I.J. Wireless and Microwave Technologies, **2024, 1, 43-51**
Published Online on February 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2024.01.04

Enhancing Cybersecurity through Bayesian Node Profiling and Attack Classification

Priyanka Desai
Software Engineer and was a Data Scientist in a Fortune 500 company, India
Email: desaipriyanka2002@gmail.com
ORCID iD: https://orcid.org/0000-0002-3196-625X

Received: 16 June, 2023; Revised: 12 August, 2023; Accepted: 08 September, 2023; Published: 08 February, 2024

Abstract: Due to the epidemic, the majority of users and businesses turned to the internet, necessitating the necessity to preserve the populace and safeguard their data. However, after being attacked, the expense of data protection runs into the millions of dollars. The phrase "Protection is better than cure" is true. The paper deals with profiling the node for safeguarding against the cyberattack. There is a lot of research on network nodes. Here, we address the requirement to profile the node before utilizing machine learning to separate the data. In order to scan the nodes for risks and save the nature of threat as a database, node profiling is being investigated. The data is then classified using a machine learning algorithm utilizing the database. This research focuses on the application of machine learning methods, specifically Gaussian Naive Bayes and Decision Trees, for the segmentation of cyberattacks in streaming data. Given the continuous nature of cyberattack data, Gaussian Naive Bayes is introduced as a suitable approach. The research methodology involves the development and comparison of these methods in classifying detected attacks. The Bayesian method is employed to classify detected attacks, emphasizing the use of Gaussian Naive Bayes due to its adaptability to streaming data. Decision Trees are also discussed and used for comparison in the results section. The research explores the theoretical foundations of these methods and their practical implementation in the context of cyberattack classification. After classification, the paper delves into the crucial task of identifying intrusions in the streaming data. The effectiveness of intrusion detection is highlighted, emphasizing the importance of minimizing false negatives and false positives in a real-world cybersecurity setting. The implementation and results section presents empirical findings based on the application of Gaussian Naive Bayes and Decision Trees to a dataset. Precision, recall, and accuracy metrics are used to evaluate the performance of these methods. The research concludes by discussing the implications of the findings and suggests that Gaussian Naive Bayes is a suitable choice for streaming data due to its adaptability and efficiency. It also emphasizes the need for continuous monitoring and detection of cyberattacks to enhance overall cybersecurity. The paper provides insights into the practical applicability of these methods and suggests future work in the field of intrusion detection.

Index Terms: Node profiling, Intrusion detection, Bayesian theorem, naïve bayes, gaussian naïve bayes (GNB), Decision tree (DT)

1. Introduction

The main goal of a cyber attacker is to take over, steal from, or destroy a person or an organisation by identifying the system's weakness. A growing business issue is this. The rationale for concentrating on the attacks is summed up in figure 1. The income of a large organisation would be significantly impacted if the attacker were to hack the data and erase or edit it. Consequently, it's important to find the attacker before any harm is done.

Any business, no matter how big or small, needs employees with internet-connected computers who are also linked to others online. Additionally, these people/businesses offer software solutions for efficient task completion.

Cyber threat presents a serious challenge to the security of information systems in the connected world of today. As technology develops, so do the methods and level of sophistication used in cyberattacks. For the sake of preserving the integrity and confidentiality of data, it is essential to accurately detect and classify these attacks. This paper delves into existing solutions, their shortcomings, and the author's objectives as it examines the research objectives of node profiling and classifying cyber-attacks using Bayesian approaches.

Servers, printers, switches, and routers are accessible through a network of PCs. These resources are offered to ensure appropriate workflow. However, occasionally all it takes is one click on a bad link to infect the entire network. Therefore, it is claimed that 45% of crimes are committed by hacking, 94% through emails, and 16% through social engineering [1]. Organisational ramifications Most businesses claim that there may have been a hardware compromise [2].

