Journal of Technology and Informatics (JoTI)
Vol. 6, No. 1, October 2024
P-ISSN 2721-4842
E-ISSN 2686-6102 DOI: 10.37802/joti.v6i1.679

Machine Learning Approach for Classification of Cyber Threats Actors in Web Region

Anthony Edet[1], Saviour Inyang[2], Imeh Umoren[3], Ubong E. Etuk[4]
[1,2,3,] Department of Computer Science, Akwa Ibom State University, Mkpat Enin, Nigeria.
[4]School of Computing Science, University of Glasgow, Glasgow G12 8QQ, UK.
anthonyedet73@gmail.com[1], sinyang5672@gmail.com[2], imehumoren@aksu.edu.ng[3], u.etuk.1@research.gla.ac.uk[4]
* Corresponding author: E-mail: anthonyedet73@gmail.com

Abstract: *In the interconnected scape of today's internet, the dark web emerges as a concealed point, covering a myriad of illicit activities that pose substantial cybersecurity risks. This study investigates the attribution of threats within the dark web environment, leveraging on a machine learning approach to bridge the gap between technical indicators and linguistic and behavioral insights. Through a comprehensive methodology involving web crawling and data gathering, a dataset encompassing key variables such as attack motivation, method, web part, and threat actor was gathered. Principal Component Analysis was employed for feature selection, followed by the application of Multinomial Naive Bayes (MNB), Support Vector Machine (SVM), Random Forest (RF), and CatBoost algorithms for classification. Performance evaluation metrics including precision, recall, and F1-score were utilized to assess the efficacy of each algorithm. Results indicate a notable prevalence of cybercrimes within the dark web, underscoring the necessity for enhanced cybersecurity strategies tailored to address its unique challenges. Furthermore, the comparative analysis demonstrates varying performance levels among the machine learning algorithms, with Multinomial Naive Bayes exhibiting the highest accuracy. This research contributes to advancing threat attribution techniques in the dark web, ultimately aiming to bolster cybersecurity defenses and mitigate future cyber threats.*

Keywords*: Threats;; Cybersecurity; Attribution; Machine Learning*

INTRODUCTION

In today's interconnected world, the dark web stands as a shadowy underbody of the internet, harboring an array of illicit activities that pose significant threats to cybersecurity. The dark web refers to the hidden, encrypted part of the internet that is not indexed by traditional search engines [1]. It is often associated with illegal and illicit activities due to its anonymity and privacy features, making it a breeding ground for cybercriminals. It has become a hub for cybercriminals, offering a haven for activities such as the sale of stolen data, hacking tools [2], illegal substances, and the organization of cyberattacks for financial gain, political motives [3], or other nefarious purposes. The anonymity and encrypted communication channels prevalent on the dark web make it exceptionally challenging to track, identify, and attribute these threats to specific actors or groups [4]. The dark web's elusive nature is compounded by the use of sophisticated complication techniques and the constant adaptation of its users to evade detection [5].

Nevertheless, traditional cybersecurity methods often rely on technical indicators such as IP addresses, malware signatures, and known vulnerabilities for threat identification [6]. These indicators, while valuable, often fall short in providing a complete picture of the threat layout and a target response, as they can be easily manipulated, concealed, or shared among different actors [7]. A targeted response in cybersecurity refers to a specific and tailored action taken to defend against or mitigate a cyber threat [8]. It is based on the attributes and motivations of the threat actor, as well as the insights obtained through threat attribution. Targeted responses can include legal actions [9], enhanced monitoring [10], and customized cybersecurity measures designed to counter the specific tactics used by the threat actor [11]. In response to this evolving cyberspace, the need for a comprehensive cybersecurity system that efficiently maps dark web activities to known threat actors has become increasingly urgent [12]. Therefore, Threat attribution involves the process of determining the origins and identities of cyber threats and threat actors which is paramount for understanding, capabilities, and modus operandi of threat actors [13], such as the source or origin of a cyber threat and identifying the individuals, groups, responsible for a cyberattack or other malicious activities [14]. Accurate threat attribution is critical for developing effective cybersecurity responses [15]. This understanding is essential for devising effective countermeasures, enhancing cybersecurity postures, and safeguarding against future attacks. [16].

Consequently, attributing cyber threats is a great challenge. It requires a combination of technological involvement [17], human intelligence, and cybersecurity expertise [18]. The traditional emphasis on technical indicators, while valuable, is only one piece of the puzzle. Hence, a more comprehensive approach must also account for the linguistic and behavioral aspects of threat actors, as well as the broader contextual information that can be assembled from dark web forums, marketplaces, and chat rooms through dark web crawling and other means [19]. On this note this study proposed a solution to meet the challenge of threat attribution in the dark web environment using Machine learning Approach [20]. Adopting Machine learning techniques will help bridge the gap between technical indicators [21] and linguistic and behavioral insights. By doing so, it seeks to enhance the efficiency and accuracy of the threat attribution process, ultimately leading to more effective and targeted responses.

