International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Cyber Threat Intelligence Extraction in Power Sector Using Deep Learning

[1]Abir Dutta, [2]Bharat Bhushan, [3]Shri Kant

Submitted: 16/01/2024 **Revised**: 24/02/2024 **Accepted**: 02/03/2024

Abstract: Techniques, tactics, and procedures (TTPs) for threat intelligence (CTI) domain identification and extraction helps security analysts to determine the technical risks and recover the entire picture of cyber-attacks. Without sufficient domain background, frameworks can scarcely offer standard and comprehensive processing methods for TTPs extracting information. In this study, a multi-instance learning method called Power Sector Mask is suggested as a remedy of such backdrops. Power Sector collects behavioural epoch from CTI and using conditional distribution, forecasts the labels of TTPs. Yet, the structure provides two ways to assess the legitimacy of terms. One employing verification from experience by obstructing already-existing epoch, the other one confirms the misrepresentation of the categorization effect. In the trials, Power Sector achieved F1 scores for TTP Techniques of power sector mask model viz. AR_mask, SV_mask and MP_mask is 20.70%, 68.33% and 68.50% and F1 scores for TTP Tactics CNN and RNN are 30.7%, 67.34% and 69.70% respectively. In particular, deep leering model is use classification of model of F1 score in Tactics is better or lower than mask Techniques. In this research we also confirm the feasibility to obtain TTPs from malware with an enhanced F1 of POS-CNN is better/lower than all CNN and RNN.

Keywords: *Multi-Instance Learning; Cyber Threat Intelligence; Tactics, Techniques and Procedures (TTPs); Behaviour Analysis; Information Extraction; Tactics.*

1. Introduction

The median weekly amount of safety issues by digital trade in 2023 climbed by 15% to 69% in comparison with 2022, as per Verify Spot's 2023 semi-data [1] 2023. With 2297, 1669, and 1457 weekly incidences, sequentially, Academic and Investigations, Federal Government, and ISP/MSP were listed as the top 3 within these. Yet, the cyber defines has progressively become more challenging and regular in the midst of hostile strikes [2]. Significant factor for this is that there is not enough proof to back up how actions should be seen and prevented [3]. On the reverse side, the profession gap in information security has grown due to the prolonged education and expertise acquisition periods [4]. In order to effectively identify, manage, and respond versus online fraud, it is crucial to fully utilize necessary details. This is the foundation of any effective defense against cyber-attacks.

Malware awareness has been highlighted as a strategy to combat major crimes in light of the rising scale and complexity of cybersecurity threats [5]. The important data in Cyber Threat Intelligence (CTI) can be organized into Indicators of Compromise (IoCs) by sharing and summarizing it. These IoCs include hashes, host id, hostname, connection or host characteristics, offensive weapons, and tools and Tactics, Techniques and Procedures (TTPs) [6]. TTPs are among the IoCs that explain the target frequency, attack techniques, objectives, and processes, as well as other critical indications for modelling risk behaviour. TTPs can provide investigators with information regarding downside problems, reactive deficiencies, as well as the detection and rejection of particular assaults by characterizing features and developing processes. TTPs are legitimately the top mark among all IoCs members as a consequence [7, 8]. The most important parts of computerized TTP assessment are now the classification and data extraction steps. Integrating textual vectors into TTPs is the primary priority of identification methods levels.

As an instance, rcATT [9] deals with the entire CTI using TF-IDF and Liner SVC, whereas HM-ACNN, TCENet [10], and ATHRNN [11]opt to merge deep neural networks. Using recurrent neural networks (RNNs), awareness, and convolutional neural networks (CNNs) to improve the greater vector meaning of Power Sector who did what to whom" feature of TTP activities is understood through data exploration activities. Utilizing Topic, Verb, and Item (SVO) only or Phrase and Entity (VO) principles, TTPDrill [12], Action Miner [13], EX-Action [14], and Injector [15] and only Verb and Object (VO) or Subject, Verb and Object (SVO) from phrases to shape methods, which was before machine-learning tools like Stanford CoreNLP [16], SpaCy [17], or Word vectors [18].The accompanying issues need to be resolved despite the fact that the aforementioned approaches could find or

[1]*Deptt. of Computer Sc. and Engg, Sharda University, Greater Noida, India, abir_wbsetcl@yahoo.com*
[2]*Deptt. of Computer Sc. and Engg, Sharda University, Greater Noida, India, bharat.bhushan@sharda.ac.in*
[3]*Center of Cyber Security and Cryptology, Sharda University, Greater Noida, India, shri.kant@sharda.ac.in*

detect some of the TTP's content in CTI. Due to their black-box nature, machine-learning-based techniques find it challenging to locate TTPs successfully Nature, making it impossible to create TTP entities. There are three key areas where knowledge discovery technologies have limitations [19]. Firstly, Difficult process- Prior knowledge extraction systems relied heavily on NLP techniques, making engineering replication and implementation difficult a difficult setting. Secondly, Incomplete verification- Web mining is good at finding similarities between behavioral sentences, but it can't figure out where the words in a phrase came from identifying techniques only look at the ability to put things into groups and lastly, Lack of data: The database extraction's primary goal is to extract Power Sector check word SVO and VO Power Sector, which will screen out non-SVO and non-VO files causing some of the proof to be erased. A cyber threat intelligence-capability model (CTI-CM) Bongsik Shin and Paul Benjamin Lowry (2020), espoused the details structure of the CTI which provides a guideline for security personnel simultaneously builds a theory for Organizational security and behavioral security in future course of action as shown in Figure 1 (Thomas D. Wagner et al., 2019; Stjepan Groš, 2020).

