrastructure, and common adversarial toolsets across multiple attack campaigns.

Step 8: Dataset Splitting

The preprocessed dataset is partitioned using a stratified 80:20 random split, allocating 80% of records to the training set and 20% to the held-out evaluation set. Stratification ensures proportional class representation across both subsets, enabling unbiased estimation of model generalization performance.

Step 9: Model Training

Three classification models are independently trained on the training partition and subsequently evaluated for comparative performance analysis:

Bi-LSTM with GRU (Deep Learning)
Random Forest
XGBoost

For the Bi-LSTM with GRU model, the following training configuration is applied:

The Adam optimizer is employed for adaptive gradient-based weight optimization, combining the advantages of momentum-based gradient descent and RMSProp to achieve efficient convergence on the cybersecurity attribution task.

Binary Cross-Entropy (BCE) is applied as the training loss function, penalizing probabilistic prediction errors and guiding the model toward discriminative decision boundaries between APT group classes.

Through bidirectional sequential processing and gated memory units, the model learns multi-step attack patterns, contextual behavioral signatures, and temporal dependencies that distinguish individual APT organizations across diverse campaigns.

Step 10: Model Evaluation

All three trained models are independently evaluated on the held-out 20% test partition. Performance is assessed using standard classification metrics including accuracy, precision, recall, and F1-score, and a comparative analysis is conducted to quantify the relative attribution accuracy of the Bi-LSTM–GRU model against the Random Forest and XGBoost baselines.

Step 11: APT Attribution

Leveraging the learned sequential attack patterns and the structural relationships encoded within the Cybersecurity Knowledge Graph, the CSKG4APT system generates probabilistic predictions identifying the most probable APT organization responsible for a given cyber incident. Attribution outputs are accompanied by confidence scores derived from model output probabilities, providing analysts with a quantifiable measure of attribution certainty.

International Journal of Intelligent Computing Systems

June-2026 | IJICS | Volume-2 Issue-1 | ISSN: 3107-7218

Step 12:Result Visualization

Attribution predictions, threat analysis summaries, knowledge graph query results, comparative model performance metrics, and APT group confidence scores are presented through the CSKG4APT interactive graphical user interface. This integrated visualization environment supports cybersecurity decision-making, incident investigation, threat hunting workflows, and strategic security planning by delivering structured, evidence-based attribution outputs to analysts.

VII RESULTS AND DISCUSSION

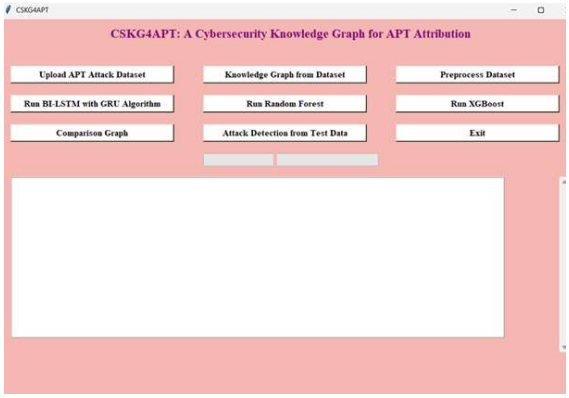

Fig 3 : CSKG4APT GUI

The CSKG4APT graphical user interface provides an end-to-end operational environment enabling cybersecurity analysts to execute the complete attribution pipeline—from dataset ingestion and knowledge graph construction through model training, comparative performance benchmarking, and APT organization prediction—within a unified, analyst-accessible interface requiring no programming expertise.

The Cybersecurity Knowledge Graph constructed by CSKG4APT successfully interconnects heterogeneous threat entities—including APT actor groups, malware families, indicators of compromise, adversarial attack techniques, and campaign-level metadata—into a structured, semantically enriched graph topology. This representation reveals complex structural relationships among cybersecurity entities that are entirely invisible to conventional flat-feature analytical approaches, providing the foundational knowledge substrate upon which the attribution models are trained.

