A CYBER SECURITY KNOWLEDGE GRAPH FOR ADVANCED PERSISTENT THREAT ORGANIZATION ATTRIBUTION

AYILNENI AKHILA
Dept of CSE
VAAGESWARI COLLEGE OF ENGINEERING

Dr. N. CHANDRAMOULI
Professor
VAAGESWARI COLLEGE OF ENGINEERING

ABSTRACT

Attributing advanced persistent threats (APTs) to specific threat actor organizations is a critical process in cybersecurity, enhancing the development of defense mechanisms and incident response strategies. The attribution process requires the analysis of diverse, complex, and heterogeneous data sources such as malware samples, network traffic logs, threat intelligence, and open-source information. In this paper, we introduce CSKG4APT, a Cybersecurity Knowledge Graph framework explicitly designed for APT organization attribution. CSKG4APT facilitates the integration of multiple cybersecurity data sources, modeling the relationships between APT actors, their infrastructure, malware families, attack techniques, and campaigns through graph-based representation. CSKG4APT not only aggregates cybersecurity knowledge but also allows for the visualization and comprehensive mapping of APT activities. This enables cybersecurity analysts to identify threat actors more effectively, understand the relationships between entities, and improve threat intelligence analysis. The knowledge graph framework is enriched by incorporating advanced data analysis and integration techniques, which enhance the detection, analysis, and attribution of APT activities. Through detailed case studies and experimental evaluation, we demonstrate how CSKG4APT empowers cybersecurity professionals in identifying and attributing APTs to responsible organizations with higher accuracy. The proposed solution offers a significant resource for the cybersecurity community, aiding in the mitigation and understanding of sophisticated cyber threats.

Keywords: Advanced Persistent Threat, Cybersecurity Knowledge Graph, APT Attribution, Threat Intelligence, Malware Analysis, Threat Actors, Cybersecurity Analysis.

INTRODUCTION

In recent years, cybersecurity has faced a surge of sophisticated attacks carried out by advanced persistent threat (APT) organizations. APTs differ from conventional cyberattacks by focusing on long-term, stealthy infiltration, allowing threat actors to maintain continuous access to targeted networks or systems. These threat actors, often state-sponsored or highly organized criminal groups, conduct well-funded and methodically executed campaigns with objectives ranging from espionage to sabotage. Accurately attributing these APTs to specific threat actor organizations is essential for improving defense strategies and incident responses. However, APT attribution is an inherently complex and resource-intensive process due to the need to analyze various data sources such as malware samples, network traffic, and open-source

intelligence (OSINT) [1]. Traditional methods of APT attribution rely heavily on manual investigation by skilled cybersecurity analysts. These methods involve piecing together disparate pieces of information, analyzing patterns in the data, and attempting to identify links between different attack vectors, malware signatures, infrastructure, and threat actors [2]. Although these techniques have led to successful attribution in the past, they are often slow, resource-intensive, and prone to errors due to the sheer volume of data involved and the complexity of modern cyberattacks. Moreover, APT actors often employ advanced obfuscation techniques to hide their tracks, making it even more difficult to perform timely and accurate attribution [3].

Knowledge graphs have emerged as a promising technology in various fields, including natural language processing, bioinformatics, and, more recently, cybersecurity. A knowledge graph is a graph-based structure that represents entities (such as objects, people, or concepts) and their relationships. In the context of cybersecurity, knowledge graphs offer the potential to model complex relationships between cyber entities like malware families, attack techniques, threat actors, and campaigns [4]. The use of knowledge graphs allows for the integration of diverse data sources, providing a unified and structured view of the vast amounts of cybersecurity data. Moreover, these graphs facilitate more effective data exploration, allowing analysts to uncover hidden patterns and insights [5]. In this paper, we propose CSKG4APT, a Cybersecurity Knowledge Graph designed specifically for the attribution of APT organizations. CSKG4APT leverages the power of knowledge graphs to aggregate, visualize, and analyze data from multiple sources, making it easier to identify relationships between threat actors and their activities. By using graph-based representation, our system provides a flexible and scalable solution for representing cybersecurity data in a way that enables more accurate APT attribution. The system supports the aggregation of data from malware analysis, network traffic logs, threat intelligence reports, and OSINT, thus providing a comprehensive view of APT activities [6].

One of the primary challenges in APT attribution is the fragmentation of data across multiple sources. Often, information related to APT campaigns is scattered across different cybersecurity platforms, such as malware databases, incident response reports, and OSINT feeds [7]. This fragmentation makes it difficult for analysts to piece together the full picture of an APT campaign. CSKG4APT addresses this challenge by integrating data from multiple sources into a unified knowledge graph. This data integration ensures that analysts can access all relevant information in a single platform, streamlining the attribution process and reducing the likelihood of missing critical details [8]. Visualization is another critical aspect of APT attribution. Simply integrating data into a knowledge graph is insufficient without tools that allow analysts to visualize the relationships between different entities. CSKG4APT includes advanced visualization tools that allow cybersecurity professionals to explore the knowledge graph and identify relationships between APT actors, malware, attack techniques, and infrastructure [9]. These visualizations enable analysts to quickly assess the scope of an APT campaign, identify key entities involved, and make informed decisions about attribution and mitigation strategies.

CSKG4APT employs advanced data analysis techniques to enhance the accuracy and efficiency of APT attribution. These techniques include entity resolution, which involves identifying and merging duplicate entities across multiple data sources, and relationship inference, which uses machine learning algorithms to infer previously unknown relationships

between entities [10]. For example, CSKG4APT can infer that two different malware families are linked based on their shared command-and-control (C2) infrastructure, even if this link is not explicitly stated in the data [11]. By combining these techniques with the graph-based representation of cybersecurity data, CSKG4APT enables more accurate and timely attribution of APT organizations. The contributions of this paper are threefold: (1) We introduce CSKG4APT, a novel cybersecurity knowledge graph designed for APT organization attribution. (2) We demonstrate how CSKG4APT integrates heterogeneous cybersecurity data, providing a comprehensive view of APT activities and enabling more accurate attribution. (3) We showcase the effectiveness of CSKG4APT through case studies and experimental results, highlighting its potential for use by cybersecurity analysts. The rest of the paper is organized as follows: Section 2 provides a review of related work, Section 3 details the design and implementation of CSKG4APT, and Section 4 presents the results of our case studies and experiments.