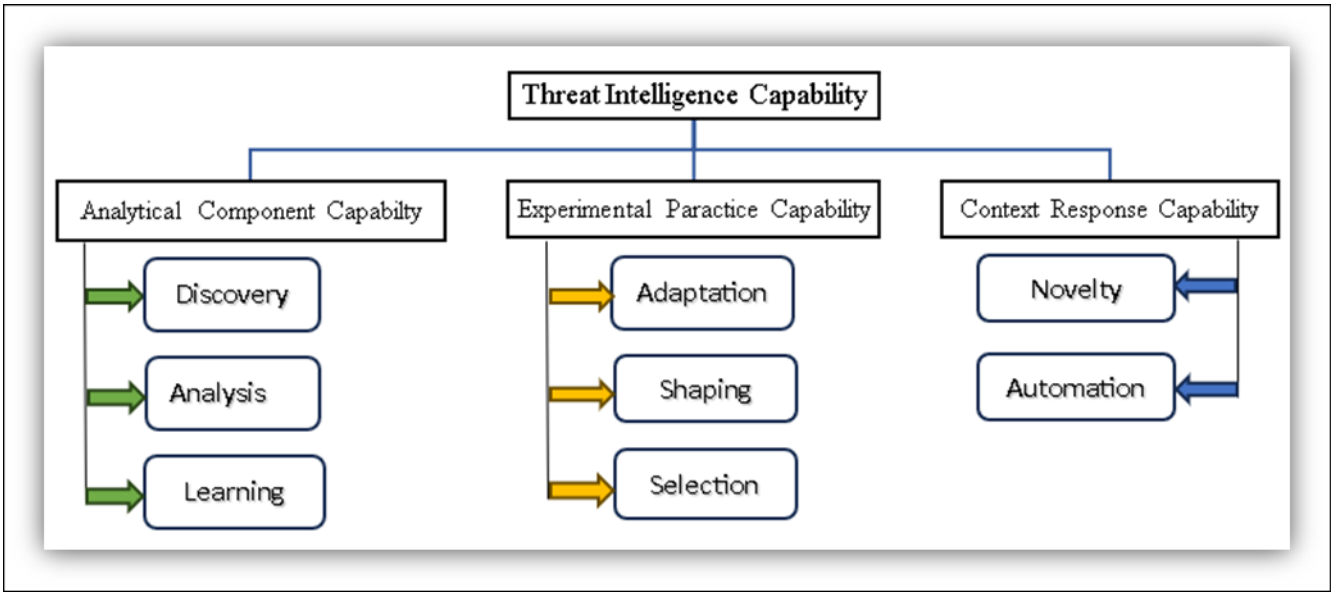


Fig 1: CTI Capability Model

In this research study following research questions are address **RQ1:** In Power Sector, how a deep neural system built on multi- instance learning (MIL), for the quick but efficient management of TTPs? **RQ2:** What will be the impact of the key phrases Power Sector filters behavioural data and identifies TTPs by applying a semantic learning algorithm to n-gram expressions and words that "lie below the median of all words in nearby subspace". **RQ3:** Unlike techniques like SVO and VO, why Power Sector does not require Piece of Talk (POS) to process the text to extract threat intelligence?

The following are indeed the novelties and additions in our research paper:

- Implementation of identity-mission checking approach in the Power Sector used to identify. TTPs in this research don't just focus on TTPs. Virus as well as complete and relatively brief CTI collection studies. The findings of the trial wholeheartedly endorse Power Sector compliance and flexibility.
- Data integrity metrics across several perspectives using Power Sector keyword extraction tool, two high-quality Techniques for analysis are described. Using the Jaccard commonality, the differences between the algorithms and the expert-screened keywords were assessed. Others "destroy" the previous model by hiding the data that scored highly and logging the decline in recognition rate.
- A derivation of weakly monitored behaviour in Power Sector. We employ MIL to collect TTPs data from CTI as opposed to the filtration approach that was created manually. A semi supervised method in Power Sector discovering scene with no established floor inspection rating that aims to explain the donation of phrases or terms to TTPs in CTI.

Rest of the paper is organized into five section like: in section II we will explain about the earlier research conducted in this domain i.e. state-of-the-art of cyber threat intelligence in energy sector especially in power domain. Whereas, Section III illustrates the approach of our proposed model using Deep learning and Machine Learning approach. Section IV of our paper describe the details of the experiment environment. Section V provided the insights of our experiment at the same time related discussion of the result and Finally, Section VI describe the conclusion of our methodology along with future prospects of the research.

2. Related Work

According to Mavroeid is [20,21], CTI is the mission of gathering evidence-based knowledge, as well as sense, mechanisms, indicators, consequences, and expert way. CTI information can be broadly categorized as statistical data on sites and financial planning [22], intelligence on vulnerabilities and weaknesses [23], data on assault behaviour and defenses [24, 25], and data on structured entities [26]. Nowadays, current research across CTI has focused on two areas. They are identifiers and content removal. Finding unique patterns from CTI, such as recognizing virus kinds [27], places and actions [28], and offensive Power Sector, is the main focus of the detection step. These methods rely on algorithms using deep learning, whose forecasts could be hazy ideas or judgments devoid of clear-cut proof. Information extraction tasks, unlike 'fuzzy' recognition tasks, anticipate obtaining information of special value from unstructured CTI text. This data, known as IoCs, can serve as direct proof of an offense and comprises servers [29], domains/URLs [30], e-mails [31], hashes [32], organizations [33], and spyware copies [34,35]. For instance, Fujii [35] uses known object acknowledgement to derive IoCs from CTI text. Yaman [36] seeks location facts from CTI text using sGlo Ve and Lengthy Short Attention Span (LSTM) networks. TTPs are the ones that need the most focus out of all the CTI-related feedback. TTPs are viewed on only one half as a link between specific evidence and activity goals [37, 38]. TTPs, on the other hand, exhibit some resilience to disruption, which can make the assault characteristics more generic and routine [39]. Moreover, TTPs have unique definitions that specify document situations, trigger events, success criteria, operational traits, and Power Sector objectives. Because of the previously mentioned three characteristics, TTPs can exist between concept and implementation, allowing data derived and detection techniques suitable for TTPs data drug activity prediction [40,41,42]. In this case, rather than receiving categorization data sources for a pair of perfectly alright tags known as "cases," replicas are wrapped into a "package" to provide a consistent yes or no reaction. The objective of the game is to research the classification laws of ‘situations’ by investigating probable logical "connections" among ‘packs’ and ‘incidents’, beginning by understanding the selected features of 'bundles'. MIL has been used in Power Sector analysis for a long time. Author [43] constructs a K-Nearest Neighbor grouping algorithm for literature by treating sentences as instances. Bao [44, 45] modifies the radial basis principle to allow for written text cross-referencing.

Although TTPs are crucial, their examination is only in the Power Sector stages. Those analytical methods also involve two steps: information recovery and classification. The identifications are primarily based on machine learning or deep learning techniques that package CTI text into a model to predict Power Sector. For instance, rcATT [46,47,48] classifies TTPs for CTI using algorithms for machine learning like SVM and irregular forest, but it omits to inform the user of the rationale and pertinent justifications for doing so. Unfetter Insight can classify TTPs faster by comparing results from Babe fish technology and CTI classifying on the website. By utilizing a hybrid approach that combines attentiveness, inverter, and RNN, ATHRNN enables CTI text to enroll in the identification of TTPs. HM-ACNN employs learned migration to achieve some parametric recycling of the sTTPs trained model. Contrary to end-to-end evidence-related approaches described above, some academics have engaged in knowledge discovery to establish what generates TTPs. The IoCs information is extracted using pattern matching and reference books, and the TTPs organization retrieval is accomplished with the aid of BERT (word embedding and illustration from converters), BiLSTM (backpropagation long short attention span), and recognition. According to TCENet, "the above technique can only release the title of TTPs, but it is difficult to provide precise details. "SECCMiner uses TF-IDF (Term Frequency-Inverse Document Frequency) rated individual lexical items in vulnerability management papers to search for TTPs. ActionMiner constructed SVO rules to exclude all words that fit the text's "who did what" facts, and it used local similarity rules using data unpredictability to eliminate phrases that fit the message's explanation of TTPs. TTPDrill uses familial separation to construct the sSVO metaphysics and TF-IDF and BM25 to assess the correlation between SVO and TTPs. The survey of TTPs is completed by EX-Action, which utilizes both earlier techniques and makes use of normalized information gain and machine learning techniques like SVM. After producing the SVO, Extractor further extracts entity relationships and behavioral conditions to refine and produce APT attack graphs.

