IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Mapping Cyber Threats: Constructing An APT Knowledge Graph From OSCTI

K. Snehalatha[1] DR. R. Yamuna[2]

1PG student, Vemu Institute of Technology,P.kothakota .

2 Associate Professor, Vemu Institute of Technology, P.kothakota.

ABSTRACT

as the project pioneers the use of open-source cyber threat intelligence (OSCTI) to bolster network security via a cybersecurity knowledge graph. This innovative graph streamlines access to a range of threat information, empowering informed decision-making. Leveraging attribution technology, the initiative detects and pinpoints advanced persistent threats (APTs) across diverse attack scenarios. Integrating cutting-edge knowledge graph technology with research on cyber threat attribution, the team introduces CSKG4APT, a robust cybersecurity platform. This platform harnesses ontology theory to craft an APT-centric knowledge graph model and deploys deep learning algorithms for knowledge extraction and updating. By introducing effective APT attack attribution techniques, the project amplifies network defense strategies, enabling proactive defense against rapidly evolving threats.

Keywords: Cybersecurity, deep learning algorithms

INTRODUCTION:

In an era marked by explosive data growth and advancements in artificial intelligence, the landscape of cybersecurity has grown increasingly complex. Advanced Persistent Threat (APT) attacks, initially coined by the U.S. Department of Defense, represent persistent, sophisticated assaults targeting critical enterprise assets, national infrastructure, and government departments. These evolving attacks, as highlighted by a Kaspersky report, encompass diverse strategies like supply-chain breaches and firmware vulnerabilities. Traditional cybersecurity defenses have proven inadequate against these sophisticated threats, largely due to the information asymmetry favoring attackers. Cyber Threat Intelligence (CTI) emerges as a pivotal tool, enhancing defense capabilities by facilitating timely intelligence sharing and analysis. While structured indicators of compromise (IoC) offer direct evidence of malicious activities, unstructured open-source cyber threat intelligence (OSCTI) reports provide in-

depth APT attack analyses. However, the burgeoning volume of threat data presents challenges in effectively leveraging OSCTI due to its varied quality and complex nature.

LITERATURE SURVEY:

Z. Zhu and T. Dumitras*et al*

Author proposes an innovative approach to integrate quantitative field data on cyber attack campaigns with qualitative manual analyses. Recognizing the time-consuming nature of manually analyzing natural language reports, the proposed solution leverages a 4-stage model from threat intelligence. This model describes each stage using Indicators of Compromise (IOCs) like URLs and IP addresses. A multi-class classifier is trained to extract and categorize these IOCs into different campaign stages. Implemented in a system named ChainSmith, this approach demonstrates high precision and recall rates in extracting IOCs and determining campaign roles. By analyzing 14,155 online security articles, ChainSmith identifies 24,653 IOCs, enabling the linkage of manual attack analysis with broader field measurements. Notably, the study reveals the prevalence and effectiveness of persuasion techniques like the "missing codec" ruse in enticing users to download malicious payloads.

Y. Gao, X. Li, H. Peng, B. Fang*et al*

Author introduces HinCTI, a groundbreaking system designed to address the complexities of modeling cyber threat intelligence (CTI) and identifying threat types. Recognizing the increasing sophistication and organization of cyber attacks, organizations worldwide are increasingly seeking open exchange of CTI to enhance their cyber defense capabilities. However, the heterogeneous nature of cyber-threat infrastructure nodes and limited labels pose challenges in CTI modeling and early threat identification. HinCTI addresses these challenges by first designing a threat intelligence meta-schema to represent semantic relationships among infrastructure nodes. Leveraging a heterogeneous information network (HIN), HinCTI integrates diverse infrastructure nodes and their relationships. The system further employs a Meta-path and Meta-graph instances-based Threat Infrastructure Similarity (MIIS) measure, coupled with a heterogeneous graph convolutional network (GCN) approach, to identify threat types effectively. Additionally, hierarchical regularization strategies mitigate overfitting, ensuring accurate threat identification. This pioneering work on HinCTI sets a new precedent by modeling CTI on HIN and introducing a GCN-based approach for infrastructure node threat type identification, validated through comprehensive real-world dataset experiments.