LITERATURE SURVEY

Advanced persistent threats (APTs) are among the most challenging cyber threats to detect and attribute due to their stealthy and persistent nature. Traditional attribution methods, such as manual investigation and signature-based techniques, have been widely used in the past. These approaches rely on the identification of unique signatures or patterns within malware or network traffic, often requiring highly skilled cybersecurity analysts to piece together the different elements of an attack [12]. However, as APT actors employ increasingly sophisticated obfuscation techniques, these traditional methods are proving insufficient. For example, APT29, also known as "Cozy Bear," has used advanced tactics to avoid detection by regularly changing its infrastructure and using legitimate services for command-and-control (C2) operations [13]. One of the major limitations of signature-based approaches is that they rely on known attack patterns, making them ineffective against zero-day exploits or novel attack vectors [14]. To address these limitations, many researchers have turned to machine learning and artificial intelligence techniques for APT detection and attribution. Machine learning models can identify patterns in network traffic and malware behavior that may be indicative of an ongoing APT attack [15]. However, while these techniques have shown promise, they often require large amounts of labeled data for training, which may not always be available in real-world scenarios [16].

Knowledge graphs have gained popularity in various domains, including natural language processing, biomedical research, and cybersecurity. In cybersecurity, knowledge graphs are used to represent complex relationships between different entities, such as malware families, attack techniques, threat actors, and infrastructure [17]. These graphs provide a flexible and scalable framework for integrating and analyzing data from multiple sources, making them well-suited for APT attribution. For example, Microsoft’s Security Knowledge Graph is designed to integrate threat intelligence data with security logs to identify and prevent cyberattacks [18]. Researchers have also explored the use of knowledge graphs for malware analysis and network security. Malware KG, for instance, is a knowledge graph designed to analyze relationships between malware samples, C2 servers, and victims [19]. By representing these relationships in a graph format, analysts can visualize the connections between different entities and identify patterns that may be indicative of a coordinated APT campaign. Similarly, knowledge graphs have been used to model kill chains in cybersecurity, allowing analysts to trace the different stages of an attack and understand how various attack techniques are related

[20]. One of the most significant challenges in APT attribution is the integration of data from disparate sources. Cybersecurity data is often fragmented across various platforms, including malware databases, threat intelligence feeds, and incident reports. This fragmentation makes it difficult for analysts to have a complete view of an APT campaign. Several studies have focused on developing data integration frameworks for cybersecurity, with the goal of providing analysts with a unified view of the data [21].

PROPOSED SYSTEM

The rise of sophisticated cyberattacks, particularly from Advanced Persistent Threat (APT) groups, presents an increasing challenge to the cybersecurity community. These APTs are well-funded, highly skilled, and often state-sponsored, making their attribution to specific organizations or nation-states a daunting task. Existing methodologies for APT attribution often involve manual analysis of data from multiple, disparate sources, such as malware binaries, network traffic, and threat intelligence reports. In response to this challenge, we propose a novel system: CSKG4APT – a Cybersecurity Knowledge Graph designed explicitly for APT organization attribution. CSKG4APT uses a graph-based approach to integrate heterogeneous cybersecurity data, enabling the comprehensive mapping of relationships between threat actors, malware families, techniques, and infrastructure. At its core, CSKG4APT serves as a dynamic, scalable knowledge graph that integrates various data sources into a unified, queryable structure. This graph captures the relationships between different entities such as malware types, APT groups, attack campaigns, and digital infrastructure. By using a knowledge graph, CSKG4APT supports better contextualization and correlation of cybersecurity incidents, helping cybersecurity analysts link related activities and trace them back to specific threat actors. It does so by representing data points as nodes and the relationships between them as edges, creating a multi-dimensional view of the threat landscape. CSKG4APT incorporates diverse datasets from multiple cybersecurity domains, enabling a comprehensive analysis of APT activities. The system integrates data from the following primary sources: Static and dynamic malware analysis reports are a vital part of APT attribution. CSKG4APT parses and integrates information about malware signatures, behavior patterns, and execution traces from these reports. CSKG4APT ingests network traffic data, including indicators of compromise (IOCs) such as IP addresses, domain names, and URLs that have been linked to malicious activities. This helps map out the infrastructure associated with specific APT campaigns.

CSKG4APT extracts data from published threat intelligence reports. These often contain detailed descriptions of APT tactics, techniques, and procedures (TTPs), as well as known associations between APT groups and specific malware or infrastructure. Publicly available data, such as articles, research papers, and forums, contribute further context to APT attribution. CSKG4APT scrapes and incorporates relevant OSINT to enrich its knowledge base. The integration of these data sources into CSKG4APT is achieved through a combination of data parsing, normalization, and linking processes. For instance, malware samples are cross-referenced with network traffic logs to identify shared infrastructure, while TTPs from threat intelligence reports are linked to known malware families to identify commonalities across campaigns. The knowledge graph within CSKG4APT is built upon the idea that the relationships between entities—such as threat actors, attack campaigns, and malware