TTPDrill, EX-Action, ActionMiner, and Extractor can get greater strategy specifics than rcATT even with accurate specialist expertise in scrubbing data, but they are unable to judge tactics as intelligently as rcATT does. Thus, the sexist task is to adjust the examination of nature and the persistence of various types of strategies and methods of information with varying levels of abstraction. To accomplish the aforementioned objective, it is essential that you think about how to persuade the algorithm to evaluate the need for the contribution and bring in the identification of TTPs only if there aren't any abstract restraints. Given similar requirements, the treatment will most likely be faulty poorly guided learner [56][57]. A fine-grained segmentation case with only generalized labels is discussed in the imperfect badly directed learning. If CTI is known to be associated with a TTPs

tag, the circumstance might be represented as the topic "If CTI is known to be associated with a TTPs tag, the evidence relating to the TTPs is requested.". The remedy to the inaccurate, poorly controlled training is MIL. MIL first appeared in medical drug activity prediction. In this case, rather than receiving categorization data sources for a pair of perfectly alright tags known as "cases," replicas are wrapped into a "package" to provide a consistent yes or no reaction. The objective of the game is to research the classification laws of ‘situations’ by investigating probable logical "connections" among ‘packs’ and ‘incidents’, beginning by understanding the selected features of 'bundles'. MIL has been used in text analysis for a long time. Author constructs a K-Nearest Neighbour grouping algorithm for literature by treating sentences as instances. Bao modifies the radial basis principle to allow for written text cross-referencing[58].Methodology

3.1. Power Sector mask method overview: The Power Sector structure is built on MIL in this study to provide a simple and comprehensive way for recognizing and separating TTP documentation. The primary goal of Power Sector is to target the process of a system analyzing in Power Sector, comprehending, and generalizing words on its own. After removing non-SVO/VO terms once, traditional information extraction techniques only leave a small window for Power Sector categorization. On the other extreme, Power Sector evaluates the text and offers the best subspace for it based on its realization of logic. It then combines the main points into the appropriate semantic labels. As a result, power sector can handle the fundamental needs of "data integrity," yet doesn't abandon the complete overview and substance when interacting with Power Sector extraction.

Power Sector must resolve the usual mixture of definitional spread in order to respond to the question of "What and how do the semantics hinder the TTP's titles?" Using deep learning techniques, such as the combination of attention mechanisms can be divided into three primary jobs- Firstly, TTPs potential assumption: Using the semantic spread to determine Power Sector and to demonstrate that the as a way to figure out how full and useful the buzzwords in the data collected by Power Sector are, a list of filtration assessment techniques has been given. The next parts will explain each of the aforementioned four stages. Secondly, information extraction: linguistics transfer of CTI scalar aspect partitioning; and finally, classifying words: how to turn CTI letters into vector features that deep learning can understand.

3.2. Text representation: Before being fed into Power Sector, CTIs will be split into lines so that they don't cause too many arguments that aren't necessary Also, to avoid needless lexicon expansion because of We applied regularized techniques for written form decrease, and data filtering to address term occlusion and case problems. As an example, whenever the assertion "TA459 has used Text Editor Flaw CVE-2023-0199 for implementation. Vocabulary character of "has used" and change or remove the digits. For example, replace "CVE-2023-0199" and "TA459" with "TA" and "sensitivity, respectively. All capitalization will thereafter be changed to normal for all signs. To summarize, the preceding sentence will be rephrased as "to have attack Word documents weakness vulnerability for action." Because Power Sector is a standard deep learning technique, CTI text must be converted into a continuously distributed word pasting signal during preparation. We taught a fast Text vector space affirmation from over 15,000 internet security publications from Shadow Research.

Clarifying a few of the writer's presumptions is important before introducing the ensuing approaches equation (1). Suppose that the first CTIs are made up of statements in a set of w that equal n units arrange:

$$S = < s^{(1)}, s^{(2)}, \ldots s^{(n)} > \quad \textbf{(1)}$$

The collection of integration service vectors in S is known as e- e = < e1, e2, …, en. Every member of the group, ei € e, has m lengths equation (2).

$$e_i = e_i^{(1)}, e_i^{(2)}, \ldots e_i^{(m)} \quad \textbf{(2)}$$

The dimension of the deep feature matrix is m in these other vocabularies. Assuming w(k) is the group of k-grams equation (3):

$$W(k) = < w_{(k)}^{(1)}, w_k^{(2)}, \ldots, w_{(k)}^{(n)} \quad \textbf{(3)}$$

It transforms the w set of sentences composed of k consecutive words equation (4). Ek is a collection of w's k-gram expression vectors (k).

$$E_k = E_{1,k}, K_{2,K,\ldots}, K_{n,k} \quad \textbf{(4)}$$

3.3. Information extraction: The necessary phases can be used to define the data optimization technique in Power Sector. In first phase is to create the terms set, as indicated in equation (5). When the shortening threshold reached? We considered CTI texts as W and the label l in TTPs with semantic distributions must be generated in the second stage equation (6) such that the dependent heterogeneity $H(l|w_\theta)$ is nearly zero. At this time, it is possible to see Was the entire collection of crucial details that are closely associated with the specific markers l, so we decided to call it $w_l^{(\theta)}$.

$$w_\theta = Extract\ (w, \theta) \quad \textbf{(5)}$$

$$H\ (l|w_\theta) \rightarrow \mathbf{0} \quad \textbf{(6)}$$

A deep learning system, like the one shown in Fig. 2, has been made to do the above operation. The model starts by using a deep feature technique to create the meaning subspace. CTI. Afterward, use CNN to determine the

combined meaning of n-grams. After creating the distributed storage for thematic arrays, Power Sector filters out crucial logic using three different consideration grading techniques referred to as Mask Attention (MA). Using such ratings, CTI would be used to choose terms within the border, and fully connected layer operations would be used to create the Power Sector characteristics. Eventually, the Power Sector functions are converted into TTP tags via a fully linked device.