K. Satvat, R. Gjomemo*et al*

Author introduces Extractor, a pioneering tool designed to streamline the extraction of precise attack behaviors from Cyber Threat Intelligence (CTI) reports. Recognizing the invaluable insights embedded in CTI reports, but hindered by their unstructured, text-heavy nature, Extractor offers a novel solution. This tool employs a flexible approach, making minimal assumptions about the text, and excels in extracting attack behaviors as provenance graphs from unstructured data. Through rigorous evaluation with real-world incident reports and

DARPA adversarial engagement reports spanning multiple OS platforms, including Windows, Linux, and FreeBSD, Extractor proves its efficacy. The evaluation underscores Extractor's capability to derive concise provenance graphs from CTI reports, validating its utility for enhancing cyber-analytics tools in threat-hunting endeavors.

PROBLEM STATEMENT:

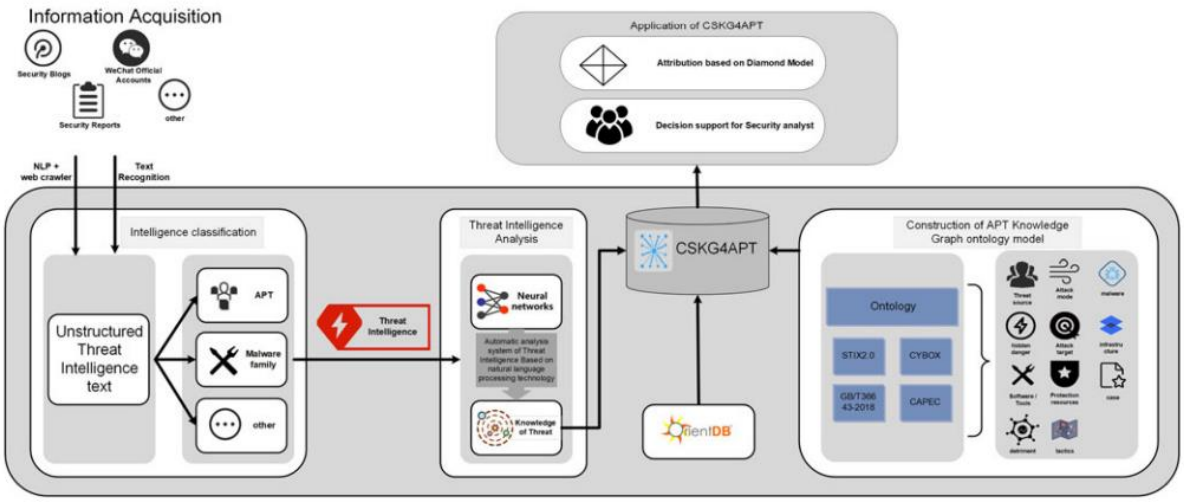
Networks always face security issues with different types of attack in which some are permanent and some are non-permanent. APT (advance Persistent Attack) remain in network permanently. Existing algorithms on cyber threat intelligence (CTI) focus on automating the extraction of threat entities from public sources thatdescribe attack events but this technique is not feasible.

PROPOSED METHOD:

Building ontology based knowledge graph from APT dataset to extract network features and then employing deep learning BI-LSTM with GRU layersalgorithm to train a model on APT graph features and this model can be applied on any network test data to identify whether test data is normal or contains any APT attacks.

To implement this project author has used APT Text base network dataset and then apply BERT (bidirectional encoder representations from transformers) algorithm on text data to convert into numeric vector and this vector contains average frequency of each words from the dataset. This BERT vector will be input to BI-LSTM with GRU algorithm to train a model and this model will be applied on test data to calculate prediction accuracy, precision, recall and FSCORE.