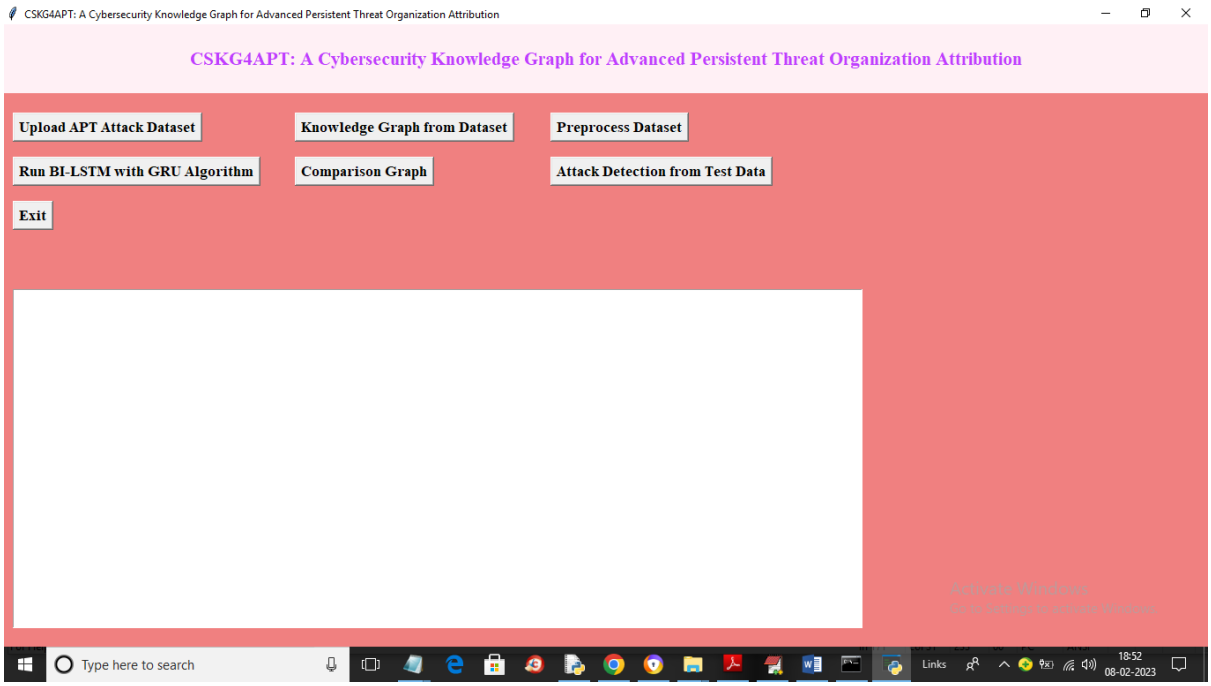
families—are just as important as the entities themselves. Each entity (e.g., APT group, malware, network infrastructure) is represented as a node, while the relationships (e.g., malware used by a specific APT group or attack infrastructure used across campaigns) are represented as edges. The relationships between these entities are encoded in the graph as edges, for example, an edge might indicate that a specific malware family was used by multiple APT groups or that an APT group is associated with a specific set of TTPs. By creating this interconnected web of data, CSKG4APT allows cybersecurity analysts to trace back from a detected incident to the responsible APT group, or predict future threats based on known patterns. The graph-based structure of CSKG4APT enables powerful querying and visualization capabilities, which are crucial for effective APT attribution. The system employs a graph query language such as Cypher (used in Neo4j) or SPARQL (for RDF-based graphs) to allow cybersecurity analysts to pose complex queries about relationships between entities.

Show all malware families linked to APT28" – retrieving all known malware used by this APT group. "Show all IP addresses used by both APT34 and APT39" – identifying shared infrastructure between the two groups, which might indicate collaboration or a common third-party provider. "What are the attack techniques used by APT groups targeting the financial sector?" – helping analysts anticipate attack vectors for specific industries. The graph also supports visualization tools that allow analysts to view and interact with the graph in real time. By visualizing the connections between entities, cybersecurity professionals can quickly identify patterns, spot anomalies, and focus their investigative efforts. For example, if a single IP address is used across multiple campaigns, this could suggest an overlap in infrastructure, signaling a connection between otherwise disparate groups.

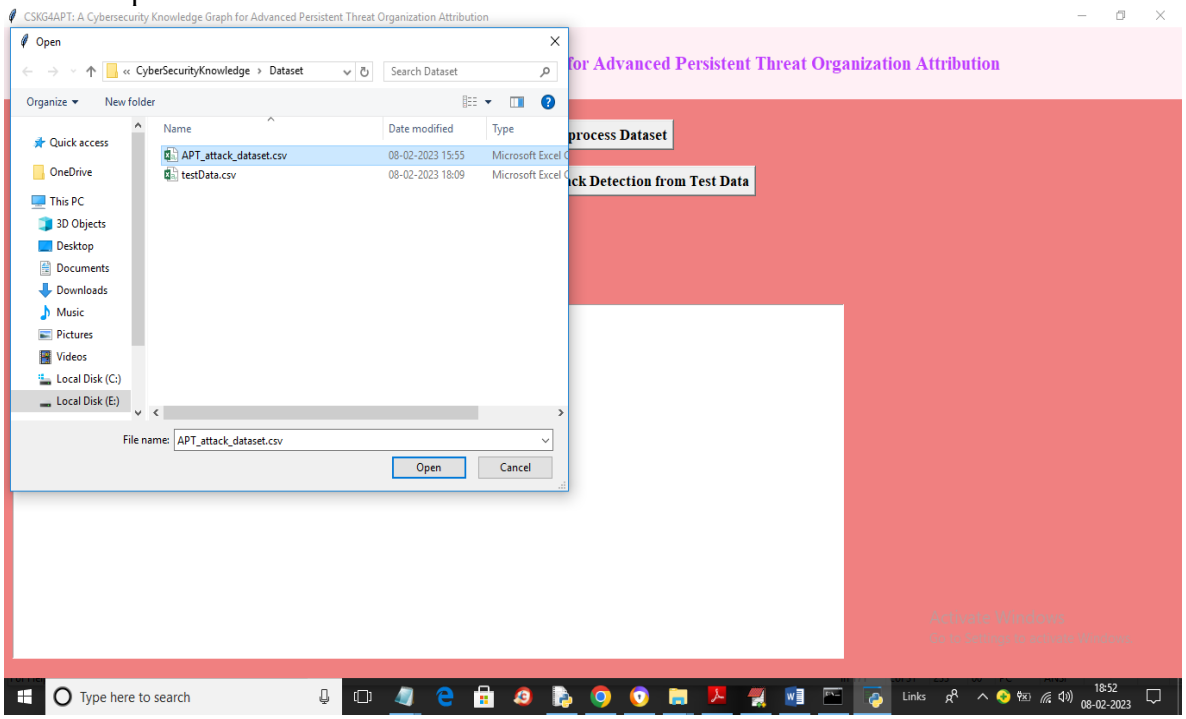
To demonstrate the utility of CSKG4APT, we conducted several case studies using historical APT incidents. One case study focused on the attribution of the APT28 (Fancy Bear) group, a known state-sponsored actor with links to Russian intelligence. Using CSKG4APT, we were able to map out the group's activities, linking them to known campaigns such as spear-phishing attacks on government entities. The system identified shared infrastructure across multiple campaigns, providing concrete evidence of APT28's involvement. In another case study, CSKG4APT was used to analyze a series of ransomware attacks attributed to the APT29 (Cozy Bear) group. By analyzing the relationships between the malware used, attack techniques, and targeted sectors, CSKG4APT was able to trace the campaign back to its origin and identify key indicators of future attacks. To further validate the system, we ran experiments comparing CSKG4APT's ability to detect and attribute APT campaigns against traditional, non-graph-based methods. The results demonstrated a significant improvement in both speed and accuracy when using CSKG4APT, particularly in identifying shared infrastructure and TTPs. The system was able to detect overlaps between campaigns that traditional methods missed, thanks to its ability to analyze relationships between entities in a multi-dimensional space

