Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021

Personality - Fractionalization of the Gloomy Net Extensively for Cybersecurity Condition Mentality

Shaik Heena[1], Shravya Chidurala[2], Dr. R. Saran Kumar [3], M. Rama[4], Shaik Asif [5]
[1, 3,4, 5] Department of Computer Science and Engineering,
[2] Software Engineer
[1,3,4,5] QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India
[2] Accenture
[1]heena.sk@qiscet.edu.in, [2]shravya.chidurala@accenture.com, [3]saran.r@qiscet.edu.in
[4]rama.m@qiscet.edu.in, [5]asif.sk@ qiscet.edu.in
Corresponding Author Mail: qispublications@qiscet.edu.in

Abstract— Recent years have seen an increase in the complexity of cyberespionage tactics. It is difficult to totally prevent intrusions, even when security measures are put in place. Another argument is that people can only actively combat online criminals. In order to deal with this situation, it is essential to foresee attacks and quickly implement the necessary defenses, which calls for expertise. The majority of malicious attackers frequently exchange information and resources that may be used to launch attacks on certain groups or on the darknet.Therefore, we assume that a large amount of knowledge, especially illicit knowledge, is available on the Internet. The assumption is that information security would be used to detect attacks in advance and build active protection. At present, unfortunately, this knowledge is retrieved only mechanically. To achieve this faster, we use machine learning (ML) to examine various darknet postings with the goal of finding online postings with threat data. We anticipate that in this way we will be able to discover threat information on the Internet in a reasonable time frame that will allow us to take the best proactive steps in advance.

Keywords— Cybersecurity condition mentality, gloomy Net, personality – fractionalization

I. INTRODUCTION

In recent years, cyber espionage tactics have gotten increasingly intricate. The majority of assaults in the past were carried out for personal benefit, but organized assaults for monetary gain are on the rise. The majority of assaults now target a single victim repeatedly with a predetermined objective, as opposed to the indiscriminate strikes of the past. Traditional spyware detection methods that rely on features are inadequate to catch all of the new ransom ware variants that are continuously emerging. Cyber espionage strategies have recently become increasingly complex. It is impossible to completely avoid intrusions, even if precautions are taken. In the past, attack targets were typically random, but today, tailored attacks that repeatedly target a single target have become the norm. Under current conditions, it is difficult to completely prevent all cyber-attacks, even with defensive measures in place. Based on these recent events, it is impossible to completely avoid all attacks, even when attack defenses are in place. Even if 99.9% of companies with very large networks

Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021

successfully fight cyber-attacks, the remaining 0.01% of breaches would cause great damage to the entire company. It can be argued that citizens can only fight cyber thieves on the attack. To cope with this scenario, it is crucial to anticipate intrusions and take appropriate countermeasures in time, which requires the use of analytics. Typically, numerous black-hat attackers share knowledge and tools on the dark net or in specialized groups that can be used for attacks, and we assume that there is a large amount of knowledge in cybercrime that includes these instances of illicit material. The use of security events should lead to early detection of attacks and the development of an unassailable shield. Unfortunately, this knowledge is currently being physically retrieved, and various scientific efforts are being made to make this more economical. The goal of this study is to more effectively gather security technologies by using ML and context2vec, an NLP approach. We gather information from blogs on the dark web that advocate for drastic action (hence they are called critical posts). We'll learn later that Black Hat thieves use the Dark net to exchange information regarding hacking techniques and the distribution of viruses. With the use of context2vec and ML, our objective is to swiftly identify such crucial material from the dark net pages. What the unflattering postings are related to depends on the chosen topics. Forum postings about virus offers, hacking strategies, payment information, and inciting attacks are some of our examples. In this study, we focus on collecting articles on the Internet related to ransom ware offers to illustrate the effectiveness of our proposed strategy. The goal of this project is to increase the productivity of intelligence-based penetration testing by developing a system to dynamically highlight relevant articles. The trend of using knowledge as an active defense against attacks is currently spreading, especially in industrialized nations, and some of them have achieved impressive success. However, the entire Internet has more than just postings that can be used as knowledge. There are many communications being sent out, including ones about drugs, pornography, chats, practical jokes, etc., and among them is information that may constitute espionage. The knowledge developed by the network administrator is both instantaneous and effective if an essential message can be rapidly recovered from the Black Web, which is made up of both helpful and worthless content. Knowledge takes time. We hope that the suggested technique will enable us to promptly and correctly acquire information on cybersecurity threat so that we can immediately implement the best defenses. Three chapters make up the remainder of this study: Similar works are summarized in Chapter II, and the suggested technique is described in Chapter III.The study is then the article is described in chapter IV and summarized in chapter V, which also deals with the future.