The one-dimensional convent is necessary for the creation of n-gram sequences. The blending of the data can be accomplished using "this very same buffer," as explained in equation (7) and equation (8). Suppose that ej is the zero-padded vector from the initial text immersion field ej € e, ‖ using concatenation as the //concatenation activity and rounds as the divide technique. For a certain set of e j|i k/2 j i + k/2, the k-gram expression plot E k will be produced using the comparable values W k Rm and bases bk∈ Rm. E′ j would be loaded with m-dimensional blank vertices [0]m if j 1 or if j > n happens; else, ej e is going to be utilized. To minimize the measurement loss in specifically, the Wk. If k = 1, then is a unit matrix, and E1 = e.

$$e_j^{'} = \begin{cases} e_j \; if \; 1 \geq j \leq n \\ [0]^m \; else \end{cases} \qquad \textbf{(7)}$$

$$\mathrm{E_k} = \underset{i=1}{\overset{n}{\|}} \left(\underset{j=i-\;k\;//2}{\overset{i+k//2}{\|}} (e_j^{'}).w_k + \; b_k \right) \qquad \textbf{(8)}$$

The MP Mask serotype chooses the key supply chain and calculates its importance by range. The intersection of every one of the directions in $E_k^{\wedge} \in R^m$ is at EK Room equation (9). The WJ ∈ $R^{m\times 1}$ is the bias, and bj ∈ Rm is the vertical load. R is the exponent of the exact length $|E_{i,k}^{(j)} - E_k^{\wedge}|$, which has a quantity that should fall between (0 and + ∞).

The AR Mask subtype thinks about employing a precise ranged zone as its evaluation as opposed to the MP Mask. Rather, the sign is a region that has the greatest and least restriction of an $E_k^{\wedge}.E_k^{max} \in R^m$ center point equation (10). The largest restriction is $E_k^{min} \in R^m$, while the smallest is Wj ∈ $R^{m\times 1}$, bj ∈ R^m,$\lambda \in R$ and the same are identical to those in MP Mask equation (11).

$$S_{E_{i,k}}^{'} = \frac{In(s_{E_{i,k}}) - In\,(s_{E_k}^{(min)}}{In(s_{E_k}^{(max)} - In\,(s_{E_k}^{(min)})} \qquad \textbf{(9)}$$

$$w_l^{(\theta)} = \mathrm{Loc}\,(w_{(k),}\theta\,)$$

$$= \left\{ w_{(k)}^{(i)} \mid s_{E_{i,k}}^{'} \geq \theta, \; w_{(k)}^{(i)} \in w_{(k)} \right\} \qquad \textbf{(10)}$$

$$w_l^{(\theta)} = \cup_k w_{(k)}^{(\theta)} \qquad \textbf{(11)}$$

3.4. TTPs possibility prediction: Understanding the most important contextual features in the CTI is crucial for making predictions about TTPs. Math equation (12) enhances the impact that is most efficient $F_{E_{i,k}}$ following tests applying the activation function for softmax, from across all dimensions $E_{i,k} \in E_k$. The important scores, $s_{E_{i,k}} \in R$, are the name of the amplification product. The value rankings $S_{E_{i,k}} \in R^{n\times m}$ are then multiplied by each byte of a line $E_{i,k} \in E_k$ in equation (13) to create the veiled tensor $v_{e_k}^{(max)} \in R^{n\times m}$. Finally, using the universal Softmax function, Principal equation (14) chooses the scalar $v_{E_{i,k}} \in R^m$ with the greatest prominence out of all $v_{E_{i,k}}$.

$$s_{E_{i,k}} = softmax\,(F_{E_{i,k}}) = \frac{exp(F_{E_{i,k}})}{\sum_{j=1}^{n} exp(F_{E_{i,k}})} \qquad \textbf{(12)}$$

$$v_{E_{i,k}} = s_{E_{i,k}} \otimes E_{i,k} = \sum E_{i,k}^{(j)} \; . s_{E_{i,k}} | \; E_{i,k}^{(j)} \in E_{i,k} \qquad \textbf{(13)}$$

$$v_{E_k}^{(max)} = \underset{i\;=\;1}{\overset{n}{max}}\; (v_{E_{i,k}}) \qquad \textbf{(14)}$$

Equation (15) merges all of the k-gram impact verticals $v_{E_K}^{(max)}$ for the name classifiers to determine the end behaviour. Attribute $V_w \in R^{km-1}$. equation (16), which is the parabolic stimulation, $w_l \in R^{km\times|l|}$ is the tag loads, and b ∈ $R^{|l|}$ is the bias, illustrates the role of obtaining chances $p(l) \in R^{|l|\times 1}$ for labelling set l having attribute Vw.

$$v_w = \underset{k}{\|} v_{E_k}^{(max)} \qquad \textbf{(15)}$$

$$\mathrm{P(l)} = \sigma\,(v_w\, w \; + \; \mathrm{b})_l \qquad \textbf{(16)}$$

3.5. Extraction evaluation: There are two unique examinations that have been created for the search query testing equipment because there isn't a common response to the methods and vital information. First is Expert Assessment (EA), analyzing the relevance of terms created by humans and machines. One is called Confidence Assessment (CA), and it encloses the initial sequence using the significance of the items in reverse and discards useless data to assess the integrity of such brand conclusions such as-

3.5.1. *Expert assessment:* A dualistic reward is the EA. It forces a number of cyber security professionals to individually assess Power Sector and search result recovery using a single collection of test data. Although experts complete their sets solely depending on their own observations, Power Sector constructs the paragraph vocabulary set $w_{l,ts_i}^{(\theta)}$, $t_{s_i} \in TS$, TS by following the processes from the above equations. Calculating assessment scores from testing sets is demonstrated in

equation (17). Assuming that $A_{ts_i}^{\gamma}$ is the set of recovered key termsby γ-th expert, and wl_{ts_i} is the collection of strings power sector has collected. θ is the solution's designated barrier. Essentially, the assessment score is a resemblance factor.

$$\text{Score}\ (ts_i, \theta, \gamma) = f_s(A_{ts_i}^{\gamma}, w_{l,ts_i}^{(\theta)}) = \frac{|A_{ts_i}^{\gamma} \cap w_{l,ts_i}^{(\theta)}|}{|A_{ts_i}^{\gamma} \cup w_{l,ts_i}^{(\theta)}|} \quad \textbf{(17)}$$

This is specifically permitted to use text splitting to determine commonality. This is because important information that falls within a certain overall score can have its authenticity questioned, localised, and decided. For noun set A, for instance, we select concepts with relevance ratings between 90 and 100, but for term set B, we select vocabulary with significance values between 0 and 50. Power Sector can be regarded as being able to correctly state the importance if A's specialist level is much greater than B's. The very next accounting can be used to explain the aforementioned procedure. The concepts whose scores fall within [min, max] are represented in equation (18-19) and quotient is appropriate for this section of the core lexicon.

$$w_{l,ts,i}^{(\theta_{max} \to \theta_{min})} = w_{l,ts_i}^{(\theta_{max})} - w_{l,ts_i}^{(\theta_{min})} \quad \textbf{(18)}$$

$$\text{Score}\ (ts_i, \{\theta_{max}, \ \theta_{min}\}, \ \gamma) = f_s(A_{ts_i}^{\gamma}, w_{l,ts_i}^{(\theta_{max} \to \theta_{min})}) \quad \textbf{(19)}$$