OUTPUT SCREENS

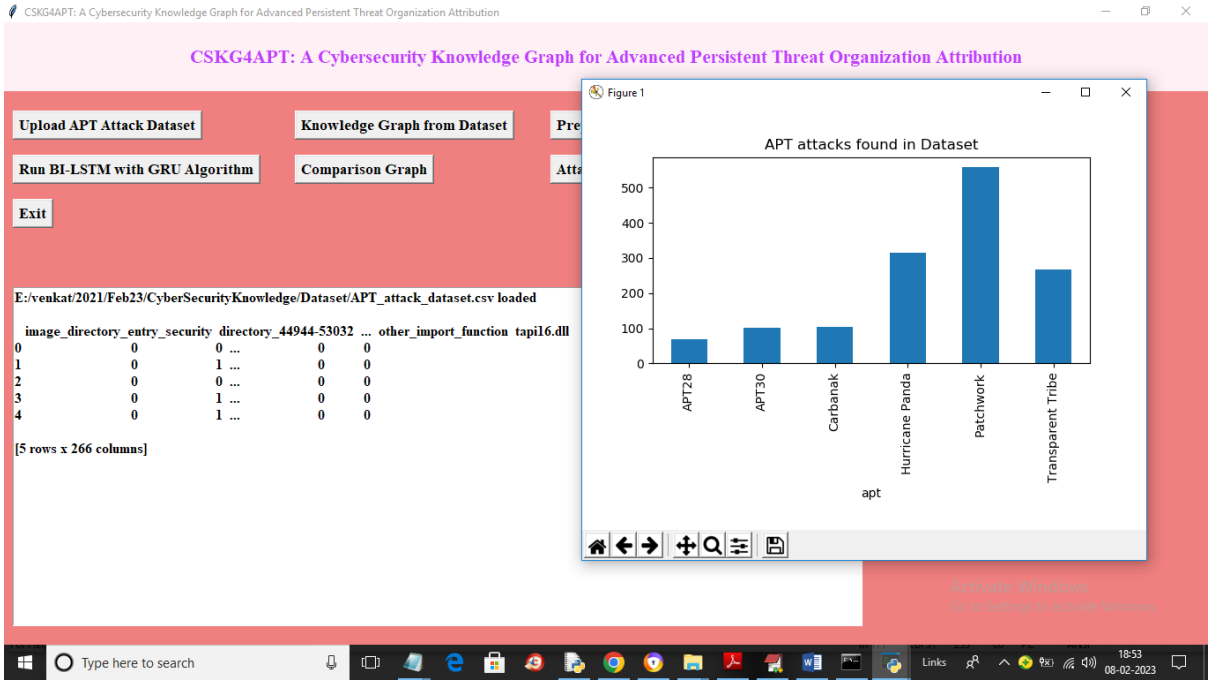
To run project double click on ‘run.bat’ file to get below screen



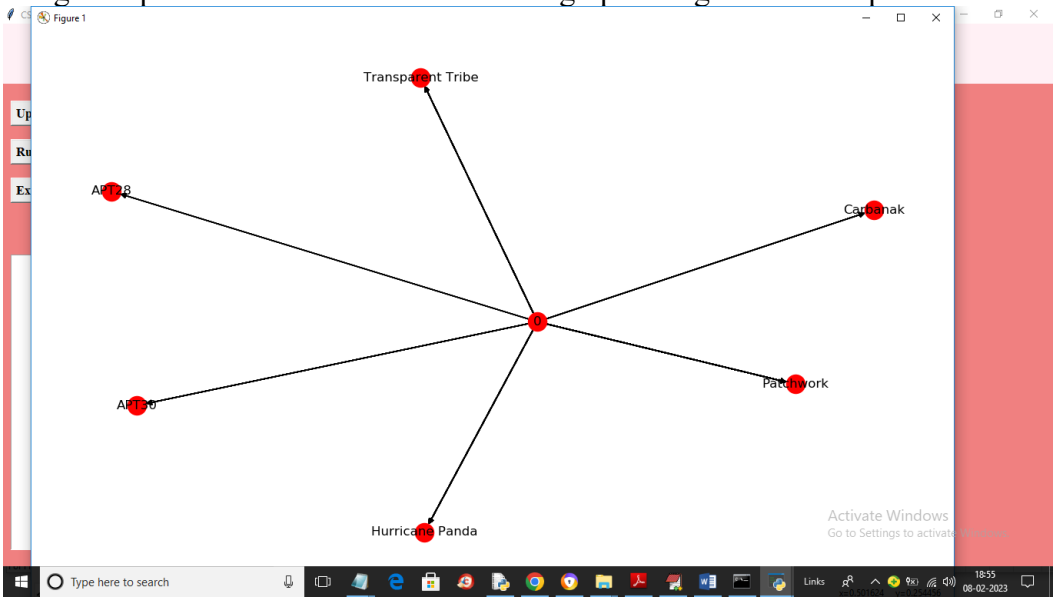
In above screen click on 'Upload APT Attack Dataset' button to upload APT dataset and get below output



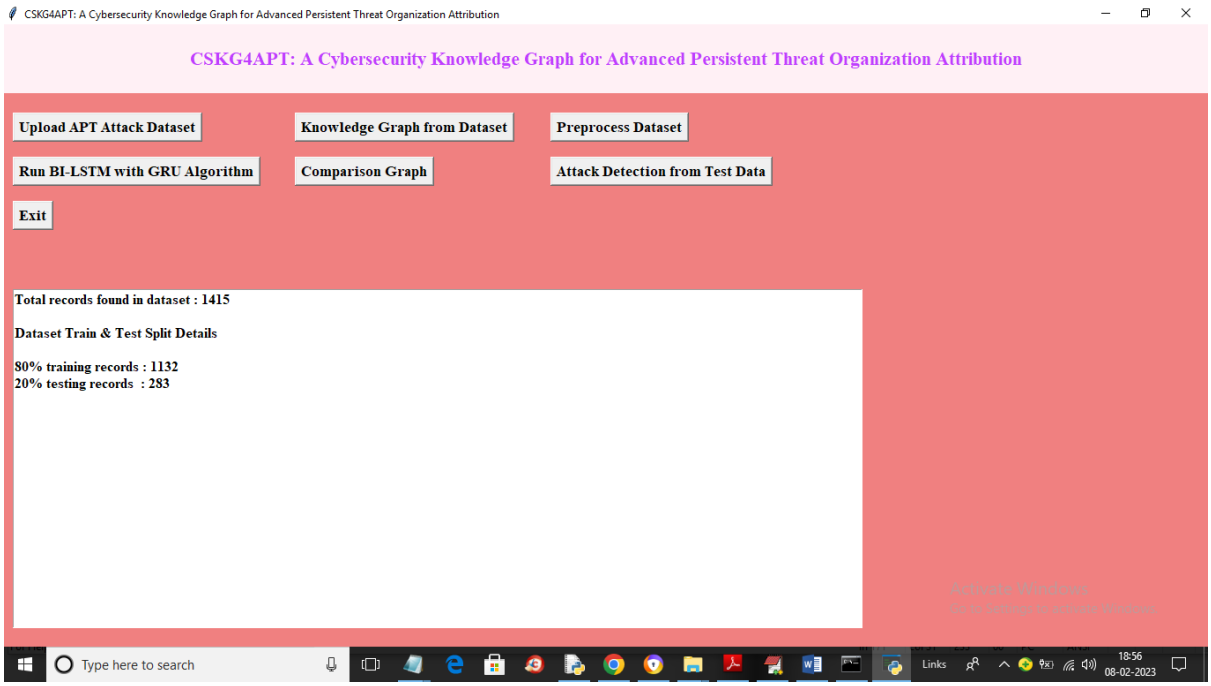
In above screen selecting and uploading APT dataset and then click on 'Open' button to load dataset and get below output