METHOD

In this study, the method adopted in this research is based framework-based method [22] which is presented in figure 1 which serves as a workflow diagram in the method in this study.

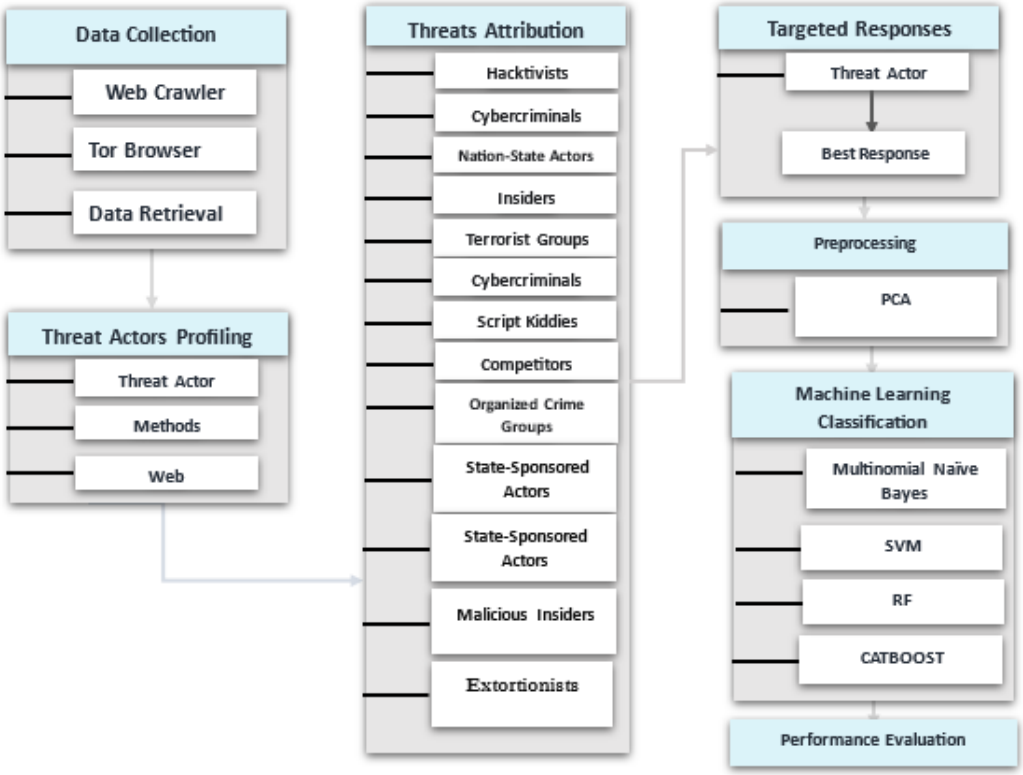

Figure 1: Workflow for Classification of Cyber Threats

A. Data Collection

In this section, the data gathering process is describe as follows;

i. **Web Crawler Tool:** To systematically traverse the Dark Web and collect relevant data for this study, a specialized web crawler tool scrapy based on python was employed. This tool is aiding the navigation through the dark web sites, extracting pertinent information related to cyber threats and their associated actors.

ii. **Tor Browser**: Access to the Dark Web was facilitated through the Tor browser, which ensures anonymity and secure data retrieval. The Tor browser enables the web crawler tool to operate within the Dark Web environment without compromising the security and privacy of the data collection process.

Data Retrieval: This process involved extracting detailed information about threats, threat actors, and their methodologies from the Dark Web. This information includes identities, motivations, capabilities, affiliations, and records of previous cyberattacks. The retrieval process was automated to handle the vast amount of data available on the Dark Web. A total of 10002 dataset was scrabe from the dark web using Scrapy tool which was process and use in the machine learning section of this study for classification of threat actors.