II. BACKGROUND

A. Related Works

Work has been intensely focused on correctly segmenting the information gathered on the Dark Web due to the sharp increase in theft and criminality, as outlined in Chapter 1. We'll talk about three ML experiments in this section. These investigations routinely reach an efficiency of approximately 80% while using a black box approach to gather classification findings. H. Chen et al. [1-3] make an effort to research dangerous posts in forums on the dark internet. They proposed a categorization algorithm for the content of dark websites. Their method analyses cyber newsgroups and identifies significant users using a collection of

Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021

features and ML techniques such as Support Vector Machine (SVM), appropriate statistical technologies Latent Dirichlet Allocation (LDA) and Recurrent Neural Networks (RNN). E. Nuns et al [4] reported studies in which they extracted messages from hidden Internet communities that could be relevant to attacks, such as personal data and cracking tactics. On the extracted data, they apply bag-of-words, which collects keywords present in a manuscript and uses the number of keywords as a feature. They use SVM and regression models to classify the subjects that succinctly summaries the information supplied. They suggested a method that combines supervised and semi-supervised training to locate web posts about intrusions in order to lower labelling costs and generate training instances. To extract spyware discussion threads from the dark net and identify the characteristics of distinct dark net websites and forums, M. Kadoguchi et al. [5] presented a work that combines natural language comprehension and machine learning. By quantizing statements of various sizes, their NLP study's context2vec method enables them to get a phrase consistency score from fragmented phrases. They created a classification model using the data gathered by doc2vec and a multilayer perceptron (MLP), a kind of NN. The classification was successful as a consequence, with an efficiency of 89.4%.

B. ML Techniques

In this part, we will go through each ML algorithm that we used in our technique. Our investigation focuses on dark net postings. Since they are textual inputs, NLP must be performed before they can be used as sources for the ML model. For NLP, we use contex2vec. The Bag-of-Words (Bow) method is now commonly used to quantize text. It is a text factorization approach that uses the occurrence of each term in the corpus as a feature. It identifies features by simply computing the frequency of occurrence of each phrase in the text. In other respects, this technique has the flaw that the signifier could be communicated since it does not include the environment in which it occurs. 2vec addresses this problem. Context2vec is an NLP approach developed by Tomas Mikolov [6], a former Google Inc. scientist] To group text, he uses an NN. As we will see in the following subsections, context2vec is a framework that takes into account the meaning of phrases. As a result, any phrase in the text that has a meaning can be vectored. The K-means technique is a grouping method. Segmentation is a kind of self-supervised training in which related information is classified into groups. There are two types of segmentation techniques: hierarchical and non-hierarchical. Hierarchical grouping is a process in which each piece of evidence is treated as a splitting criterion and groups with a small range are gradually merged. Non-hierarchical grouping, on the other hand, is a strategy in which the information is divided into a predefined number of nodes and the best splitting technique is searched We employ the second kind, non-hierarchical grouping, in our investigation. In K-means, the starting number of groups, k, is predefined, and the center of each group is randomly selected. Each piece of information is then assigned to the group with the closest distance (mean). The mean of the values in each group is then used to establish the new midpoint, and each piece of data is once more allocated to the group with the closest proximity. These steps continue until the mean of each group remains constant. Caron et al. [7] presented Deeply Grouping, a combination of a grouping algorithm and Convent (Convolutional). Information is initially routed through a convent in deep grouping to produce characteristics. K-means is then used

Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021

to modify the convolutional parameters by applying it to the features and utilizing the discovered groupings as dummy names. Self-supervised training can be accomplished by continuing this method.

III. PROPOSED METHODOLOGY

We talk about our suggested machine learning-based approach in this section for classifying the dark Internet according to cyber risk data.It is important to construct a specific model for each type of information to be retrieved using the proposed technique [5]. Once a model is created, the contributions that have been gathered must be gathered and categorized. Creating a model is expensive. First, elements of the study's suggested methodology are underlined. utilizing the method outlined in our prior work, are extracted by doc2vec from the gathered replies. The next machine learning technique is deep clustering, which combines auto-encoding with clustering. Grouping is applied to the characteristics that were obtained. Without assigning labels, the contributions were categorized and arranged within each cluster. The objective is to create a model that categorizes various contributions into distinct categories and labels them as vital or not. In this particular investigation, we aim to determine whether or not our approach can accurately classify the posts on the dark net. Regarding the experiment for our example in Chapter 4 of this research, we took forum talks concerning virus offerings. Key post, in the manner advised by our past work The following details each stage. of the proposed method.