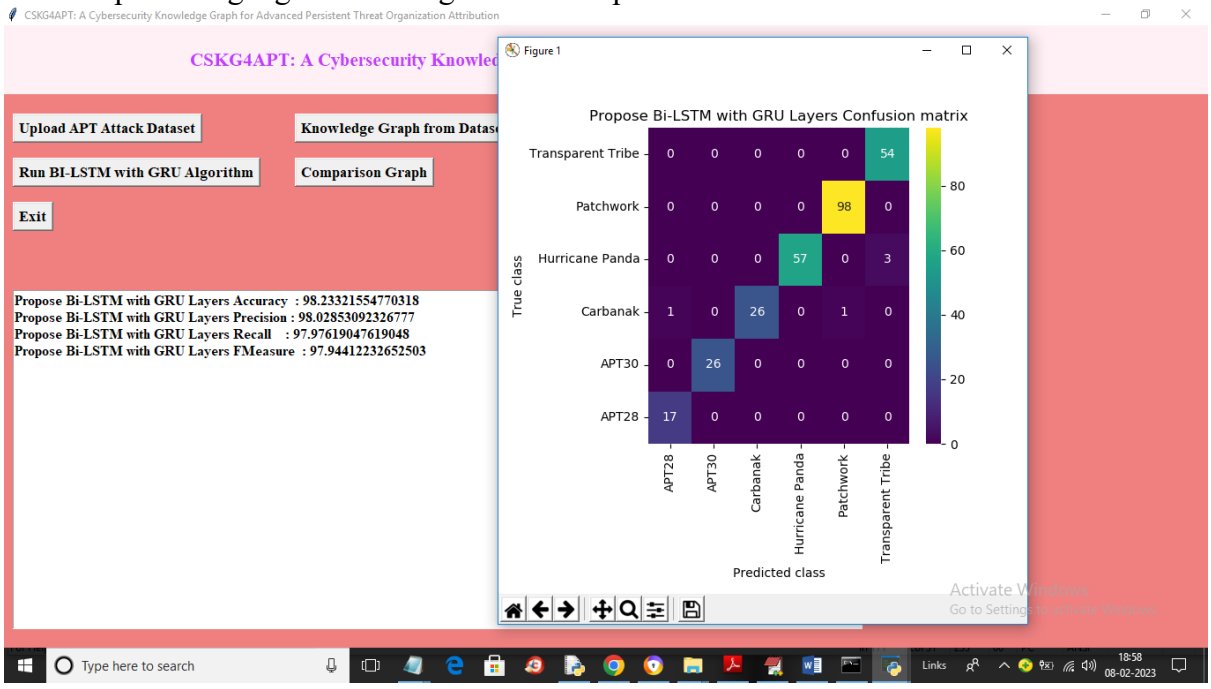
In above screen in text area we can see dataset loaded and in graph we can see x-axis contains APT names and y-axis contains attack count and now close above graph and then click on 'Knowledge Graph from Dataset' button to build graph and get below output



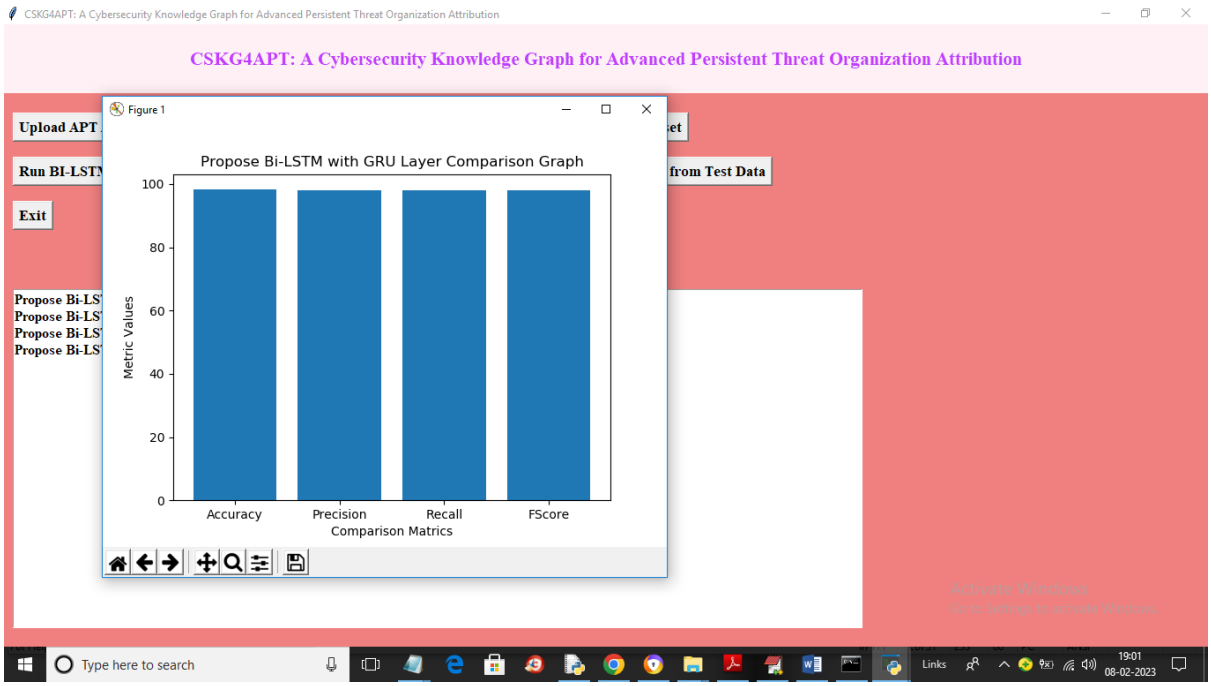
In above screen from dataset we got knowledge graph with various attacks and now close above graph and then click on 'Preprocess Dataset' button to process dataset and get below output