B. Threat Actors Profiling

This involves creating comprehensive profiles of the threat actors found on the dark web. These profiles should include information such as their identities, motivations, capabilities, affiliations, previous cyberattacks, and other relevant details. The aim is to build a clear picture of who these individuals or groups are. Table 1 shows the comprehensive profile of dark web threat actors:

Table 1: Threat Actors, Motivation, Methods and Web

Threat Actor	Motivation	Methods	Web
Hacktivists	Activism	Disruption	Surface Web
Cybercriminals	Financial gain	Malware attacks	Dark Web
Nation-State Actors	Espionage	APTs	Surface Web
Insiders	Malicious intent	Unauthorized access	Surface Web
Terrorist Groups	Disruption	Cyber-terrorism	Surface Web
Script Kiddies	Thrill-seeking	Exploits	Surface Web
Competitors	Corporate espionage	IP theft	Dark Web
Organized Crime Groups	Financial gain	Ransomware	Dark Web

State-Sponsored Actors	Geopolitical influence	Cyber-espionage	Surface Web
Malicious Insiders	Revenge	Data theft	Surface Web
Extortionist	Financial gain	Ransomware	Dark Web
Hacktivist Groups	Activism	Coordinated cyber campaigns	Surface Web
APT Groups	Long-term cyber-espionage	Highly sophisticated attacks	Surface Web
Rogue Employees	Internal dissatisfaction	Exploiting internal access	Surface Web
Data Brokers	Profit from selling stolen data	Acquiring and selling data on the dark web	Dark Web
Hacktivist Collectives	Collective activism	Coordinated cyber campaigns	Surface Web
Mercenary Hackers	Hired for cyber-attacks	Carrying out attacks for others	Dark Web

C. Threat Attribution

Accurate threat attribution is crucial in cybersecurity because it enables organizations, law enforcement, and cybersecurity professionals to understand who is behind an attack. This knowledge is essential for taking appropriate countermeasures, including legal action, if necessary. Here we map each threat in the dark web against an actor to clearly model the best response. It is a combination of the threat actors profile and threats carried out by them. Below is the threat attribution list:

Hacktivists: Malware, Phishing, Denial of Service (DoS) Attack, Distributed Denial of Service (DDoS) Attack, Social Engineering, Form Spoofing, DNS Hijacking, Clickjacking, Hijacking Clicks, Click Fraud

Cybercriminals: Malware, Phishing, Denial of Service (DoS) Attack, Distributed Denial of Service (DDoS) Attack, Man-in-the-Middle (MitM) Attack, SQL Injection, Cross-Site Scripting (XSS), Zero-Day Exploits, Ransomware, Credential Stuffing, Fileless Malware, IoT-Based Attacks, Supply Chain Attacks, Crypto-Malware

Nation-State Actors: Advanced Persistent Threats (APTs), Cyber-espionage, Zero-Day Exploits, Social Engineering, DNS Hijacking, Clickjacking, Watering Hole Attack, Eavesdropping, USB-Based Threats, SIM Card Swapping, Macro-Based Malware, DNS Tunneling.

Insiders: Unauthorized access, Data theft, Sabotage, Social Engineering, Insider Threats, Clipboard Hijacking, File Upload Vulnerabilities, Cross-Site Request Forgery (CSRF), Session Hijacking, Formless Attack

Terrorist Groups: Cyber-terrorism, Phishing, Exploits, Social Engineering, Denial of Service (DoS) Attack, Distributed Denial of Service (DDoS) Attack, Form Spoofing, Clickjacking, Hijacking Clicks, File Upload Vulnerabilities, HTTP Request Smuggling, Fileless Malware, AI-Powered Attacks, ATM Skimming, Formless Attack, Evil Twin Wi-Fi Attack, Juice Jacking, Hijacking Clicks, Shadow IT, Honeypot Attacks, Distributed.

Script Kiddies: Exploits, Malware attacks, Denial of Service (DoS) Attack, Phishing, Social Engineering, Ransomware, File Upload Vulnerabilities, Clickjacking, DNS Tunneling, Formless Attack, Click Fraud

Competitors: IP theft, Phishing, Ransomware, Social Engineering, Form Spoofing, DNS Hijacking, Clickjacking, Watering Hole Attack, USB-Based Threats, Macro-Based Malware, DNS Tunneling, File-Extension Spoofing

Organized Crime Groups: Ransomware, Malware attacks, Data Exfiltration, Social Engineering, Phishing, Denial of Service (DoS) Attack, Distributed Denial of Service (DDoS) Attack, Formjacking, Bluejacking, Whaling, Clickjacking, Watering Hole Attack, Eavesdropping, USB-Based Threats, SIM Card Swapping, Macro-Based Malware, Brute Force Attacks, File Upload Vulnerabilities, Cross-Site Request Forgery (CSRF), Crypto-Malware.