A. Data Preparation

It's crucial to gather a lot of data for supervised learning or machine learning. The acquired data must then be classified as valid or wrong in order to provide training data. An automated web crawler with a focus on gathering information from the dark net is used to obtain the data. 850 forum posts were gathered. I utilized both as training examples in the experiment: posts concerning malware offerings and 850 other articles on unrelated subjects. The data was gathered using Six gill [8].

B. Feature Extraction and NLP

Since topic postings contain text, natural language processing must be done on the data before it can be fed into a machine learning algorithm. Additionally, the initial stage in machine learning is to extract characteristics that may be categorized. Language processing and pattern segmentation are two examples of how context2vec is used for natural outcomes. The term's notion as it is employed in various situations is represented by the extracted characteristics. To operate successfully, nap needs preprocessing. Document factorization and feature extraction parsing, cleaning and other techniques are used in our technique. Batch processing highlights the differences between the words. Everything not absolutely necessary is eliminated during the cleanup process, including digits and parentheses (). The text is normalized into upper- or lowercase letters.

Clustering in depth

Deep feature clustering is done after context2vec extracts the natural language and features. The auto-encoder is initially fed with the context2vec features. Using K-means, the encoder output from the auto-encoder is then categorized into clusters. We modify the auto-strengths

Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021

encoder's to provide the best clustering results, using the classification result as a pseudo-label for classification. It is not necessary to explicitly label the data because the K-means result is utilized as a pseudo-label. Based on the grouping outcome discovered after training, each cluster is categorized.

C. Classification of Unseen Data

As small datasets, we feed our model with the freshly collected black web content. To obtain the features, doc2vec performs natural language processing on the collected data, the features are then fed into the model and the collected postings are assigned to each group.

IV. EXPERIMENTS

The effectiveness of the advised strategy is examined in the trials that follow. This approach aims to extract particular articles on hackers. This is referred to as subject postings connected to malware offerings in the report. The study that was conducted there is described in TABLE I's environment section. 850 relevant data points were gathered for the investigation. Posts regarding virus offers and 850 other entries on unrelated subjects were used. Both of these were utilized as research information. Data were gathered using six gill. Six Gill is crucial since it helps to keep track of hacker activity on the dark web, social media, and other platforms and provides information about hierarchy. English-language subject entries were gathered. NLP and Feature Extraction Correct quantization requires first doing natural language handling pre-processing. Among the methods we employed were word normalization, text categorization, limitation, splitting, and cleaning. The result was a doc2vec model and raster texts. When learning, it's required for doc2vec. to put up hyper-parameters that are unknown. We determined that the sparsely was 200 for a total of 300 learning cycles.

A. Machine Learning

Context2vec's output from Deep clustering was utilized in conjunction with the clustering method. The auto-encoder and the K-mean approach, along with all other machine learning methods utilized in this research, are all included in the Python package Koras [9]. The software we created is built on the scripts that can be accessed at the following website [10]. A total of eight Means clusters were categorized. Pre-training epoch count is set to 128 and packet size is set to 256. Extensive testing has been done on the auto encoder’s hyper-parameters. The failure error function with a mean square was chosen. Figure 1 exhibits the auto-encoder setup along with the pre-training development, and Figure 2 presents the error function, which calculates the extent of the difference between the predicted and actual outcomes. The value is shown on Fig. 3's horizontal axis, and the label is shown on its vertical axis. Considering several clusters Deals with malware are indicated by the vertical scale label 1, whereas postings unrelated to malware offers are indicated by the label 0. Both forums are open for clusters 0 and 7. It is common to find blogs about virus offers and other subjects. On the other side, forum postings related to virus offers or other topics predominate in Clusters 1-6. every combination of groups.