3.5.2. *Confidence assessment (CA):* By obscuring the linguistic proof, CA seeks to ascertain whether categorizations are valid. It would be beneficial for CA if the relevant terms $w_l^{(\theta)}$ were eliminated equation(20). The letters w - $w_l^{(\theta)}$ through w and the remaining characters l are insufficient to provide a foundation for the designer's development. Whenever the dependent entropy H (l|w - $w_l^{(\theta)}$) equals the factor that gives H(l) of l, w - $w_l^{(\theta)}$ and TTPs labelled l, can be used to represent it statistically.

$$\text{CA}\ (\theta) : H(\ l|w - w_l^{(\theta)}) \to H\ (l) \quad \textbf{(20)}$$

3. Experiment

Experiments with Power Sector are carefully planned to achieve the two objectives of TTP isolation and classification. Inter- designation tests centered on techniques are used for categorization and methods using measures like Precise, Remember, and the F1 score. AntiMask eliminates every result. An example of font disguise via AntiMask is shown in Table 1. By assessing the framework indicated, the research studies for the applicability of keyword processing concentrate on the accuracy of the data. For the database, this article employs a tracker to capture more than 6500 examples of ATT&CK [49-52] V8 edition strategies and procedures from Mitre's online webpage (attack.mitre.org). The suggestions provided for the Mitre method T1548.002 are displayed in Table 2. The crew at Mitre has primarily completed the categorization tags for 12 strategies and 184 methods from the ATT&CK V8 edition. The key frames were created using a pre-trained FastText word net that was trained using 30 000 digital posts and cybersecurity-related stories.

The Drebin, TTPDrill, and rcATT datasets are chosen for further testing to show how the Power Sector can be used with little need for Power Sector. A resource for classifying mobile malware families is called the Drebin information. Its research is intended to demonstrate if Power Sector is capable of foreseeing application programming interfaces. Another ATT&CK test set is the TTPDrill dataset. Its test aims to determine whether Power Sector is reliable for multiple TTP datasets. The rcATT collection is a complete CTI database. This information will be used to test Power Sector ability to identify TTPs in lengthy and challenging articles.

Table 1: Comparison of relative percentages of AntiMask and Power Sector mask

information	the	Backdoor	registry	APT	gather	can	window	System	query	to	Power Sector mask
NULL	the	NULL	NULL	APT	NULL	can	window	system	query	to	AntiMaskText
0.989	02.4	84.9	1.38	94.95	9.23	82.4	47.4	9.48	855	94.2	$s(anti\ 1)$ $E_{i,k}$
0.09	0.0	27.48	0.5	0.378	0	477	0.0	0.47	93.4	0.0	$s(anti\ 2)$ $E_{i,k}$
578.0	3.29	94.0	8.29	0.374	0.0	73.2	47.5	2.38	9.3	0	s, $E_{i,k}$

Table 2: An illustration of a few of the explanations for T1548.002 provided by the Mitre AT&CK conceptual model official site

Technique	Bypass User Account Control T1548.002
Tech IDs	APT29: APT29 has bypassed UAC. APT37: APT37 has a function in the initial dropper to bypass Windows UAC in order to execute the next payload with higher privileges.
Group	Procedure Examples

A selection of the rcATT dataset [53] is made for further testing. A library for classifying mobile malware families is called the Drebin data frame. The research on it is intended to test Power Sector capacity to forecast application programming interfaces. Another source of ATT&CK information is the TTPDrill database. Its test seeks to determine when Power Sector is reliable for several TTP datasets. A complete CTI file is indeed the rcATT dataset. These datasets will be used to test Power Sector ability to identify TTPs in lengthy and challenging sentences. The records were also divided into the following partitions for the main TTP characterization trials in this document: 9:1, 8:2, 7:3, and 6:4. As indicated in Table 3, other files, with the exception of rcATT's collection for 9:1, were primarily broken down into testing and training groups based on the 6:4 ratio. Numerical values of different parameters are described in Table 4. The followings are all the comparison methods-

- POS: To assess how well the routine essential filtering techniques employed by ActionMiner, TTP-Drill, and EX-Action compare to Power Sector under multiple POS, SVO, and VO processing conditions.
- CNN: Using CNN, Yagcioglu finds cybersecurity-related happenings.
- Self-Attention (SelfATT): Yu uses CTI to pay attention to TTP categories.
- rcATT: SVM is used by rcATT as the ideal model for categorizing TTPs [54][55]. Given that the TF-IDF approach was to transform to ongoing sensory field feed SVM since the baseline rcATT will make the term table too big to master, the word wrapping with t-SNE is utilized.

Table 3: The number of lines in the ATT&CK and Drebin arrays learn and evaluation batches

Total Number	Number of the Sentences in Train sets	Test sets	Datasets
8568	3047	2037	rcATT
3873	2783	8824	Drebin
2394	3019	3028	ATT&CK
5244	4974	1028	TTPDrill

Table 4: Consistent mathematical model setups

Value	**Parameter**	**Value**	**Parameter**
482	N	248	m
0.3	Optimizer	Binary Cross entropy	Other epochs
95.3	Dense dims	Adam	Learning rate
10.38	Other loss	Bi-GRU	RNN dim
7.2-4	Framework	647,512	ATT dim
0.0002	λ in MP_Mask	0.4	λ in AR_Mask

≥ 392	Batch size	94-17	Dropout
1	Conv1D count	Tensorflow	Version
≥832	RNN type	Categorical Hinge	rcATT epochs

4. Result and Discussion

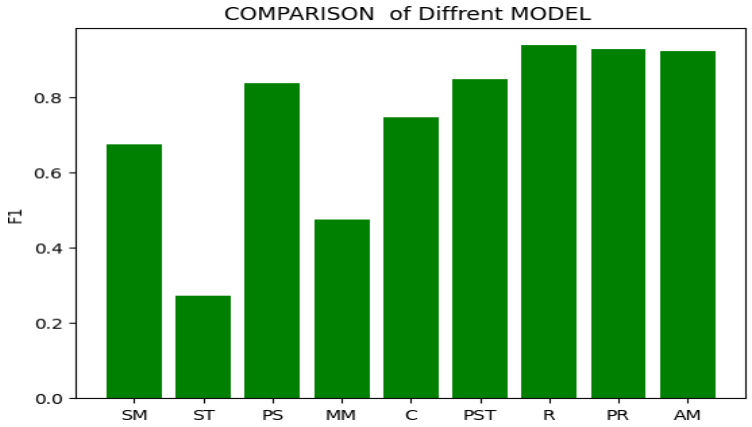
TTPs classification is considered as the outcomes of employing Power Sector as well as other approaches to the segmentation of techniques and strategies on the collection ATT&CK.1-k is the type multi-layer using many sheets with n-grams that range from 1 to k. The three different types of Power Sector masks are SV Mask, MP Mask and AR Mask. used to compare every plan using the most effective performance in taxonomies of tactics and approaches based on the quantity of factors and the speed of each phase. The predictor for structures that use POS computation uses the same layout and dimensions as models without POS handling. The results shown in Table 5 can be used to look at the following conclusions.