State-Sponsored Actors: Advanced Persistent Threats (APTs), Cyber-espionage, Zero-Day Exploits, Social Engineering, DNS Hijacking, Clickjacking, Watering Hole Attack, Eavesdropping, USB-Based Threats, SIM Card Swapping, Macro-Based Malware, DNS Tunneling, AI-Powered Attacks, EternalBlue Exploit, Formless Attack, Smart Contract Exploits, AI-Enhanced Social Engineering, Packet Sniffing, Backdoor Exploits

Malicious Insiders: Unauthorized access, Data theft, Sabotage, Social Engineering, Insider Threats, Clipboard Hijacking, File Upload Vulnerabilities, Cross-Site Request Forgery (CSRF), Session Hijacking, Formless Attack

Extortionists: Ransomware, Denial of Service (DoS) Attack, Phishing, Social Engineering, Form Spoofing, DNS Hijacking, Clickjacking, Watering Hole Attack, USB-Based Threats, Macro-Based Malware, DNS Tunneling, File-Extension Spoof.

D. Targeted Response

Once the dark web activities have been linked to known threat actors or campaigns and detailed profiles are constructed, organizations can develop more effective and targeted response strategies. This might involve enhancing cybersecurity defenses, sharing threat intelligence with other organizations or authorities, or taking legal action against the threat actors. In this work, responses have equally been matched against individual threat and actors to facilitate targeted response. This study presents the targeted response in table 2.

Table 2: Targeted responses

Threat Actor	Best Responses
Hacktivists	Enhance cybersecurity measures, monitor for DDoS attacks, educate users on phishing prevention.
Cybercriminals	Employ robust antivirus software, conduct regular security audits, implement intrusion detection systems.
Nation-State Actors	Invest in advanced threat intelligence, use network segmentation, conduct regular security assessments.
Insiders	Implement least privilege access, conduct thorough background checks, monitor user activities.
Terrorist Groups	Strengthen cybersecurity infrastructure, collaborate with law enforcement agencies, monitor for unusual activities.
Script Kiddies	Educate users on basic cybersecurity, implement intrusion detection systems, enforce strong password policies.
Competitors	Secure intellectual property, use encryption for sensitive data, conduct regular security training.
Organized Crime Groups	Implement advanced threat detection, conduct penetration testing, secure critical data with encryption.
State-Sponsored Actors	Implement advanced threat intelligence, use network segmentation, conduct regular security assessments.
Malicious Insiders	Implement least privilege access, conduct thorough background checks, monitor user activities.
Extortionists	Regularly backup critical data, use endpoint protection, educate users on phishing prevention.
Hacktivist Groups	Enhance cybersecurity measures, monitor for DDoS attacks, educate users on phishing prevention.
APT Groups	Invest in advanced threat intelligence, use network segmentation, conduct regular security assessments.
Rogue Employees	Implement least privilege access, conduct thorough background checks, monitor user activities.
Data Brokers	Encrypt sensitive data, implement secure data sharing practices, conduct regular security audits.
Hacktivist Collectives	Enhance cybersecurity measures, monitor for DDoS attacks, educate users on phishing prevention.
Mercenary Hackers	Employ advanced threat detection tools, use network segmentation, conduct regular security assessments.

E. Data Collection

This study delves into the profiling of Darkweb threat actors and the attribution of threats to known actors on the surface web. To achieve this objective, a web crawler tool was employed to systematically traverse the Darkweb, gathering specific data features and values. Access to the Darkweb was facilitated through the Tor browser, enabling the retrieval of information pertaining to threats, threat actors, and attack methodologies, which was then stored in a CSV format for subsequent machine learning analysis. Hence, the cross-sectional of the data set gathered figure 2.

INPUT VARIABLES			OUTCOME (CLASS VARIABLE)
attack_motivation	attack_method	web_part	threat_actor
Ransomware	Malware	Surface Web	Mercenary Hackers
Political Ideology	Advanced Persistent Thr	Surface Web	Hacktivist Groups
Financial Gain	Ransomware	Dark Web	Organized Crime Groups
Financial Gain	Advanced Persistent Thr	Surface Web	Extortionists
Financial Gain	Phishing	Surface Web	Extortionists
Criminal Activities	Supply Chain Attacks	Surface Web	Mercenary Hackers
Espionage	Ransomware	Surface Web	APT Groups
Political Ideology	Phishing	Surface Web	Hacktivist Collectives
Internal Disruption	Zero-Day Exploits	Dark Web	Insiders
National Interest	Advanced Persistent Thr	Surface Web	APT Groups
Ransomware	Advanced Persistent Thr	Surface Web	Mercenary Hackers
Advanced Persistent Threa	Social Engineering	Surface Web	APT Groups
Internal Disruption	Zero-Day Exploits	Surface Web	Rogue Employees
Political Ideology	Cryptojacking	Surface Web	Hacktivist Groups
Data theft	Malware	Dark Web	Extortionists
Ideological	Zero-Day Exploits	Dark Web	Terrorist Groups
Financial Gain	Phishing	Dark Web	Organized Crime Groups
Internal Disruption	Social Engineering	Dark Web	Rogue Employees
Data Monetization	SQL Injection	Dark Web	Data Brokers
Political Ideology	Cryptojacking	Dark Web	Hacktivists
Disruption	Zero-Day Exploits	Surface Web	Script Kiddies

Figure 2: Cross Section of the data.