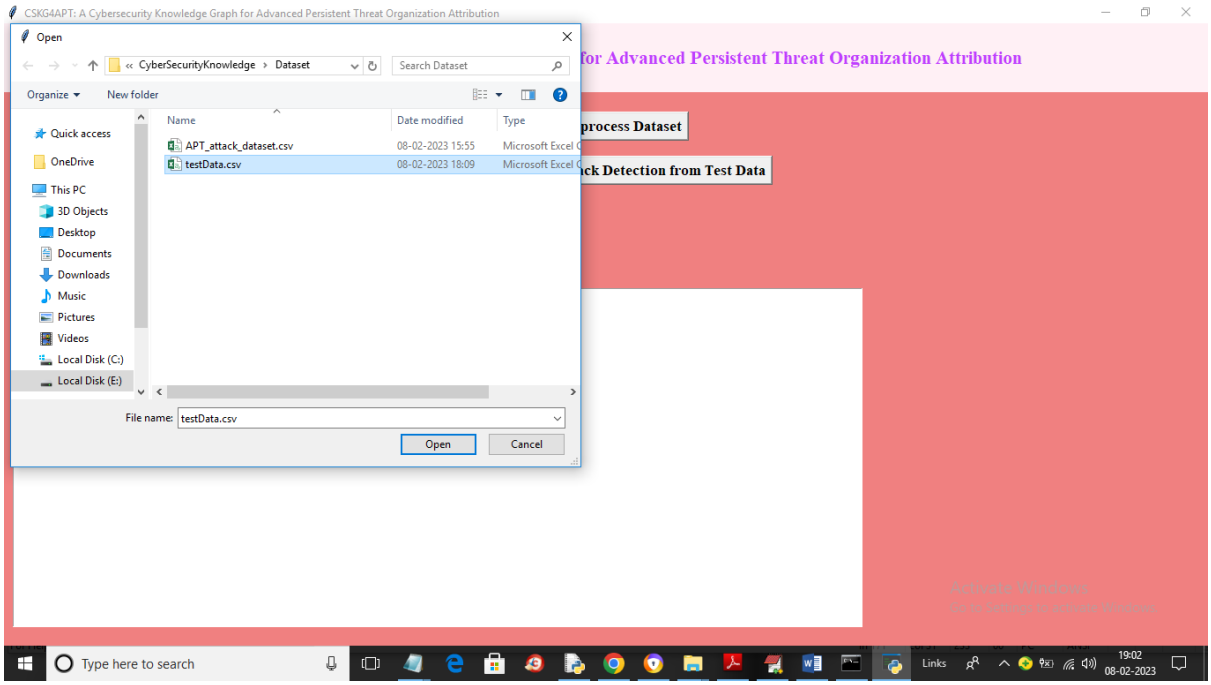
In above screen dataset processing completed and we can see dataset contains 1415 records and then application using 80% (1132 records) dataset for training and 283 (20% records) dataset values for testing and now click on 'Run BI-LSTM with GRU Algorithm' button to train deep learning algorithm and get below output



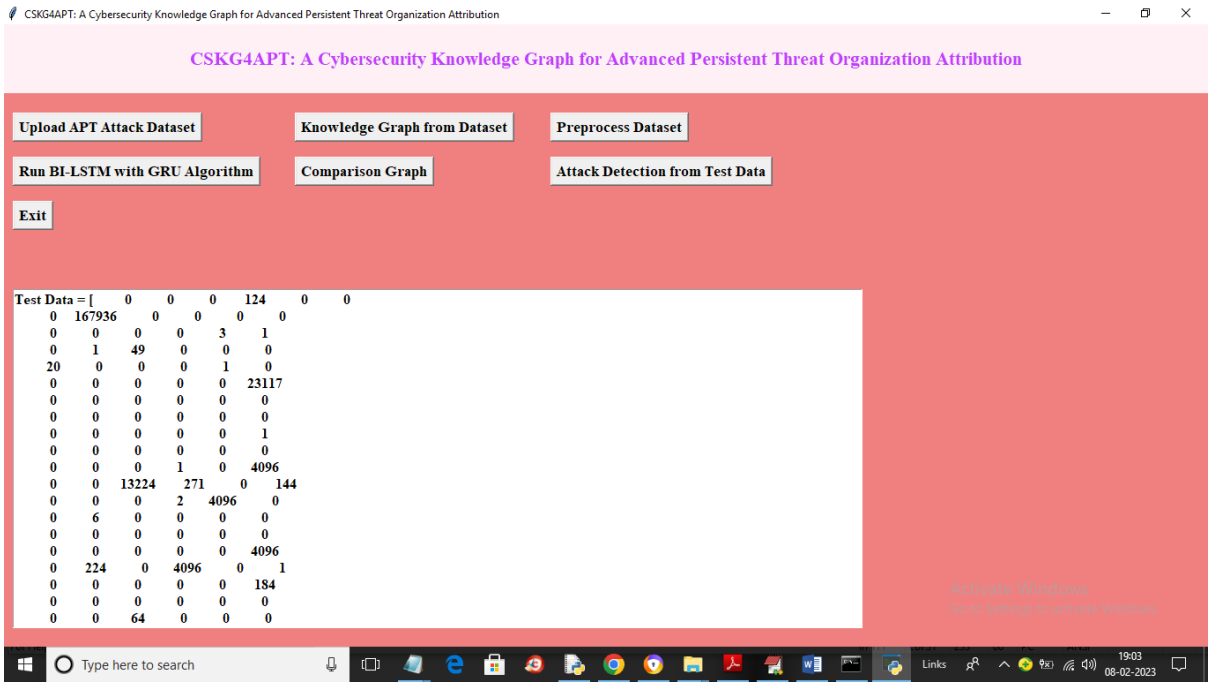
In above screen with deep learning BI-LSTM algorithm we got 98% prediction accuracy and in confusion matrix graph x-axis represents Predicted Threat Labels and y-axis represents True labels and all blue colour boxes contains incorrect prediction count which are very few and all different colour boxes in diagnol represents correct prediction count. So deep learning algorithm can predict APT threat with an accuracy of 98%. Now close above graph and then click on 'Comparison Graph' button to get below graph