B. Sorting out previously unknown data

Utilizing the developed model, we try to cluster unknown data. We attempt to cluster unknown data using the developed model. We utilized 170 instances of blogposts about malware offers and 170 examples of other blogposts not about malware offers from Six gill

Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021

as an unknown dataset. Figure 4 displays the classification's findings. Clusters 0 and 7 were given the bulk of the data since they had a lot of forum postings on malware-related ideas and several open positions throughout the training period. During the training period, Clusters 0 and 7 had access to a large number of malware-related forum posting ideas as well as certain other activities, thus they received the majority of the information.

TABLE I. **SETTINGS OF OUR SYSTEM**

Feature	**Configuration**
Kernel	4.1.0 Coding Platform
Machine	3.0 GHz Intel Core i5
Storage	32 GB
Coding Platform	OS X EI Capitan Ver.10.11.8
Settings	Pharm

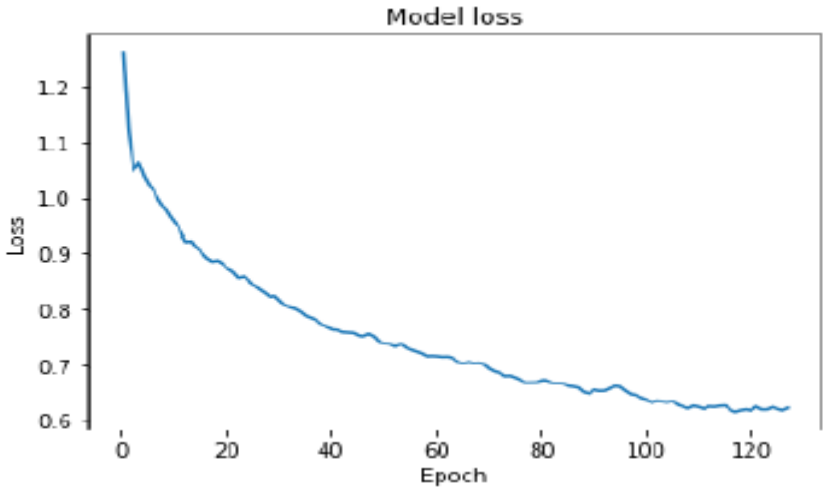


Fig. 1. Model pre-training loss

Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021

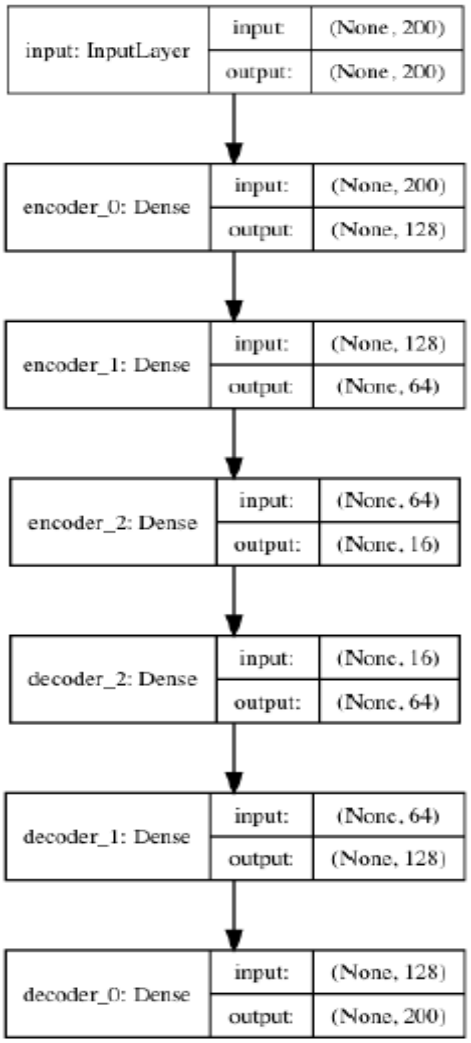


Fig. 2. Configuration autoencoder

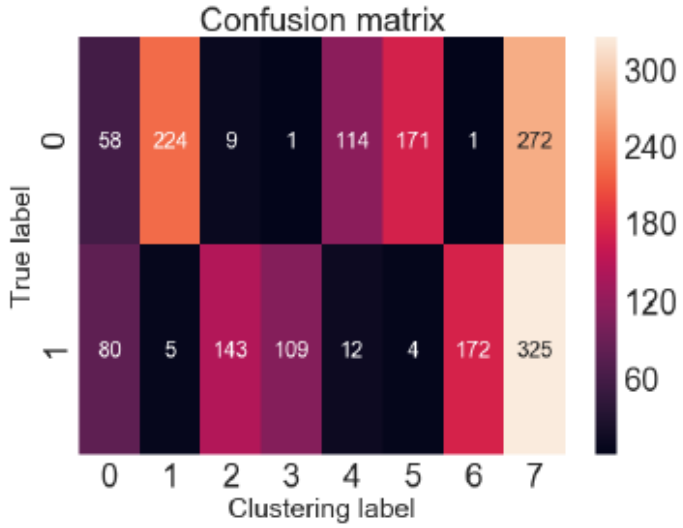


Fig. 3. Classification result of deep clustering

Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021

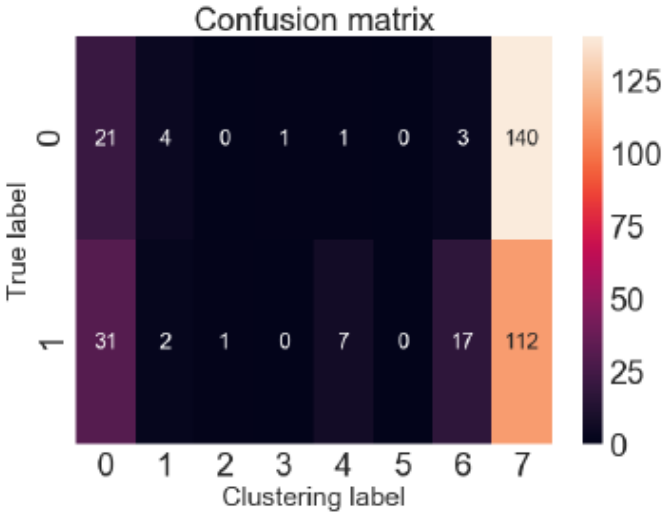
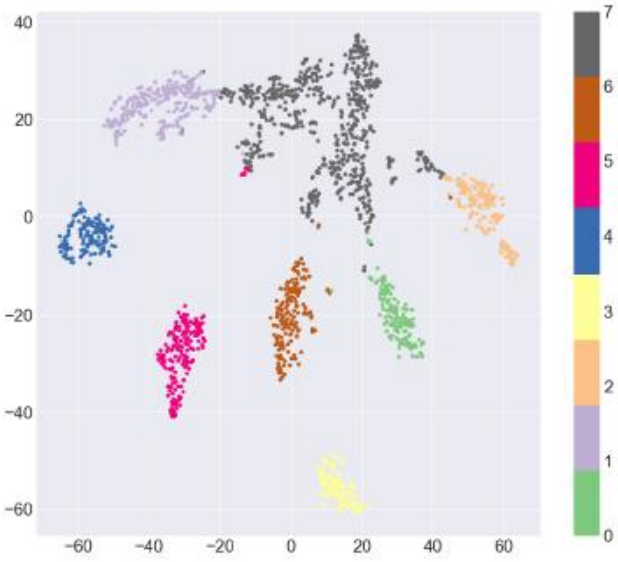


Fig. 4. Clustering result of unseen data

V. DISCUSSION

During the cognitive exercise of this approach, six of the eight categories were clearly separated into forums tied to malware offerings and various other postings. On the opposite side, the two discussion threads were combined to create the two extra sets. These two cells were in charge of 733 posts out of the 1700, or over 43% of all posts. 967 of the 1700 responses—or around 57% of all the articles—were distributed to the six remaining groups. We judge two groups to be category failures because they combine content about malware and other topics. However, even with soul knowledge, the remaining 57% of posts were correctly categorized, for a total of about 97 percent. Using the t-distributed Probabilistic Neighborhood Extrusion (t-SNE) approach, the fields are reduced across 2 components to examine. Even while deep learning alone cannot yet accurately categories any forums, we demonstrated that it is feasible to boost the productivity of extracting critical messages. However, about 89 data sets have been classified. This feature could increase the quantity of data. The size and substance of the training and testing datasets have an impact on the results of deep learning. In this test, our algorithm was still unable to distinguish between groups that had a mixture of infection pitches and other postings based on their attributes. We think we may identify the variations in such groups' attributes by improving the quantity and quality of data. Multiple aspect changes can also be thought of as a development strategy. Various elements were investigated.

Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021



VI. Training model T-sne outcome

VII. CONCLUSION

The study's summary and potential issues are covered in this section.