Furthermore, the dataset comprises four key variables, as depicted in the structure outlined in Figure3: attack motivation, attack method, web part, and threat actor. These variables were meticulously selected during the dataset collection process to ensure the dataset encompassed sufficient features conducive to the analytical framework elucidated in this study.

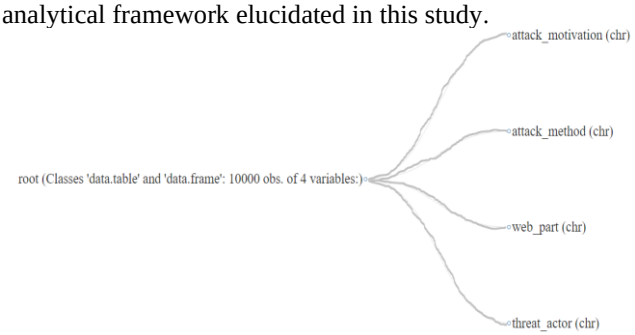

Figure 3: Dataset Structure

F. Preprocessing

Data preprocessing is an important step to prepare the data which will be used for the formation of a model. Data cleaning, data transformation, and feature selection are all key phases in data preprocessing [26]. In this study, Principal component Analysis will be used in feature selection. From the data gathered, PCA was used for feature selection.

First in this study to carryout feature ranking, we will take the hold dataset consisting of $d+1$ dimension. Furthermore, we compute the mean and dimension of every section in the dataset, Again, the computation of the covariance matrix is performed in in eqn 1

$$CO(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x-\bar{x})\ (y-\bar{y}) \qquad 1$$

Furthermore, the computation of eigenvectors and their corresponding eigenvectors will be carried out appropriate and we sort the eigenvectors in ascending order. Finally, we, transform the data into the new subspace using this $d * 1$ eigenvector matrix where each feature can be rank as principal components which is shown in figure 4 depicts the different principal components in the datasets and rank the components based on their relevance.

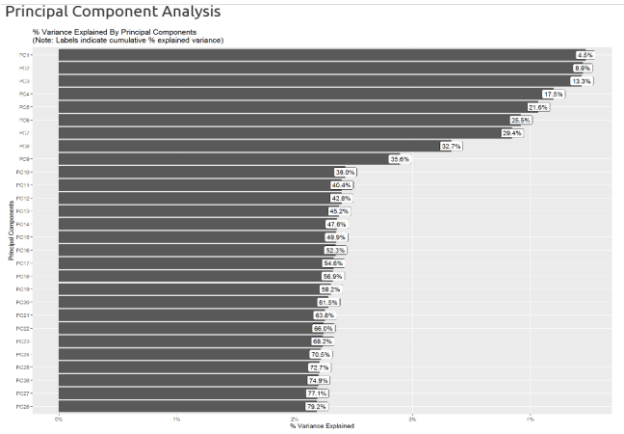

Figure 4: Principal Components ranks

G. Machine Learning Classification

Machine learning classification stands as the fundamental task of sorting input data into distinct classes, drawing upon one or more defining variables [24]. This pivotal process operates under the of supervised learning category, wherein meticulously labeled training datasets are used for algorithms to discern patterns and effectively categorize forthcoming data points [25]. Through a diverse array of algorithms and methodologies, classification endeavors to assign future datasets into relevant categories, thus facilitating informed decision-making and predictive analytics in this study, Multinomial Naive Bayes, Support Vector Machine, Random Forest and CATBOOT algorithms were used for effective classification and comparative result analysis.

H. Performance Evaluation

Performance Evaluation in this study involves the assessment of the machine learning algorithms performances that was use in the classification process in order to ascertain how better each algorithm performs. here confusion matrix will be used for the evaluation of the algorithms while recall, precision and f1score and supports will also aid in showing the performance of each training processes of the ML models.

RESULT AND DISCUSSION

Threat actors play a extensive role, making contributions to the cyber threat data, while others contribute comparatively less. Nevertheless, the figure 5 underscores that all categories of threat actors in this study that consistently remain active, instigating issues and wreaking havoc in various ways. This observation highlights that hackers within these profiles are consistently engaged, conducting daily activities to compromise organizations and execute attacks aligned with their motivations.