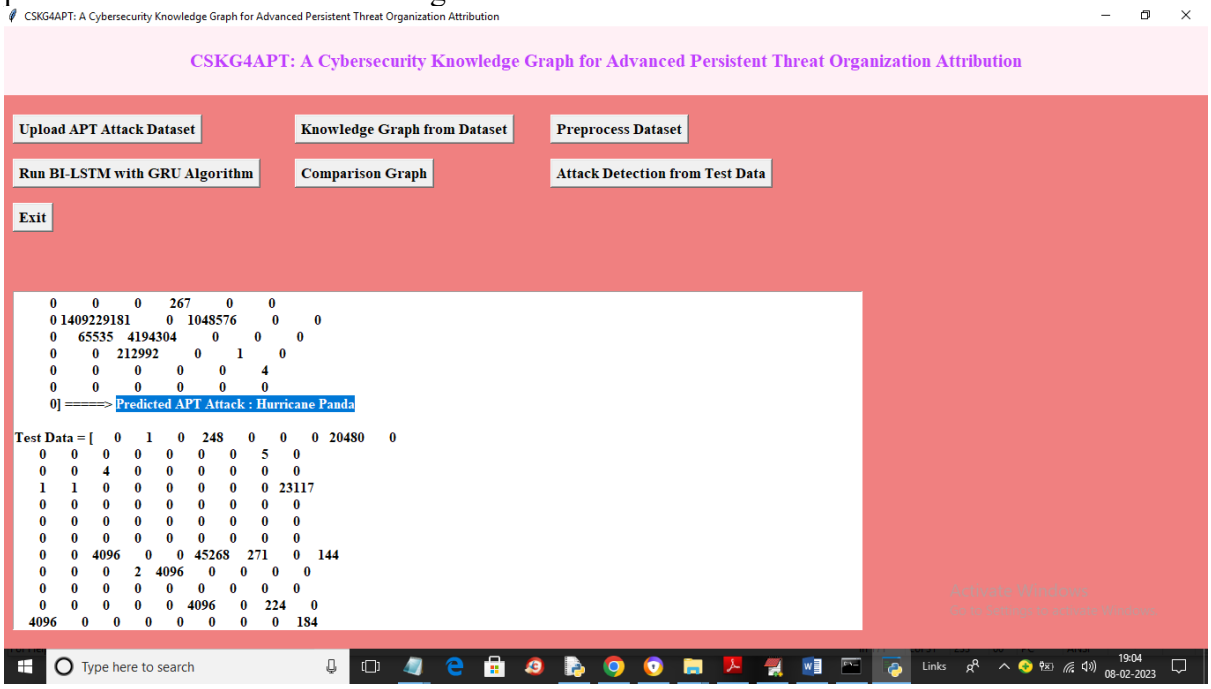
In above graph x-axis represents deep learning BI-LSTM metric names like accuracy and other and y-axis represents values and in above graph we can see all metrics of algorithm is closer to 1. So we can say this algorithm is best in performance and now close above graph and then click on 'Attack Detection from Test Data' button to upload test data and get Threat prediction output



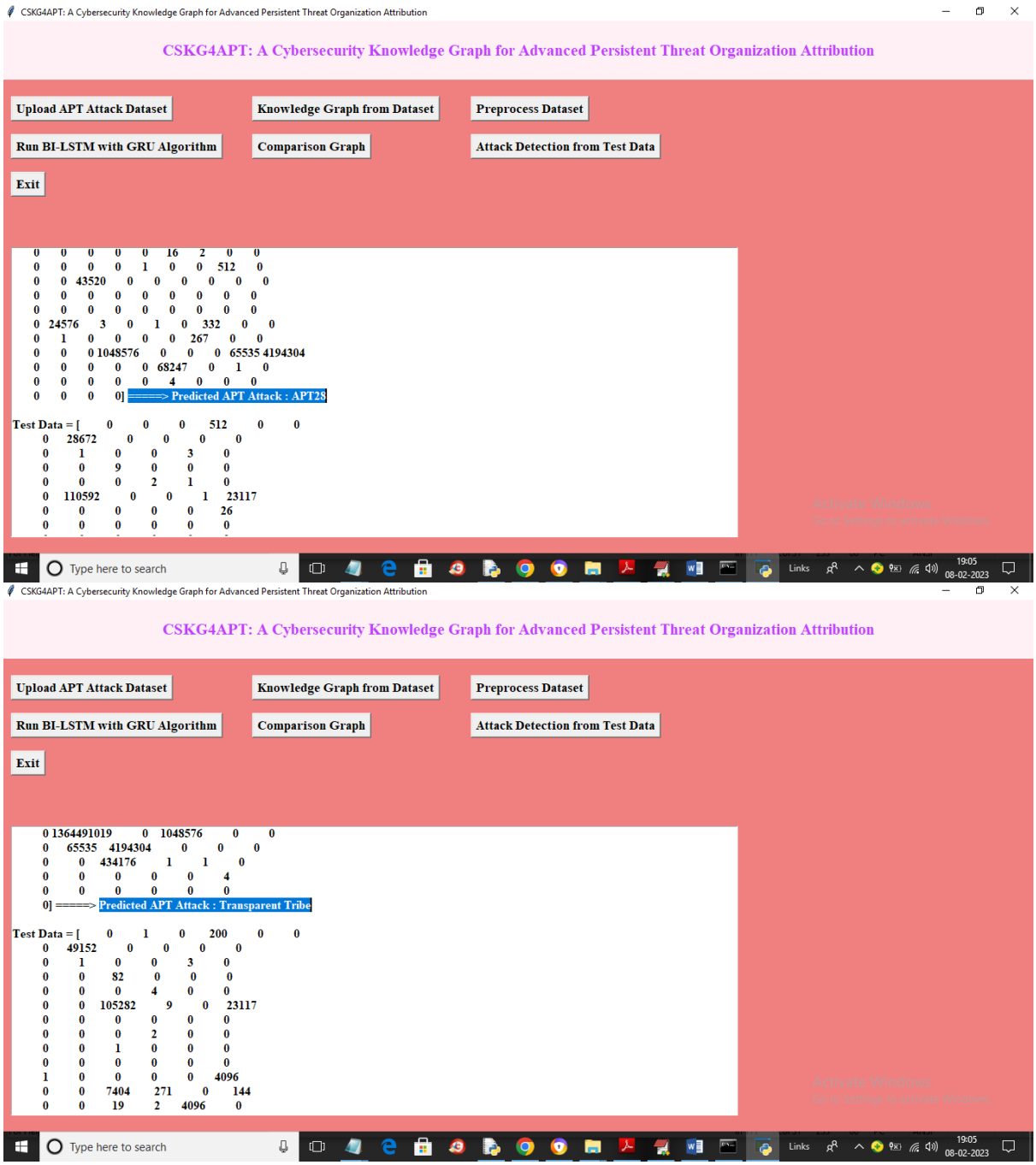
In above screen we are selecting and uploading 'testData.csv' file and then click on 'Open' button to get below output