ARCHITECTURE:



CYBER SECURITY DATASET:

In above dataset screen first 4 rows contains words from the dataset and remaining words contains average frequency of each words under that column word name. This dataset will be input to deep learning algorithm to train a APT attack detection model

METHODOLOGY:

User Interface Development:

The project initiates with the creation of an intuitive user interface (UI) using Tkinter, a renowned GUI toolkit compatible with Python. Tkinter facilitates the development of an interactive and user-centric interface that ensures seamless navigation and functionality.

Data Loading:

Users are provided with the capability to upload the Advanced Persistent Threat (APT) attack dataset directly through the graphical interface. Upon selecting the dataset file, the program leverages the Pandas library to load the dataset efficiently. It further offers a preview by displaying the initial rows of the dataset, allowing users to inspect the data before proceeding with analysis.

Knowledge Graph Creation:

The dataset undergoes meticulous processing to construct a comprehensive knowledge graph, illustrating intricate relationships between various attributes like MD5 hash values, APT attacks, and Dynamic Link Library (DLL) files. The networkx library serves as a valuable tool in formulating the knowledge graph based on the refined dataset. To enhance user understanding and visualization of the data relationships, Matplotlib is employed to depict the knowledge graph graphically, enabling users to discern patterns and connections among different entities in the dataset.

Dataset Preprocessing:

To ensure accurate and efficient analysis, the dataset necessitates preprocessing before training the machine learning model. This phase involves addressing missing values by substituting them with zeros and employing the LabelEncoder from Scikit-learn to transform categorical variables into a numerical format. Subsequently, the dataset is divided into input features (X) and target labels (Y) to facilitate supervised learning through training and testing stages.

Algorithm Implementation:

The project emphasizes the implementation of the Bidirectional Long Short-Term Memory (BI-LSTM) model, augmented with Gated Recurrent Unit (GRU) layers, specifically tailored for APT attack detection. The BI-LSTM model architecture encompasses input layers, bidirectional GRU layers to capture temporal dependencies effectively, dropout layers for regularization to prevent overfitting, and output layers dedicated to prediction. The model is meticulously compiled, incorporating suitable loss function and optimizer configurations to optimize training efficiency. During the training phase, the BI-LSTM model is trained utilizing the training data while validating against the test data. Furthermore, model checkpoints are integrated to preserve the best-performing model for future utilization and deployment.

Performance Evaluation:

Upon successful training of the BI-LSTM model, its efficacy and performance are rigorously evaluated utilizing diverse metrics such as accuracy, precision, recall, and F1-score. Confusion matrices are generated to offer a visual representation of the model's proficiency in categorizing different APT attacks accurately. Additionally, the trained BI-LSTM model is deployed to predict APT attacks from the test data, enabling the assessment of its generalization capability and reliability.

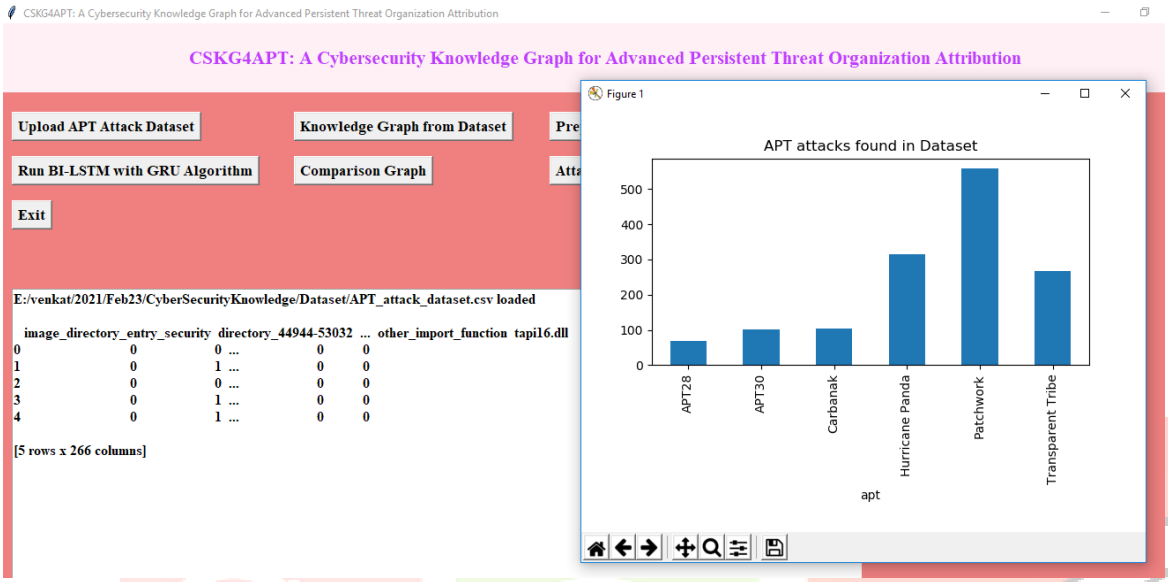
Visualization:

To furnish users with comprehensive insights into the performance and efficiency of the BI-LSTM model, comparative visualizations are generated. Bar graphs are crafted utilizing Matplotlib to exhibit the comparison of metrics including accuracy, precision, recall, and F1-score across various algorithms or models, facilitating informed decision-making and analysis.

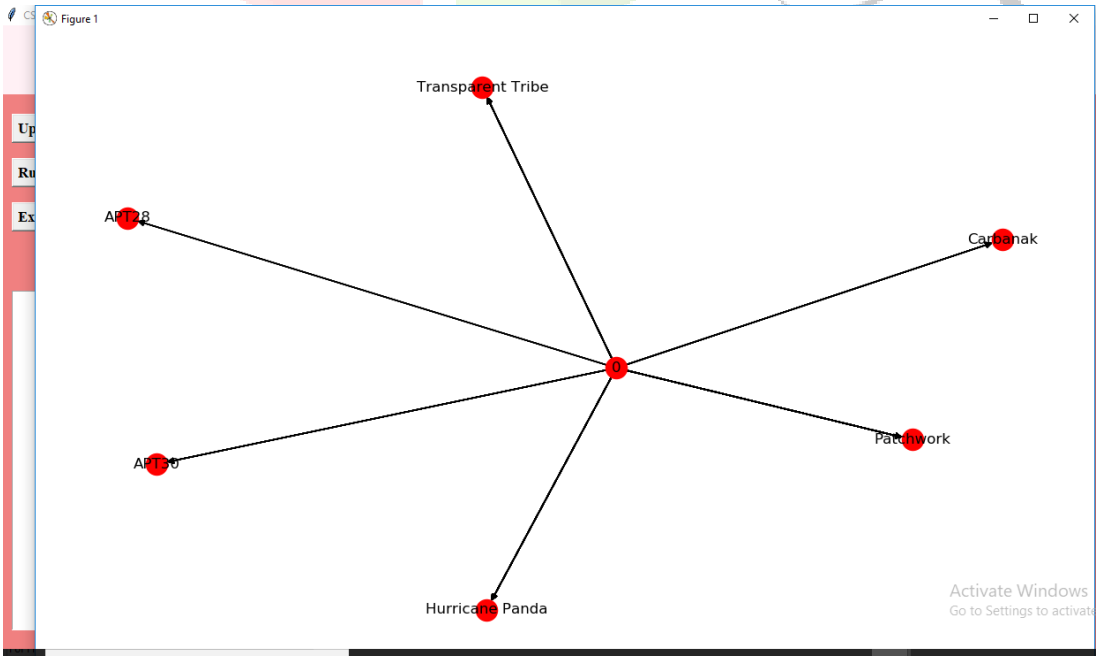
Attack Prediction from Test Data:

Empowering users with an interactive experience, the developed system facilitates input of test data to the trained BI-LSTM model for APT attack prediction. The model meticulously evaluates each input data point, predicting the corresponding attack type. The predictions are subsequently displayed to the users via the intuitive GUI, offering actionable insights and aiding in proactive threat management and response strategies.