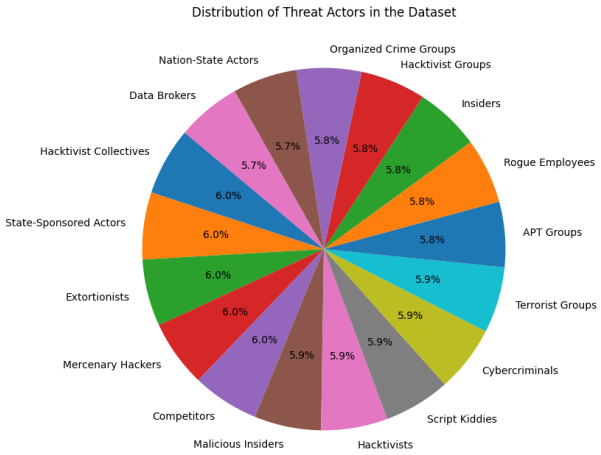

Figure 5: Distribution of Threat Actors

Correlation heatmap is presented in figure 7 illustrating the relationships among the features in the dataset. This visualization provides a clear depiction of the interconnections between each feature within the threat dataset, meaning that any threat actor can employ any type of threat to cause havoc.

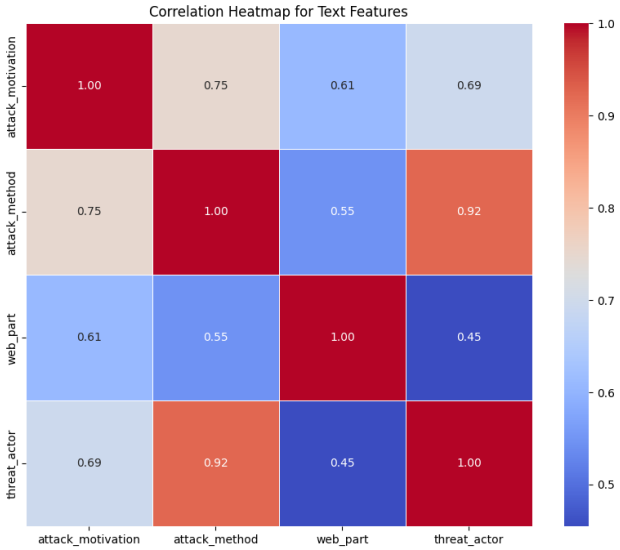

Figure 6: Correlation Heatmap of Features

Furthermore, Machine Learning algorithms was applied in the classification of threat actors based on crucial factors such as motivation, attack method, attack type, and the specific web part utilized. Multinomial Naive Bayes accuracy gave 94%, Support Vector Machine yielded an accuracy of 82%, Random Forest Algorithm gave 82% and CatBoost gave 82% classification results respectively, these results are presented in table 3 to table 5.

Table 3: Multinomial Naïve Bayes

	Precision	Recall	f1-score	support
accuracy			0.94	10000
macro avg	0.91	0.94	0.92	10000
weighted avg	0.91	0.94	0.92	10000

Table 4: SVM

	Precision	Recall	f1-score	support
accuracy			0.82	10000
macro avg	0.75	0.82	0.77	10000
weighted avg	0.75	0.82	0.77	10000

Table 5: Random Forest

	Precision	Recall	f1-score	support
accuracy			0.82	10000
macro avg	0.75	0.82	0.77	10000
weighted avg	0.75	0.82	0.77	10000

Table 6: CatBoost

	Precision	Recall	f1-score	support
accuracy			0.82	10000
macro avg	0.75	0.82	0.77	10000
weighted avg	0.75	0.82	0.77	10000

Furthermore, a comparative analysis is presented in figure 8 comparing all the algorithm and how each performs better than others in the classification process.

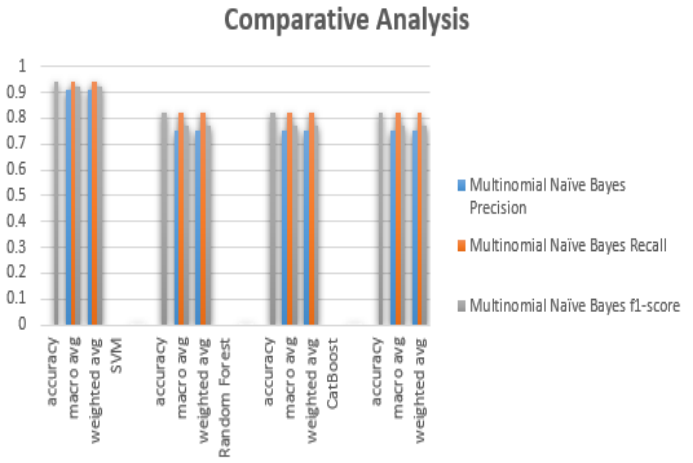

Figure 7: Comparative Analysis

Nevertheless, from the achieve result in this study, we present the findings that is emphasize the relevance of this study as follows:

1. **Consistent Activity of Threat Actors**: Threat actors remain actively engaged, conducting daily activities aimed at compromising organizations and executing attacks aligned with their motivations. This highlights the persistent and evolving nature of cyber threats.
2. **Interconnected Features in Threat Dataset**: The correlation heatmap in Figure 6 illustrates the complex interconnections among features within the threat dataset. This indicates that threat actors can employ a wide range of threat types, adding to the complexity of defending against cyber threats.
3. **Algorithm Performance**: The application of ML algorithms for classifying threat actors yielded varying levels of accuracy, with Multinomial Naive Bayes achieving the highest accuracy at 94%. This suggests that the probabilistic nature of Multinomial Naive Bayes makes it particularly effective for this classification task.

Hence, this study highlights the persistent and multifaceted nature of cyber threats, emphasizing the need for robust and comprehensive cybersecurity measures. The findings also demonstrate the effectiveness of using ML algorithms, particularly Multinomial Naive Bayes, in accurately classifying threat actors based on various features. This study contributes to a deeper understanding of the dynamics of cyber threats and provides valuable insights for enhancing cybersecurity defenses.

CONCLUSION AND SUGGESTION

Insufficient threat attribution and profiling within the dark web pose significant challenges and limitations, largely stemming from the intricate and covert nature of activities in this concealed cyberspace. Addressing these complexities, the present research introduces a novel solution using a Machine learning approach. The application of these Machine Learning algorithms has significantly contributed to our understanding and classification of threat actors based on crucial factors such as motivation, attack method, attack type, and the specific web part utilized. Multinomial Naive Bayes demonstrated the highest accuracy of 94%, followed by SVM, Random Forest, and CatBoost, each yielding 82% During the training and validation of the datasets. Through the systematic analysis of dark web data, the research seeks to provide a comprehensive and accurate understanding of activities occurring in this hidden environment known as the dark web. In the course of this study, we have accomplished a comprehensive analysis encompassing threat attribution, threat actor profiling, and the classification of threat actors. Our endeavors have yielded valuable insights into the intricate domain of cyber threats, particularly within the concealed domain of the dark web. A significant achievement of this work is the successful identification and mapping of cyber threats to threat actors originating from the dark web. Through meticulous analysis and using advanced techniques, we have proficiently correlated these threats in the dark web with known threat actors in the surface web. This not only enhances the general understanding of the diverse motives driving malicious activities but also fortifies our ability to discern and attribute threats emanating from this elusive and often obscured corner of the digital space. The conclusion of our efforts reveals the importance of a holistic approach to cybersecurity, extending beyond surface-level defenses to address the intricacies of the dark web. The successful execution of

threat attribution and actor classification positions this study serves as a valuable contribution to the ongoing pursuit of cyber resilience and the safeguarding of digital space against evolving threats. For further studies, we recommend that focus should be on the inclusion of other web parts other than surface and dark web addressed in this research.

REFERENCES

[1] H. Albasheer, M. Siraj, A. Mubarakali, O. Elsier Tayfour, S. Salih, M. Hamdan, S. Khan, A. Zainal, and S. Kamarudeen, "Cyber-Attack Prediction Based on Network Intrusion Detection Systems for Alert Correlation Techniques: A Survey," Sensors, vol. 22, no. 4, pp. 1494, 2022. [Online]. Available: https://doi.org/10.3390/s22041494.

[2] S. Amit, J. Jay, and K. Gaurav, "Intrusion Detection System: A Comparative Study of Machine Learning-based IDS," Journal of Research Square, vol. 3, no. 2, pp. 1-30, 2022. [Online]. Available: https://doi.org/10.21203/rs.3.rs-1634802/v1.

[3] L. Ashiku and C. H. Dagli, "Network Intrusion Detection System using Deep Learning," Procedia Computer Science, vol. 185, no. 6, pp. 239-247, June 2021. [Online]. Available: https://doi.org/10.1016/j.procs.2021.05.025.

[4] Elsayed, H. A. G., Chaffar, S., & Belhaouari, S. B. (2020). A two-level deep learning approach for emotion recognition in Arabic news headlines. International Journal of Computers and Applications, vol. 44, no. 7, pp. 604-613. doi: 10.1080/1206212X.2020.1851501.