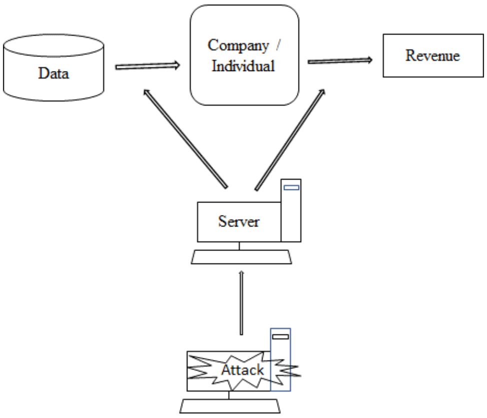


Fig.1. Reason to focus on cyber-attack

The flow that the attacker uses is shown in the figure 2, therefore network node profiling is crucial to prevent infiltration. Node profiling gives an intrusion detection system a better grasp of the network and each of its constituent parts, increasing the effectiveness of the system. An IDS can spot anomalies, identify potential threats, and enhance the network's overall security posture by observing and analysing the behaviour of network nodes.

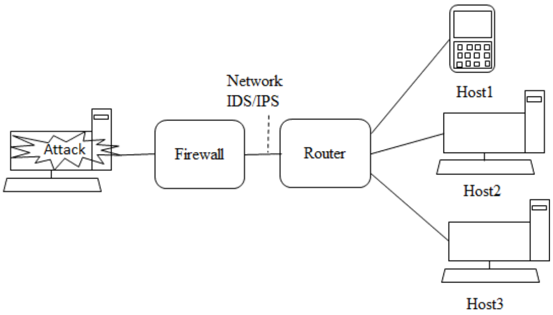


Fig.2. Cyber network- network risk management using attacker profiling

The need for effective and efficient methods to characterize and categorize cyberattacks on network nodes is the main issue this essay addresses. Individual gadgets, such PCs and Internet of Things (IoT) devices, to full servers and data centres can all function as network nodes. Malware infections, denial-of-service attacks, incursion attempts, and data breaches are just a few examples of the many different ways that cyberattacks can manifest. For effective reaction and mitigation, these assaults must be accurately identified and categorized.

The existing challenge is that networks are dynamic and constantly changing, which results in novel attack patterns, emergent dangers, and changes in network behaviour.

There are several existing solutions for detecting and classifying cyber-attacks, including signature-based approaches, anomaly detection, and machine learning-based techniques. Systems that use signatures rely on previously established patterns or signatures of known attacks. Systems for anomaly detection look for differences from typical network behaviour. Machine learning methods use past data to forecast and categorize threats.

Although the cybersecurity provided by current solutions has improved significantly, they still have some drawbacks. Signature-based systems struggle with zero-day exploits and developing threats but are successful against established assaults. False positives can be produced by anomaly detection, and it might struggle to adjust to shifting network conditions. Large labelled datasets are frequently needed for machine learning algorithms, which can be resource-intensive.

The primary research objectives in this paper are as follows:

• Create a Bayesian-based method for accurately profiling network nodes using Gaussian Naïve bayes: The purpose of this article is to provide a novel method based on Bayesian methods for accurately profiling network nodes and their typical behaviour.

• Use Bayesian inference to categorize cyberattacks: This study aims to show how Gaussian Bayesian inference can be used to categorize cyberattacks effectively and efficiently.

• Assess the performance of the suggested methodology: This paper aims to provide empirical proof of the efficiency of the Bayesian-based approach in comparison to other approaches.

• Address the shortcomings of current solutions: The research tries to overcome some of the shortcomings of current cyber-attack detection and classification approaches by recommending a Bayesian-based methodology.

The paper hopes to achieve the following outcomes:

• Better node profiling accuracy: The suggested Gaussian Bayes-based technique that should provide a more precise and flexible method of profiling network nodes, lowering false positives and negatives.

• Improved classification of cyber-attacks: By utilizing Bayesian inference, the paper seeks to offer a reliable system that can correctly classify a variety of cyber-attacks.

• Reducing current restrictions: The research aims to contribute to ongoing initiatives to get beyond restrictions placed on current solutions, potentially resulting in more effective cybersecurity measures.

This paper introduces a Bayesian-based approach for node profiling and attack categorization in order to solve the urgent problem of cyber-attack detection and classification. While Bayesian approaches have many benefits, it's crucial to remember that they are only as good as the data they are applied to, the prior distributions they are chosen with, and the complexity of the underlying network structure. For intrusion detection systems to produce accurate and trustworthy node profiles, careful model design, feature selection, and parameter estimates are essential. Use of Gaussian naïve bayes for node profiling in intrusion detection system due to its ease of use, effectiveness, handling of continuous data, and resistance to irrelevant characteristics, Gaussian Naive Bayes is a common option for node profiling in intrusion detection systems. It offers a solid trade-off between computational effectiveness and performance, especially where data availability or interpretability are key considerations.