A. Summary

B. In this work, learning algorithms were employed to accurately gather threat detection from the dark net as a defense against attacks. We offered a method for gathering items from ominous discussion forums and classifying them using strong grouping as vital or quasi. The project's objective was to categories messages without explicitly tagging the content. During the testing round, almost 57% of the forums were accurately recognized with astounding precision. However, after the assessment of the unknown facts, almost 89 percent of the posts were given to groups that are neither urgent nor quasi. We believe that by addressing the concerns mentioned in the following sections, organizing the dark web for cybersecurity using algorithms will be a valuable technique. We anticipate that our

C. Future Challenges

We have noted the four problems listed below. The first problem was the amount of data that the algorithms were using. In computer science, academic quality is directly connected to the volume of data or its subjects. It is essential to gather the right degree of data based on the content that has to be categorized. The type of information that has to be gathered must also be taken into account, as must the question of whether it can be done so given the large volume of data available on the dark net. The second requirement is that different milliliter parameters must be modifiable. The optimal conditions for this study were carefully selected through conjecture. On the other hand, when the variety and volume of information increase, updating the highest accuracy architecture and centroids requires a lot of care. Therefore, a method for manually finding the important criteria based on the categorization of the data is needed. Third, although we restricted our analysis to discussion threads concerning Trojan offers, our long-term goal is to utilize a similar technique to classify various kinds of crucial forums. Ultimately, we must consider viral offers, as well as other articles like hacking techniques, the trafficking of payment information, and encouragement of attacks, as vital articles, as well as evaluate and categories data. Finally, these four procedures—text analysis

Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021

and feature identification (doc2vec), algorithms, and classification of data—are often carried out.

REFERENCES

[1] H. Chen, (2008). " IEDs in the dark web: genre

[2] improvised explosive device web pages, " 2008 IEEE Int. Conf. on Intelligence and Security Informatics, Taipei, Taiwan, 2008, pp. 94 – 97, doi:10.1109/ISI.2008.4565036., in press.

[3] H. Chen,"IEDs in the dark web: Lexicon expansion and genre classification,"2009 IEEE Int. Conf. on Intelligence and Security Informatics, Dallas, TX, 2009, pp. 173-175, doi: 10.1109/ISI.2009.5137293. , in press.

[4] S. Huang and H. Chen, "Exploring the online underground marketplaces through topic-based social network and clustering," 2016 IEEE Conf. on Intelligence and Security Informatics (ISI), Tucson, AZ, 2016, pp. 145- 150, doi: 10.1109/ISI.2016.774545. , in press.

[5] E. Nunes et al., "Darknet and deepnet mining for proactive cybersecurity threat intelligence," 2016 IEEE Conf. on Intelligence and Security Informatics (ISI), Tucson, AZ, 2016, pp. 7-12, doi: 10.1109/ISI.2016.7745435. , in press.

[6] M. Kadoguchi, S. Hayashi, M. Hashimoto and A. Otsuka, (2019) "Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning," 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 2019, pp. 200–202, doi: 10.1109/ISI.2019.8823360.

[7] Mikolov Tomas, Sutskever Ilya, Chen Kai, Corrado, Greg, and Dean, Jeffrey, "Distributed representations of phrases and their compositionality", In Advances on Neural Information Processing Systems, 2013J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[8] Mathilde Caron, Piotr Bojanowski, Armand Joulin, Matthijs Douze; The European Conference on Computer Vision (ECCV), 2018, pp. 132- 149.K. Elissa, "Title of paper if known," unpublished.

[9] Sixgill, https://www.cybersixgill.com/, (accessed Aug. 15, 2020).

[10] Keras Documentation, https://keras.io/ja/, (accessed Aug. 15, 2020).

[11] How to do Unsupervised Clustering with Keras, https://www.dlology.com/blog/how-to-do-unsupervised-clusteringwith-keras/M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[12] O'Hear, Steve. "Sixgill claims to crawl the Dark Web to detect future cybercrime". TechCrunch. Retrieved 2018-02-01.

[13] . Jump up to:a b Weinglass, Simona (August 12, 2015). "Ex-Israeli agents want to shine a flashlight on the dark web". The Times of Israel. Retrieved 2018-02-01.

[14] Jump up to:a b Boyer, Sam. "Cyber intelligence company trawling Dark Web to foil impending cyberattacks on clients". Insurance Business. Retrieved 2018-02-01.