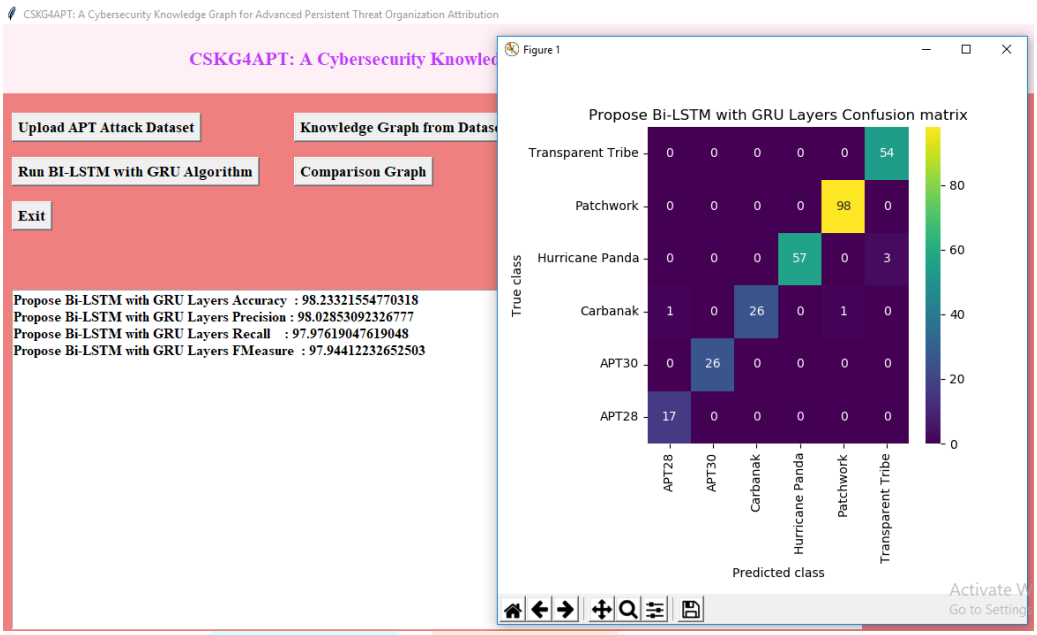
RESULTS:



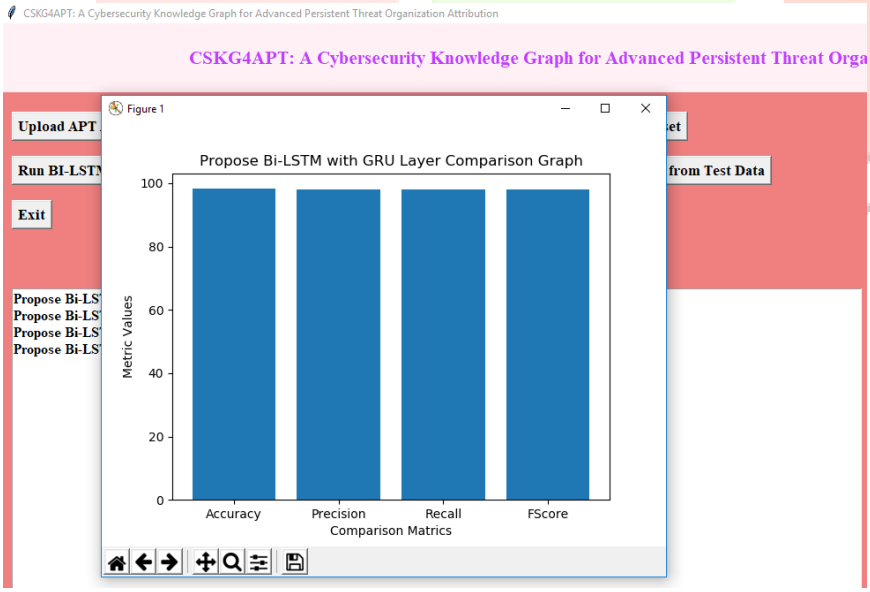
In above in text area we can see dataset loaded and in graph we can see x-axis contains APT names and y-axis contains attack count and now close above graph and then click on 'Knowledge Graph from Dataset' button to build graph and get below output