- MP Mask is more stable and doesn't require as much knowledge of n-grams to get the basic spread for tags that have different levels of abstraction.
- POS takes out words from sentences that don't mean anything special, which is the same as adding a lexical value screening where it's not needed yet, when producing Local SVO/VO sayings and POS can throw off the overall meaning of a sentence and make it less clear. This "cut-off" for the strategies makes sure that the regional content has the most descriptive power possible, which can be seen in how the RNN method has gotten better. POS may result in a lack of massive data for the implementation of methods.
- AR Mask performs worse in tag definitions than SV Mask, MP Mask when considering the spread of hashtags in hypercube. The outcomes confirm that "key terms reside distant from typical words", but they also demonstrate that taking delivery width and advised length into account can assist the system in locating essential elements.
- RNN handles the distillation of general knowledge, such as strategies, better than conventional techniques. On the other side, CNN and SelfATT are attentive to local approaches resembling logic. In TTP's classifications, Power Sector (mask) continues to hold a relative edge for both local and worldwide details.
- Even though SV Mask makes TTP recognition more accurate, a lot of its properties can be messed up by subjectivity. This also illustrates the difficult chasm between approaches and strategies.

Table 5: Outcomes of the evaluation of actions using multiple models

F1	Recall	Model
0.6746	0.9247	SV Mask (SM)
0.2738	0.9236	SelfATT (ST)
0.8378	0.9172	POS-CNN(PS)
0.4748	0.1273	MP Mask (MM)
0.4782	0.8646	CNN(C)
0.3718	0.3675	POS-self ATT(PST)
0.8138	0.8764	RNN (R)
0.9273	0.1938	POS-RNN(PR)
0.8399	0.9236	AR Mask (AM)

To find out how Power Sector works, more research was done on how the training collection and the test collection were split. The dataset was separated into testing and training sets for these studies in the9:1, 8:2, 7:3, and 6:4 are the ratios. Skill recognition is more impacted by information fusion than strategy. This can be seen in the increased deterioration of F1 skills.



Fige 2: the effectiveness of each model using various TTPs dataset segmentation for F1

Figure 2 shows how each model performed using various TTP information train and test ratios. The proportion of experimental and training units.

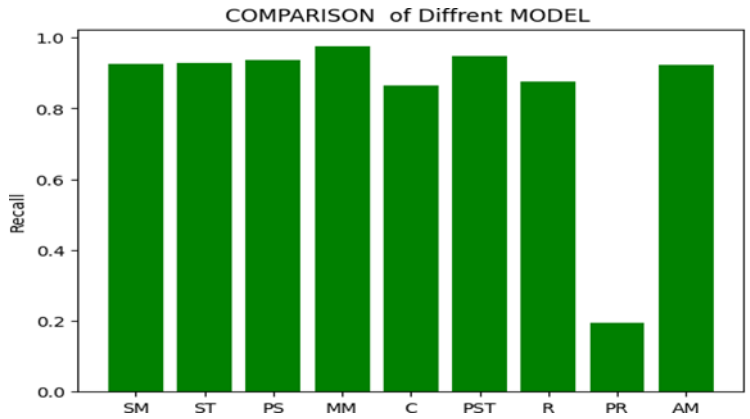


Fig 3: the effectiveness of each model using various TTPs dataset segmentation for Recall

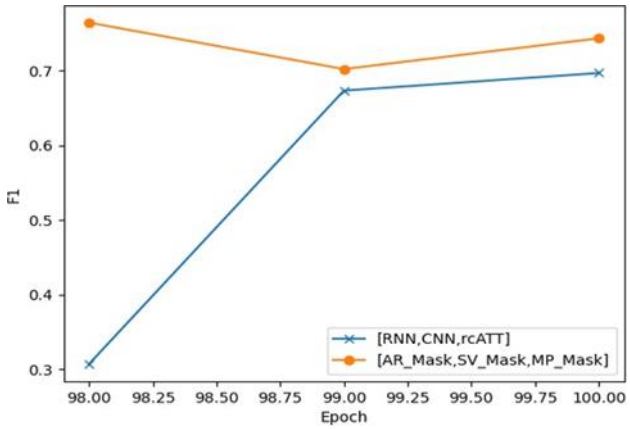


Fig 4: Comparison between power sector mask method and Deep learning for tactical model

Even though MP Mask runs more continuously in power sector, AR Mask still outperforms it at 6:4. Yet, given that the AR Mask is quite sensitive, Compared to AR Mask, MP Mask is much easier to employ when compared to n-grammes throughout mentoring. Figure 3 explains the Recall in respect of the effectiveness of each model against various TTPs data segmentation. Compared to conventional approaches, power sector mask TTP identification is much more precise Figure 4. Specifically, compared to other approaches, MP mask and AR mask are more secure.

5. Conclusion

To ensure consistency in the detection and extraction of this study suggests a multi-instance structure for TTPs for CTI known as Power Sector Mask Attention is used by the model to choose the by looking at the edge between keywords and regular words in the vector space, we can extract the basic meaning of a sentence. Then comes the Deep learning is a technique used to map the semantics of the tag text for TTP. The focus of the tests is on recognizing behaviour from statements in text form, large documents, And malware. The Four datasets were used in

the categorization experiments: tactics and methods, POS-CNN, SelfATT, CNN and RNN Power Sector Categorization F1 score minimum to maximum was 36.49 to 83.78%, 12.83 to 38.72,47.82 to 74.78, 81.31 to 93.83, which increased to comparing the values of 047%, 25.89%, 26.96%, and 12.52%, to many models. These outcomes not only show that the power sector can easily pull TTPs out of CTI text and show that power sector can handle the effects of a number of sources of illumination. This study discusses the extraction of crucial data from TTPs. employs expert judgment and confidence analysis to confirm the. It's important to note that neural networks are capable of using the anti-mask approach to find out why phrases are needed in a largely unsupervised environment Manner.

- Future research endeavors aim to combine AntiMask and Power Sector capabilities to further accomplish machine learning independence in determining whether data is crucial and how it can recognize actions.
- Implementation of Mask approach to the dataset which are significant for smart grid will also be explored in future.

References:

[1] Check Point Research (2023). Cyber attack trends: 2023 mid-year report. Check Point Software Technologies Ltd, San Carlos, California, USA. https://pages.checkpoint.com/cyber-attack-2022-trends.html.

[2] Bendovschi, A. (2015) Cyber-attacks - trends, patterns and security countermeasures. Procedia Economics and Finance, 28,24–31 7th International Conference on Financial Criminology 2015, 7th ICFC 2015, 13-14 April 2015,Wadham College,Oxford University, United Kingdom.

[3] Yu, Z., Wang, J., Tang, B. and Lu, L. (2022) Tactics and techniques classification in cyber threat intelligence. The Computer Journal, bxac048.

[4] Splunk (2022). State of observability 2022 report reveals organizations with mature observability practices significantly reduce costs while increasing innovation. Splunk Inc, San Francisco, USA. https://www.splunk.com/en_us/newsroom/press-releases/2022/state-of-observability-2022-report-revealsorganizations-with-mature-observability-practices-significantly -reduce-costs-while-increasing-innovation.html.