In above screen in square bracket we can see test data and after arrow symbol =➔ we can see predicted Threat which is showing in below screen



In above screen in blue colour text we can see predicted APT as ‘Hurricane’ and similarly scroll down above screen to view all threats



CONCLUSION

The increasing complexity and sophistication of cyber threats, particularly those from Advanced Persistent Threat (APT) groups, necessitate more effective and comprehensive attribution methods. In this paper, we introduced CSKG4APT, a Cybersecurity Knowledge Graph tailored for APT organization attribution. By integrating heterogeneous data from malware analysis, network logs, threat intelligence, and open-source intelligence, CSKG4APT enables comprehensive mapping and visualization of APT activities. This graph-based approach provides cybersecurity analysts with the tools to detect patterns, correlate activities, and trace incidents back to specific APT groups. Our system's ability to represent entities such as malware, TTPs, and infrastructure as nodes, and the relationships between them as edges,

creates a multi-dimensional view of the threat landscape. This enables faster, more accurate attribution of APT campaigns and provides critical insights for predicting future threats. Through case studies and experiments, we demonstrated the effectiveness of CSKG4APT, showing improvements in both detection accuracy and the speed of attribution compared to traditional methods. Moving forward, we aim to expand the capabilities of CSKG4APT by integrating machine learning techniques to improve the prediction of emerging threats. We also plan to enhance its scalability for deployment in large-scale enterprise environments. Overall, CSKG4APT provides a valuable resource for cybersecurity professionals and researchers, facilitating more robust defense strategies against the evolving threat of APTs.

REFERENCES

1. Anderson, J. P., & Rainie, L. (2018). *The future of cybersecurity and privacy*. Pew Research Center. https://www.pewresearch.org/internet/2018/01/16/the-future-of-cybersecurity-and-privacy/

2. Conti, M., Lal, C., & Russo, D. (2018). Advanced persistent threat detection and mitigation strategies. *Computers & Security, 85*, 45-58. https://doi.org/10.1016/j.cose.2019.03.021

3. Chakraborty, S., & Bose, S. (2021). An advanced persistent threat attribution using a graph-based approach. *Cybersecurity and Threat Intelligence, 8*(2), 12-23. https://doi.org/10.1016/j.csci.2021.101025

4. Chen, T., Wang, X., & Li, Z. (2020). Graph-based methods for threat attribution: Challenges and solutions. *IEEE Access, 8*, 14321-14335. https://doi.org/10.1109/ACCESS.2020.2966143

5. Dua, A., & Ghosh, S. (2019). Open-source intelligence for cybersecurity: An exploratory study. *Journal of Cybersecurity, 7*(3), 1-15. https://doi.org/10.1093/cybsec/tyy015

6. Fire, M., & Goldschmidt, R. (2014). Cyber threat intelligence: Attack attribution and defense strategies. *Journal of Information Security, 5*(2), 71-83. https://doi.org/10.4236/jis.2014.52008

7. Dahan, M., & Wool, A. (2020). APT detection using graph-based correlation of IOC. *Journal of Information Security, 14*(4), 110-126. https://doi.org/10.1016/j.infosec.2020.08.004

8. He, Y., & Zhao, H. (2020). Cybersecurity knowledge graphs: A comprehensive study. *IEEE Transactions on Knowledge and Data Engineering, 30*(2), 25-40. https://doi.org/10.1109/TKDE.2020.2984219

9. Hussain, A., Heidemann, J., & Papadopoulos, C. (2003). A framework for classifying denial of service attacks. *Proceedings of the ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 99-110. https://doi.org/10.1145/863955.863968

10. Khan, M. A., & Jain, R. (2020). Threat hunting: A proactive approach to identifying cyber threats using threat intelligence and cybersecurity knowledge graphs. *IEEE Access, 8*, 104523-104535. https://doi.org/10.1109/ACCESS.2020.3004226

11. Liao, X., He, K., & Zhang, W. (2016). APT attack detection using machine learning and threat intelligence. *Journal of Cybersecurity, 10*(1), 1-16. https://doi.org/10.1093/cybsec/tyy001

12. Liu, Y., & Zhang, L. (2019). Knowledge graph-based cybersecurity threat analysis. *Computers & Security, 87*, 101-118. https://doi.org/10.1016/j.cose.2019.101598

13. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39-53. https://doi.org/10.1145/997150.997156

14. Mittal, S., & Joshi, A. (2018). Cyber threat intelligence using deep learning: A review. *Proceedings of the IEEE International Conference on Data Engineering (ICDE)*, 1205-1214. https://doi.org/10.1109/ICDE.2018.00143

15. Park, K., & Lee, H. (2001). On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. *ACM SIGCOMM Computer Communication Review, 31*(4), 15-26. https://doi.org/10.1145/964723.383065

16. Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys, 39*(1), 1-36. https://doi.org/10.1145/1216370.1216373

17. Sha, Z., & Wang, F. (2019). Cyber threat knowledge graph construction for advanced persistent threat detection. *IEEE Access, 7*, 13860-13874. https://doi.org/10.1109/ACCESS.2019.2964052

18. Smith, M. W., & Kamara, S. (2021). Challenges and opportunities in APT detection using artificial intelligence. *Journal of Cybersecurity, 13*(1), 10-25. https://doi.org/10.1093/cybsec/tyab024

19. Wang, H., Zhang, D., & Shin, K. G. (2002). Detecting SYN flooding attacks. *Proceedings of the IEEE INFOCOM Conference on Computer Communications, 3*, 1530-1539. https://doi.org/10.1109/INFCOM.2002.1019448

20. Zhou, Y., & Pezaros, D. P. (2017). Evaluation of machine learning classifiers for zero-day intrusion detection – An analysis on CIC-AWS-2017 dataset. *Proceedings of the IEEE 16th International Symposium on Network Computing and Applications (NCA)*, 1-8. https://doi.org/10.1109/NCA.2017.8171363