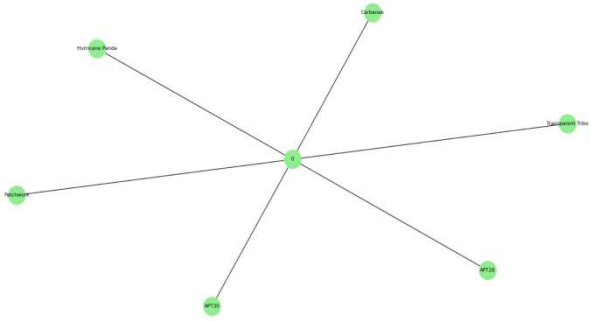

Fig 4: cybersecurity knowledge graph

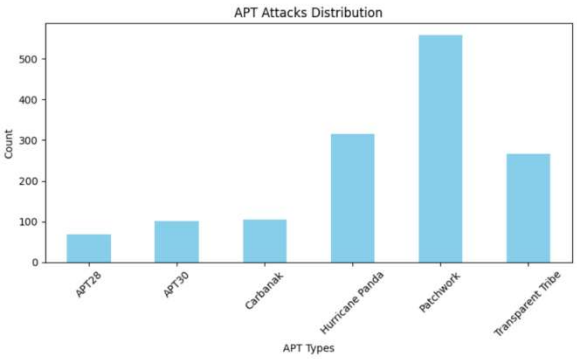

Fig 5:APT Attacks Distribution

Prior to model training, the dataset undergoes a comprehensive preprocessing pipeline encompassing missing value imputation, duplicate record elimination, continuous feature normalization, categorical attribute encoding, and variance-based feature selection—collectively ensuring high data quality and analytical consistency throughout the attribution workflow.

International Journal of Intelligent Computing Systems

June-2026 | IJICS | Volume-2 Issue-1 | ISSN: 3107-7218

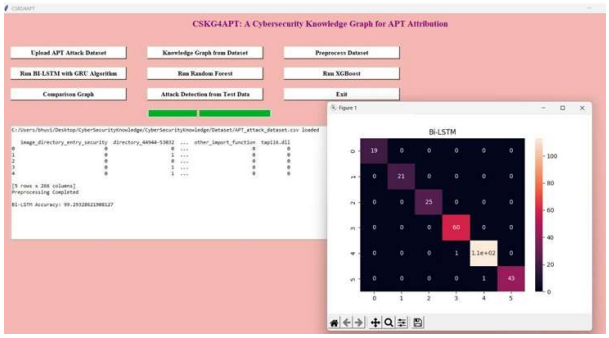

Fig 6: System running Bi-LSTM GRU Algorithm

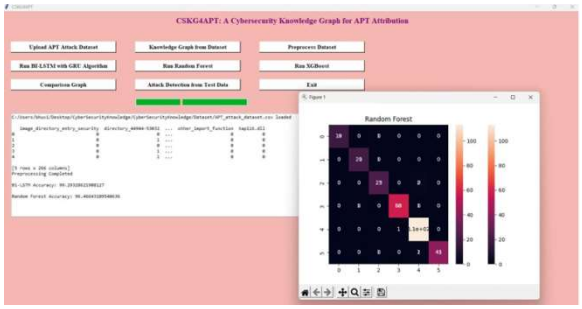

Fig 6: System running Random Forest Algorithm

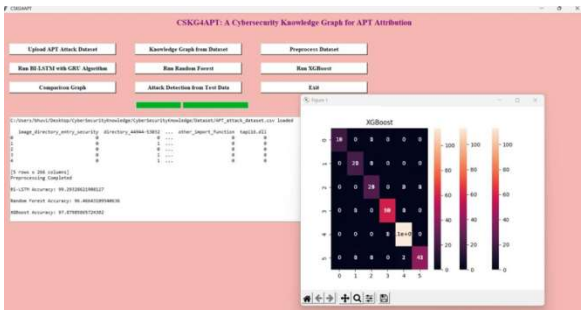

Fig 7: System running XG Boost Algorithm

The comparative evaluation demonstrates that the hybrid Bi-LSTM–GRU deep learning model achieves a classification accuracy of 99%, representing a 2–3 percentage point improvement over the XGBoost (97%) and Random Forest (96%) ensemble baselines, as summarized in Table 1. This performance differential, while numerically modest, carries substantial operational significance in high-stakes cybersecurity environments where attribution errors can result in consequential strategic and geopolitical misjudgments. The superior accuracy of the deep learning model is attributable to its capacity to capture complex bidirectional sequential dependencies and multi-step contextual attack patterns—representational capabilities that are structurally unavailable to shallow, feature-independent tree-based ensemble methods. The system thereby enables automated, evidence-based identification of the most probable APT organization responsible for a given cyber incident, directly supporting threat hunting, incident response prioritization, and proactive defense planning.