[5] Abu, M.S., Selamat, S.R., Ariffin, A. and Yusof, R. (2018) Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10, 371–379.

[6] Carvey, H. (2014) Follow up on TTPs post. http://windowsir. blogspot.com/2014/04/follow-up-on-ttps-post.html (accessed June 1, 2022).

[7] Maymí, F., Bixler, R., Jones, R. and Lathrop, S. (2017) Towards a definition of cyberspace tactics, techniques and procedures. In Jian-Yun Nie (ed), 2017 IEEE International Conference on Big Data (Big Data), pp. 4674–4679. IEEE, Boston, MA, USA.

[8] Bahrami, P.N., Dehghantanha, A., Dargahi, T., Parizi, R.M., Choo, K.-K.R. and Javadi, H.H. (2019) Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. Journal of information processing systems, 15, 865–889.

[9] Legoy, V., Caselli, M., Seifert, C. and Peter, A. (2020) Automated retrieval of att&ck tactics and techniques for cyber threat reports. arXiv preprint arXiv:2004.14322. Cornell University, Ithaca, New York, USA.

[10] You, Y., Jiang, J., Jiang, Z., Yang, P., Liu, B., Feng, H., Wang, X.and Li, N. (2022) Tim: threat context-enhanced ttp intelligence mining on unstructured threat data. Cybersecurity, 5, 1–17.

[11] Liu, C., Wang, J. and Chen, X. (2022) Threat intelligence att&ck extraction based on the attention transformer hierarchical recurrent neural network. Appl. Soft Comput., 122, 108826.

[12] Husari, G., Al-Shaer, E., Ahmed, M., Chu, B. and Niu, X. (2017) Ttpdrill: Automatic and accurate extraction of threat actions from unstructured text of cti sources. In David Balenson (ed) Proceedings of the 33rd annual computer security applications conference Orlando FL USA, 12, pp. 103–115. Association for Computing Machinery, New York, United States.

[13] Husari, G., Niu, X., Chu, B. and Al-Shaer, E. (2018) Using entropy and mutual information to extract threat actions from cyber threat intelligence. In Dongwon Lee (ed) 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (Vol. 11), pp. 1–6. IEEE, Miami, FL, USA.

[14] Zhang, H., Shen, G., Guo, C., Cui, Y. and Jiang, C. (2021) Exaction: Automatically extracting threat actions from cyber threat intelligence report based on multimodal learning. Security and Communication Networks, 2021, 1–12.

[15] Satvat, K., Gjomemo, R. and Venkatakrishnan, V. (2021) Extractor: Extracting attack behavior from threat reports. In Lujo Bauer (ed) 2021 IEEE European Symposium on Security and Privacy

(EuroS&P), pp. 598–615. IEEE, Vienna, Austria.

[16] Manning, C.D., Surdeanu, M., Bauer, J., Finkel, J.R., Bethard,S. and McClosky, D. (2014) The stanford corenlp natural language processing toolkit. In Kalina Bontcheva and Jingbo Zhu (eds) Proceedings of 52nd annual meeting of the association for computational linguistics: system demonstrations Baltimore, Maryland USA, 06, pp. 55–60. Association for Computational Linguistics, Baltimore, Maryland.

[17] Schmitt, X., Kubler, S., Robert, J., Papadakis, M. and LeTraon, Y. (2019) A replicable comparison study of ner software: Stanfordnlp, nltk, opennlp, spacy, gate. In Mohammad Alsmirat and Yaser Jararweh (eds) 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS),pp. 338–343. IEEE, Granada, Spain.

[18] Miller, G.A. (1995) Wordnet: A lexical database for english.Commun. ACM, 38, 39–41.

[19] Papagiannopoulou, E., Tsoumakas, G., and Papadopoulos, A.N. (2020) Keywords lie far from the mean of all words in local vector space. arXiv preprint arXiv:2008.09513. Cornell University, Ithaca, New York, USA.

[20] Zhou, Z. (2018) A brief introduction to weakly supervised learning. Natl. Sci. Rev., 5, 44–53.

[21] Mavroeidis, V. and Bromander, S. (2017) Cyber threat intelligence model: An evaluation of taxonomies, sharing standards,and ontologies within cyber threat intelligence. In Joel Brynielsson (ed) 2017 European Intelligence and Security Informatics Conference (EISIC), pp. 91–98. IEEE, Athens, Greece.

[22] Casey, T. (2007) Threat Agent Library Helps Identify Information Security Risks. Intel White Paper, Santa Clara, USA.

[23] Pham, V. and Dang, T. (2018) Cvexplorer: Multidimensional visualization for common vulnerabilities and exposures. In Naoki Abe, Huan Liu, Calton Pu, Xiaohua Hu, Nesreen Ahmed, Mu Qiao, Yang Song, Donald Kossmann, Bing Liu, Kisung Lee, Jiliang Tang, Jingrui He and Jeffrey Saltz (eds) 2018 IEEE International Conference on Big Data (Big Data), pp. 1296– 1301. IEEE, Seattle, WA, USA.

[24] Strom, E.B., Applebaum, A., Miller, P.D., Nickels, C.K., Pennington, G.A. and Thomas, B.C. (2018) Mitre ATT&CK™:Design and Philosophy. Mitre Corporation, Bedford, Massachusetts or McLean, Virginia.

[25] Nielsen, T.L., Abildskov, J., Harper, P.M., Papaeconomou, I. and Gani, R. (2001) The capec database. J. Chem. Eng. Data, 46, 1041–1044.

[26] Barnum, S. (2021) Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™). Mitre Corporation, Bedford, Massachusetts or McLean, Virginia.

[27] Grisham, J., Samtani, S., Patton, M. and Chen, H. (2017) Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence. In Xiaolong Zheng, Hui Zhang, Chunxiao Xing, G. Alan Wang, Lina Zhou and Bo Luo (eds) 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 13–18. IEEE, Beijing, China.

[28] Yagcioglu, S., Seyfioglu, M. S., Citamak, B., Bardak, B., Guldamlasioglu, S., Yuksel, A., and Tatli, E. I. (2019) Detecting cybersecurity events from noisy short text. arXiv preprint arXiv:1904.05054. Cornell University, Ithaca, New York, USA.

[29] Usman, N., Usman, S., Khan, F., Ahmad Jan, M., Sajid, A., Alazab, M. and Watters, P. (2021) Intelligent dynamic malware detection using machine learning in ip reputation for forensics data analytics. Future Generation Computer Systems, 118, 124–141.

[30] Sun, X., Wang, Z., Yang, J. and Liu, X. (2020) Deepdom: Malicious domain detection with scalable and heterogeneous graph convolutional networks. Comput. Secur., 99, 102057.

[31] AbdulNabi, I. and Yaseen, Q. (2021) Spam email detection using deep learning techniques. Procedia Computer Science,184, 853–858.