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

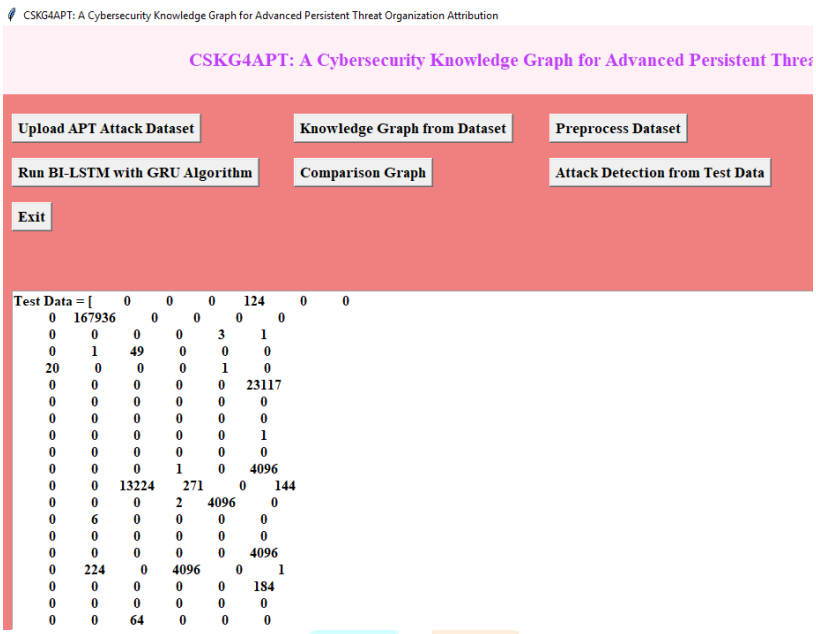


In above screen with deep learning BI-LSTM algorithm we got 98% prediction accuracy and in confusion matrix graph x-axis represents Predicted Threat Labels and y-axis represents True labels and all blue colour boxes contains incorrect prediction count which are very few and all different colour boxes 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

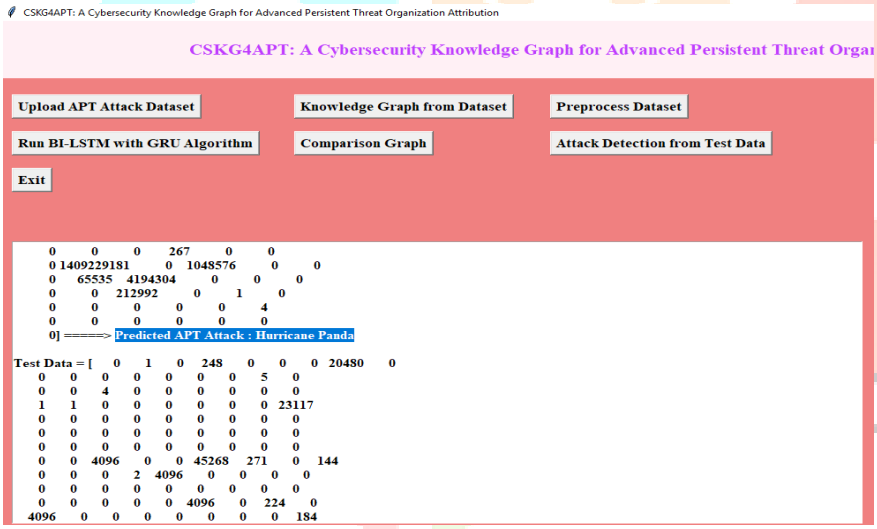


In above graph x-axis represents deep learning BI-LSTM metric names like accuracy and other and y-axis represents values and in above graph we can see all metrics of algorithm is closer to 1. So we can say this algorithm is best in performance and now close above graph and then click on ‘Attack Detection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

Prediction:



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 in blue colour text we can see predicted APT as ‘Hurricane’

CONCLUSION

This CSKG4APT project aims to revolutionize cybersecurity by leveraging advanced technologies like Knowledge Graphs and Deep Learning to detect and attribute Advanced Persistent Threat (APT) attacks. By constructing an ontology-based knowledge graph from real APT attack scenarios and employing a BI-LSTM algorithm with GRU layers, the project achieves remarkable accuracy in identifying APT attacks. The methodology involves uploading the APT dataset, building a knowledge graph, preprocessing the data, training the deep learning model, and evaluating its performance. Through extensive testing and comparison, the proposed approach demonstrates superior performance, achieving 98% prediction accuracy. This project signifies a significant advancement in cybersecurity threat detection and attribution.