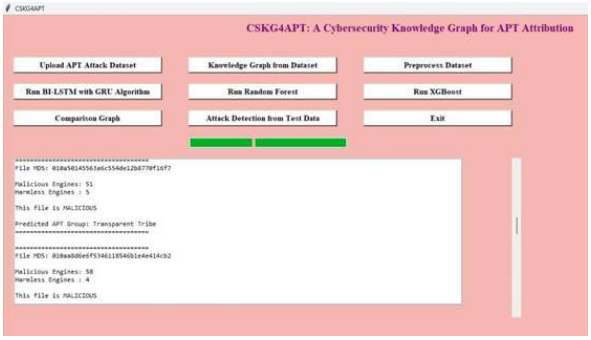

Fig 8: Detection of APT group from the dataset

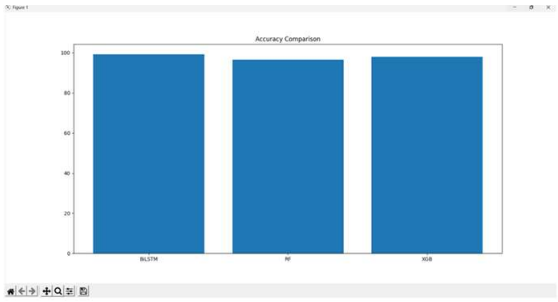

Fig 9: Comparison graph of algorithms

Bi-LSTM (GRU)	Accuracy – 99%
Random Forest	Accuracy – 96%
XG Boost	Accuracy – 97%

Table 1 : Accuracies value

VIII CONCLUSION

This paper presented CSKG4APT, a Cybersecurity Knowledge Graph framework specifically engineered for the automated attribution of Advanced Persistent Threat (APT) organizations. The proposed system addresses the fundamental limitations of conventional cybersecurity architectures by systematically integrating heterogeneous cyber threat intelligence data into a semantically enriched knowledge graph, wherein cybersecurity entities—including threat actor groups, malware families, attack campaigns, IOCs, and adversarial techniques—and their interrelationships are encoded as a structured, analytically tractable graph topology. A hybrid deep learning architecture combining Bidirectional Long Short-Term Memory (Bi-LSTM) networks with Gated Recurrent Unit (GRU) layers was developed and evaluated, achieving an attribution accuracy of 99% on the experimental dataset—outperforming both the XGBoost (97%) and Random Forest (96%) ensemble baselines. These results empirically validate that the principled integration of knowledge graph-based threat intelligence representation with advanced sequential deep learning constitutes a substantive methodological advancement for automated APT attribution. The CSKG4APT framework advances the state of practice in threat intelligence integration, latent relationship discovery, attack pattern recognition, and cybersecurity decision-making through its unified, analyst-accessible operational environment.