[32] Kim, G., Lee, C., Jo, J. and Lim, H. (2020) Automatic extraction of named entities of cyber threats using a deep bi-lstm-crf network. International journal of machine learning and cybernetics,11, 2341–2355.

[33] Arnold, N., Ebrahimi, M., Zhang, N., Lazarine, B., Patton, M. and Samtani, S. (2019) (2019) Dark-net ecosystem cyberthreat intelligence (cti) tool. IEEE International Conference on Intelligence and Security Informatics (ISI), 07, 92–97.

[34] Rastogi, N., Dutta, S., Zaki, M.J., Gittens, A. and Aggarwal,C. (2020) Malont: An ontology for malware threat intelligence. In Wang, G., Ciptadi, A., Ahmadzadeh, A. (eds) Deployable Machine Learning for Security Defense, Cham, pp. 28–44.Springer International Publishing, London, UK.

[35] Fujii, S., Kawaguchi, N., Shigemoto, T. and Yamauchi, T. (2022) Cyner: Information extraction from unstructured text of cti sources with noncontextual iocs. In Cheng, C.-M., Akiyama, M. (eds) Advances in Information and Computer Security, Cham, pp. 85–104. Springer International Publishing, London,UK.

[36] Yaman, E. and Krdzalic-Koric, K. (2019) Address entities extrac- ˇtion using named entity recognition. In Muhammad Younas,Irfan Awan and Filipe Portela (eds) 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 13–17. IEEE, Istanbul, Turkey.

[37] Bromander, S., Jøsang, A. and Eian, M. (2016) Semantic cyberthreat modelling. In Kathryn Blackmond Laskey, Ian Emmons, Paulo C.G. Costa, Alessandro Oltramari (eds) The 11th International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS 2016), Fairfax, Virginia Campus, USA, November 2016. 74–78.

[38] Milajerdi, S.M., Eshete, B., Gjomemo, R. and Venkatakrishnan,V. (2019) Poirot: Aligning attack behavior with kernel audit records for cyber threat hunting. In Lorenzo Cavallaro, Johannes Kinder (eds) Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security London, UK, CCS '19, pp. 1795–1812. Association for Computing Machinery, New York, US.

[39] Carvey, H. (2014). TTPs. http://windowsir.blogspot.com/2014/ 04/ttps.html (accessed June 1, 2022).

[40] Unfetter-Discover (2018). Unfetter insight. Github, https:// github.com/unfetter-discover/unfetter-insight.

[41] Niakanlahiji, A., Wei, J. and Chu, B.-T. (2018) A natural language processing based trend analysis of advanced persistent threat techniques. In Naoki Abe, Huan Liu, Calton Pu, Xiaohua Hu, Nesreen Ahmed, Mu Qiao, Yang Song, Donald Kossmann, Bing Liu, Kisung Lee, Jiliang Tang, Jingrui He and Jeffrey Saltz (eds) 2018 IEEE International Conference on Big Data (Big Data) (Vol. 12), pp. 2995–3000. IEEE, Seattle, WA,USA.

[42] Dietterich, T.G., Lathrop, R.H. and Lozano-Pérez, T. (1997) Solving the multiple instance problem with axis-parallel rectangles. Artificial Intelligence, 89, 31–71.

[43] He, W. and Wang, Y. (2009) Text representation and classification based on multi-instance learning. In LAN Hua (ed) 2009 International Conference on Management Science and Engineering, pp. 34–39. IEEE, Moscow, Russia.

[44] Bao, X., Liu, G., Yang, G. and Wang, S. (2020) Multiinstance multi-label text categorization algorithm based on multi-quadric function radial basis network model. In Zhang Jingzhong, WANG Jun (ed) 2020 3rd International Conference on Artificial Intelligence and Big Data (ICAIBD), pp.133–136. Sichuan Province Computer Federation, Chengdu,China.

[45] Joulin, A., Grave, E., Bojanowski, P. and Mikolov, T. (2017) Bag of tricks for efficient text classification. the. In Phil Blunsom,Alexander Koller (ed) 15th Conference of the European Chapter of the Association for Computational Linguistics (Vol. 01), pp.427–431. Association for Computational Linguistics, Valencia,Spain.

[46] Yacouby, R. and Axman, D. (2020) Probabilistic extension of precision, recall, and f1 score for more thorough evaluation of classification models. In Steffen Eger, Yang Gao, Maxime Peyrard, Wei Zhao and Eduard Hovy (eds) Proceedings of the First Workshop on Evaluation and Comparison of NLP Systems Online, 11, pp. 79–91. Association for Computational Linguistics, New York, US.

[47] Arp, D., Spreitzenbarth, M., Hübner, M., Gascon, H. and Rieck,K. (2014) Drebin: Effective and explainable detection of android malware in your pocket. Symposium on Network and Distributed System Security (NDSS), 02, 23–26.

[48] MLDroid (2017). Drebin/examples. Github Inc, San Francisco, California, US. https://github.com/MLDroid/drebin/tree/master/ src/Androguard/examples.

[49] MITRE, "Common Vulnerabilities and Exposures, Accessed on: 25th May 2023. Available: https://cve.mitre.org.

[50] MITRE, Common Weakness Enumeration, Accessed on: 28th May 2023. Available: https://cwe.mitre.org/about/index.html.

[51] MITRE, ATT&CK®, Accessed on: 28th May 2023. Available: https://attack.mitre.org/

[52] MITRE, Scoring CWEs, Accessed on: 29th May 2023. Available: https://cwe.mitre.org/scoring/index.html.

[53] KaiLiu-Leo (2020). Ttpdrill/all.csv. Github Inc, San Francisco, California, US. https://raw.githubusercontent.com/KaiLiu-Leo/ TTPDrill-0.5/master/ontology/examples/All.csv.

[54] Vlegoy (2020). rcatt/training_data_original.csv.

Github Inc, San Francisco, California, US. https://raw.githubusercontent.com/ vlegoy/rcATT/master/classification_tools/data/training_data_original.csv

[55] Mall, Pawan Kumar, et al. "Rank Based Two Stage Semi-Supervised Deep Learning Model for X-Ray Images Classification: AN APPROACH TOWARD TAGGING UNLABELED MEDICAL DATASET." Journal of Scientific & Industrial Research (JSIR) 82.08 (2023): 818-830

[56] kumar Mall, Pawan, et al. "Self-Attentive CNN+ BERT: An Approach for Analysis of Sentiment on Movie Reviews Using Word Embedding." International Journal of Intelligent Systems and Applications in Engineering 12.12s (2024): 612-62.

[57] Narayan, Vipul, et al. "7 Extracting business methodology: using artificial intelligence-based method." Semantic Intelligent Computing and Applications 16 (2023): 123.

[58] Narayan, Vipul, et al. "A Comprehensive Review of Various Approach for Medical Image Segmentation and Disease Prediction." Wireless Personal Communications 132.3 (2023): 1819-1848