[15] "Israeli cyber security co Sixgill raises $5m - Globes English". Globes.

[16] "¿Iniciará Corea del Norte una guerra cibernética?". CNN (in European Spanish). 2017-11-17. Retrieved 2018-02-01.

[17] "Israeli startups have raised $561 million in June – so far".

[18] "Sixgill Named a "Cool Vendor" by Gartner". finance.yahoo.com. etrieved 2019-06-28.^ "CNC Intelligence". cncintel.com. Retrieved 2021-0

[19] Jump up to:a b "Sixgill's new cyber threat intelligence platform is tailored to meet the needs of MSSPs". Help Net Security. 2019-06-04. Retrieved 2019-06-.

[20] Mackie, Thomas (30 October 2017). "'He's a CHILD!' Britain FURIOUS as ISIS 'threatens to KILL Prince George at school'".

Article Received: 05 September 2021, Revised: 09 October 2021, Accepted: 22 November 2021, Publication: 26 December 2021
[21] Binding, Lucia (29 October 2017). "Isis pledge sickening threat to kill Prince George at school".
[22] "How children playing Fortnite are helping to fuel organised crime". The Independent. 2019-01-13. Retrieved 2019-06-28.
[23] Crecente, Brian (2019-01-15). "Dark Web Creating 'Thriving Criminal Eco-System' Around Game". Variety. Retrieved 2019-06-28.
[24] 24. "Epic's battle royale game Fortnite used to launder money". IT PRO. Retrieved 2019-06-28.
[25] "Israeli cyber security sartup Sixgill raises $5 million to crawl the Dark Web for cyber crime - Jewish Business News". 16 June 2016.
[26] P Ramprakash, M Sakthivadivel, N Krishnaraj, J Ramprasath. ”Host-based Intrusion Detection System using Sequence of System Calls” International Journal of Engineering and Management Research, Vandana Publications, Volume 4, Issue 2, 241-247, 2014
[27] N Krishnaraj, S Smys.”A multihoming ACO-MDV routing for maximum power efficiency in an IoT environment” Wireless Personal Communications 109 (1), 243-256, 2019.
[28] N Krishnaraj, R Bhuvanesh Kumar, D Rajeshwar, T Sanjay Kumar, Implementation of energy aware modified distance vector routing protocol for energy efficiency in wireless sensor networks, 2020 International Conference on Inventive Computation Technologies (ICICT),201-204
[29] Ibrahim, S. Jafar Ali, and M. Thangamani. "Enhanced singular value decomposition for prediction of drugs and diseases with hepatocellular carcinoma based on multi-source bat algorithm based random walk." Measurement 141 (2019): 176-183. https://doi.org/10.1016/j.measurement.2019.02.056
[30] Ibrahim, Jafar Ali S., S. Rajasekar, Varsha, M. Karunakaran, K. Kasirajan, Kalyan NS Chakravarthy, V. Kumar, and K. J. Kaur. "Recent advances in performance and effect of Zr doping with ZnO thin film sensor in ammonia vapour sensing." GLOBAL NEST JOURNAL 23, no. 4 (2021): 526-531. https://doi.org/10.30955/gnj.004020 , https://journal.gnest.org/publication/gnest_04020
[31] N.S. Kalyan Chakravarthy, B. Karthikeyan, K. Alhaf Malik, D.Bujji Babbu,. K. Nithya S.Jafar Ali Ibrahim , Survey of Cooperative Routing Algorithms in Wireless Sensor Networks, Journal of Annals of the Romanian Society for Cell Biology ,5316-5320, 2021
[32] Rajmohan, G, Chinnappan, CV, John William, AD, Chandrakrishan Balakrishnan, S, Anand Muthu, B, Manogaran, G. Revamping land coverage analysis using aerial satellite image mapping. Trans Emerging Tel Tech. 2021; 32:e3927. https://doi.org/10.1002/ett.3927
[33] Vignesh, C.C., Sivaparthipan, C.B., Daniel, J.A. et al. Adjacent Node based Energetic Association Factor Routing Protocol in Wireless Sensor Networks. Wireless Pers Commun 119, 3255–3270 (2021). https://doi.org/10.1007/s11277-021-08397-0.
[34] 9. C Chandru Vignesh, S Karthik, Predicting the position of adjacent nodes with QoS in mobile ad hoc networks, Journal of Multimedia Tools and Applications, Springer US,Vol 79, 8445-8457,2020