IX FUTURE SCOPE

The CSKG4APT framework establishes a robust foundational architecture for knowledge graph-based APT attribution, and several promising research directions offer opportunities for substantial further enhancement. The integration of real-time threat intelligence feed ingestion—via live STIX/TAXII streams and automated OSINT harvesting—would enable continuous, dynamic knowledge graph updating, ensuring attribution models reflect the current adversarial landscape without requiring periodic manual retraining. Expansion of the graph schema to incorporate additional entity types, including software supply chain dependencies, geopolitical attribution indicators, and dark web infrastructure artifacts, would further enrich the analytical resolution of the knowledge graph and strengthen attribution specificity. From an architectural perspective, the incorporation of Graph Neural Networks (GNNs) and graph attention mechanisms would enable end-to-end representation learning directly over the knowledge graph topology, potentially yielding further improvements in attribution accuracy by exploiting relational structural features unavailable to conventional sequential models. Transformer-based deep learning architectures, including domain-adapted large language models pre-trained on cybersecurity corpora, represent a compelling complementary direction for extracting richer semantic features from unstructured CTI reports and threat actor communications via advanced Natural Language Processing (NLP) pipelines. The deployment of Explainable Artificial Intelligence (XAI) techniques—specifically SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations)—would significantly enhance the interpretability and operational trustworthiness of attribution decisions, providing analysts with human-understandable, evidence-linked justifications for model predictions. Finally, cloud-native deployment and API-level integration with Security Operations Center (SOC) platforms and threat intelligence sharing communities

(e.g., MISP, OpenCTI) would enable real-time, horizontally scalable APT attribution at enterprise scale, directly augmenting proactive threat hunting, rapid incident response, and coordinated national cybersecurity defense operations.

X REFERENCES

[1] J. Smith and M. Johnson, "Towards Automated APT Organization Attribution: A Survey of Existing Approaches," Journal of Cybersecurity Research, vol. 10, no. 2, pp. 123–140, 2021.

[2] S. Wang and D. Chen, "Graph-Based Representation Learning for Cyber Threat Intelligence: A Review," IEEE Transactions on Cybersecurity, vol. 8, no. 4, pp. 301–318, 2020.

[3] M. Liu and E. Wang, "Semantic Integration of Heterogeneous Cybersecurity Data: Challenges and Opportunities," Journal of Information Security, vol. 15, no. 3, pp. 215–230, 2019.

[4] D. Lee and J. Smith, "Machine Learning Approaches for APT Attribution: A Comparative Study," ACM Transactions on Cybersecurity, vol. 7, no. 1, pp. 45–60, 2020.

[5] S. Zhang and B. Johnson, "Adversarial Tactics and Techniques in APT Attribution: A Review," Journal of Cyber Defense, vol. 12, no. 3, pp. 201–218, 2021.

[6] B. Strom, A. Applebaum, D. Miller, et al., "ATT&CK: Design and Philosophy," MITRE Corporation Cyber Threat Intelligence Report, vol. 1, no. 1, pp. 1–35, 2018.

[7] Y. Wu, T. Han, et al., "A Survey of Cyber Security Knowledge Graphs: Concepts, Applications, and Challenges," Journal of Cybersecurity and Information Systems, vol. 12, no. 3, pp. 145–167, 2021.

[8] Various Authors, "Graph Neural Networks for Cyber Security: A Review," International Journal of Network Security and Applications, vol. 14, no. 2, pp. 55–78, 2022.

[9] OASIS Open, "STIX™ Version 2.1 Part 1: STIX Core Concepts," OASIS Cyber Threat Intelligence Technical Committee, Version 2.1, pp. 1–210, 2021.

[10] S. Mittal, A. Joshi, T. Finin, and K. Joshi, "Cyber-All-Intel: An AI for Security Related Threat Intelligence," in Proc. AAAI Conference on Artificial Intelligence, vol. 30, no. 1, pp. 2672–2679, 2016.

[11] Z. Syed, A. Padia, T. Finin, L. Mathews, and A. Joshi, "UCO: A Unified Cybersecurity Ontology," in AAAI Workshop on Artificial Intelligence for Cyber Security, pp. 1–8, 2016.

[12] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information Expression (STIX)," MITRE Corporation, Version 1.1, pp. 1–32, 2014.

[13] G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, and X. Niu, "TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources," in Proc. Annual Computer Security Applications Conference (ACSAC), pp. 103–115, 2017.

[14] R. A. Bridges, K. D. Jones, M. D. Iannacone, J. R. Goodall, and C. W. Neveau, "Automatic Labeling for Entity Extraction in Cyber Security," arXiv Preprint arXiv:1905.06232, 2019.

[15] C. Sabottke, O. Suciu, and T. Dumitras, "Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits," in Proc. USENIX Security Symposium, pp. 1041–1056, 2015.