[5] E. A. Emad, E. Wafa, and F. O. Ahmed, "Intrusion Detection Systems using Supervised Machine Learning Techniques: A Survey," in International Conference on Ambient Systems Networks and Technologies, vol. 8, no. 3, pp. 205-212, 2022.

[6] S. B. Erukala, S. R. Mekala, P. Rambabu, R. N. Soumya, and S. Achyut, "A Hybrid Intrusion Detection System against Botnet Attack in IoT using Light Weight Signature and Ensemble Learning Technique," Research Square Journals, vol. 4, no. 2, pp. 1-17, 2022. [Online]. Available: https://doi.org/10.1109/IndiaCom.2014.6828073.

[7] A. D. Evarakonda, N. Sharma, P. Saha, and S. Ramya, "Network intrusion detection: a comparative study of four classifiers using the NSL-KDD and KDD'99 datasets," Research Square Journals, vol. 4, no. 2, pp. 1-17, 2022. [Online]. Available: https://doi.org/10.1088/1742-6596/2161/1/012043

[8] J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A. B. Opare, "An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers," Technologies, vol. 9, no. 1, pp. 14-29, 2021. doi: 10.3390/technologies9010014.

[9] X. Gao, C. Shan, C. Hu, Z. Niu and Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection," in IEEE Access, vol. 7, pp. 82512-82521,2019.

[10] L. Guangrui, Z. Weizhe, L. Xinjie, F. Kaisheng, and Y. Shui, "VulnerGAN: a backdoor attack through vulnerability amplification against machine learning-based network intrusion detection systems," *Science China Information Sciences*, vol. 65, no. 1, pp. 1-19, 2022.

[11] K. Gurbani and K. Dharmender, "Classification of Intrusion using Artificial Neural Network with GWO," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 4, pp. 599-606, 2020.

[12] I. A. Hidayat and A. Arshad, "Machine learning based intrusion detection system: an experimental comparison," Journal of Computational and Cognitive Engineering, vol. 3, no. 1, pp. 23-43, 2022.

[13] Ziaul, H., "Cyber Security of the Maritime ICTs, Threat Vectors and Implications on Global Sea Lanes of Commerce (SLOC)," *Global Journal of Science Frontier Research: E Marine Science*, vol. 23, no. 1, pp. 1-10, 2023.

[14] Alanazi, A. T., "Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats," Cureus, vol. 15, no. 10, e47026, Oct. 2023. doi: 10.7759/cureus.47026

[15] O. Zahra, Z. El, C. Habiba, and B. Salmane, "Cyber-attack crisis management in the context of energy companies," Web of Conferences, vol. 412, p. 01106, 2023. doi: 10.1051/e3sconf/202341201106

[16] N. Jeffrey, Q. Tan, and J.R. Villar, "A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems," Electronics, vol. 12, no. 15, pp. 3283, Aug. 2023. doi: 10.3390/electronics12153283.

[17] A. Jawad, A. S. Syed, L. Shahid, A. Fawad, Z. Zhuo, and P. Nikolaos, "A deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things," Journal of King Saud University – Computer and Information Sciences, vol. 3, no. 3, pp. 1-10, 2022. [Online].Available:https://pureportal.coventry.ac.uk/files/57466468/Published.pdf

[18] S. B. Erukala, S. R. Mekala, P. Rambabu, R. N. Soumya, and S. Achyut, "A Hybrid Intrusion Detection System against Botnet Attack in IoT using Light Weight Signature and Ensemble Learning Technique," Research Square Journals, vol. 4, no. 2, pp. 1-17, 2022.

[19] K. Wolsing, W. Eric, S. Antoine, and H. Martin, "Breaking up Silos of Protocol-dependent and Domain-specific Industrial Intrusion Detection Systems," in *International Symposium on Research in Attacks, Intrusions and Defenses*, 2020, pp. 1-17. doi: 10.1145/3545948.3545968

[20] I. J Umoren & S. J. Inyang, "Methodical Performance Modelling of Mobile Broadband

Networks with Soft Computing Model," International Journal of Computer Applications, vol. 174, no. 25, pp. 7-21, 2021.

[21] A. E. Edet and G. O. Ansa, "Machine Learning Enabled System for Efficient Classification of Intrusion Severity," Global Journal of Engineering and Technology Advances, vol. 16, no. 3, pp. 41-50, 2023.

[22] S. Inyang and I. Umoren, "From Text to Insights: NLP-Driven Classification of Infectious Diseases Based on Ecological Risk Factors," Journal of Innovation Information Technology and Application (JINITA), vol. 5, no. 2, pp. 154-165, 2023.[Online].Available:https://ejournal.pnc.ac.id/index.php/jinita/article/view/2084.