REFERENCES:

[1] Advanced Persistent Threat, 2020. [Online]. Available: https://en. wikipedia.org/wiki/Advanced_persistent_threatInfo rmation and communication technology

[2] APT Annual Review, 2021. [Online]. Available: https://securelist. com/apt-annual-review-2021/105127

[3] T. Zhihong, "Detection and traceability of high covert unknown threats in cyberspace," Inf. Commun. Technol., vol. 14, no. 06, pp. 4–7, 2020.

[4] L. Yue et al., "Overview of network security threat intelligence sharing and exchange," Comput. Res. Develop., vol. 57, no. 10, pp. 2052–2065, 2020.

[5] Z. Zhu and T. Dumitras, "ChainSmith: Automatically learning the semantics of malicious campaigns by mining threat intelligence reports," in Proc. IEEE Eur. Symp. Secur. Privacy, 2018, pp. 458–472.

[6] Y. Ghazi, Z. Anwar, R. Mumtaz, S. Saleem, and A. Tahir, "A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources," in Proc. Int. Conf. Front. Inf. Technol., 2018, pp. 129–134.

[7] Y. Zhao, B. Lang, and M. Liu, "'Ontology-based unified model for heterogeneous threat intelligence integration and sharing," in Proc. 11th IEEE Int. Conf. Anti-Counterfeiting Secur. Identification, 2017, pp. 11–15.

[8] Y. Guo et al., "CyberRel: Joint entity and relation extraction for cybersecurity concepts," in Proc. Int. Conf. Inf. Commun. Secur., 2021, pp. 447–463.

[9] G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, and X. Niu, "TTPDrill: Automatic and accurate extraction of threat actions from unstructured text ofCTI Sources," in Proc. 33rd Annu. Comput. Secur. Appl. Conf., 2017, pp. 103–115.

[10] Z. Li, J. Zeng, Y. Chen, and Z. Liang, "AttacKG: Constructing technique knowledge graph from cyber threat intelligence reports," 2021, arXiv: 2111.07093.

[11] A. Singhal, "Introducing the knowledge graph: Things, not strings," Official Blog (of Google), 2012. Online]. Available: http:// googleblog.blogspot.co.uk/2012/05/introducing-knowledgegraph-things-not.html

[12] W. Haofen, Q. Guilin, and C. Huajun, Knowledge Graph: Method, Practice and Application, Beijing, China: Publishing House Electron. Ind., 2019.

[13] STIX, 2022. [Online]. Available: https://oasis-open.github.io/ctidocumentation/stix/intro

[14] CAPEC, 2019. [Online]. Available: http://capec.mitre.org/about/ index.html

[15] C. N. Li and S. A. Thompson, "Mandarin chinese: A functional reference grammar," J. Asian Stud., vol. 42, no. 3, pp. 10–12,1989. [16] A. Alsaheel et al., "ATLAS: A sequence-based learning approach for attack investigation," in Proc. 30th USENIX Secur. Symp., 2021, pp. 3005–3022.

[17] CYBOX, 2020. [Online]. Available: http://cyboxproject.github.io/ sample

[18] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," Center for Cyber Intelligence Analysis and Threat Research Hanover Md: Ft. Meade, MD, USA, 2013.

[19] TAXII, 2019. [Online]. Available: https://taxiiproject.github.io/

[20] MANDIANT, "Sophisticated indicators for the modern threat landscape: An introduction to OpenIOC," White Paper, Jun. 2017. [Online]. Available: http://openioc.org/resources/AnIntroductiontoOpenIOC. pdf