The paper's goal is to enhance the cybersecurity landscape as a whole by increasing the efficacy and accuracy of cyber-attack detection. Let's examine node profiling as a possible solution utilising the Bayesian approach. The aim of the research is use of Gaussian Nave Bayes to profile the nodes at data collection locations to discover abnormalities, although the data gathering method is not described as the network data is very private, the public cannot access it.

2. Literature Review

Profiling Nodes:

Clients communicate with servers, as well as routers, switches, firewalls, and intrusion detection systems (IDS). Each component produces data, and this data may be analysed to determine security. Observation- oi, node-ni, and source data-si, time-ti ,the current values as shown in figure 3.

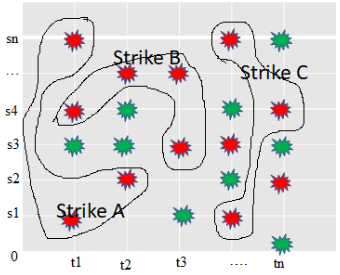


Fig. 3. Source and time of the nodes

A red line delineates the source data that is being attacked at any particular time. Four potential events that might occur on the data include: These are displayed in pink as having a higher likelihood of being malignant due to the attempted intervention.

Green indicates good correlation with known and relevant data. A person attempting to log in repeatedly and failing, or an unknown user attempting to use cmd.exe are some instances of apprehensive-these may be malicious or benign. Not recorded: Because the detection mechanism is inadequate, some attacks go unreported because they are not noticed. One of the main worries is that the precise source of the attack is unknown. Internet Control Message Protocol (ICMP) unreachable message due to virus or intruder assaults is not necessarily harmful as it may be caused by router collapse and not an interference. It is important to understand the attack's motivation, which will be discussed later.

Basic source: A good algorithm is capable of spotting an incursion. Assume that source A is being attacked by sources s1 s2... sn. It is necessary to track down the attack's pattern on the data. One of the main worries is this.

Past information: All of the evidence data is stored in every interference detection system; however, it is only accessible for a short period of time [3]. Since there is a lot of network traffic, keeping data before deleting it is difficult due to issues with processing and storage. Guidelines for incidence that must be researched in order to find the assault A on source s1 s2...sn are required. Instead of using packet information, logs are kept to identify the source. However, analysing these logs is a significant undertaking that may be expensive [4,5,6,7].

The existing articles by Meng, Y. et.al.[8] proposes Bayesian node detection method for wireless intrusion detection systems is evaluated in this conference article. In order to evaluate the effectiveness of the Bayesian model in terms of detection accuracy, false positive rate, and false negative rate, Meng conducts comprehensive experiments using real-world datasets. The review shows the advantages and disadvantages of the Bayesian methodology while contrasting it with other widely used intrusion detection methods.

Yousif et.al. [9] gives an overview of network node intrusion detection technologies in this thorough analysis. In order to identify intrusions aimed at network nodes, the study investigates various intrusion detection methods, such as signature-based, anomaly-based, and behaviour-based ones. The survey covers the benefits and drawbacks of various strategies and pinpoints new developments and difficulties in the industry.

Huang [10] gives an overview of applying the Naive Bayes algorithm for network intrusion detection in this thorough examination. The paper goes through the fundamentals of the Naive Bayes algorithm, how it's used to detect network intrusions, as well as its benefits and drawbacks. The Naive Bayes algorithm is extended and modified in the review in order to improve its performance in identifying various kinds of network intrusions.

3. Research Methodology

Here, the emphasis is on using machine learning methods like decision trees and Gaussian Naive Bayes [11,12] to segment cyberattacks. Due to the fact that data from cyberattacks is continuous, the proposed Bayes theorem is changed to gaussian naive bayes. In the results section, a comparison of the decision tree [13,14] and gaussian naive bayes algorithm is shown.

3.1. Bayes method to classify the detected attacks:

Take a look at the Bayes theorem using nave bayes for two events. Finally, given that we are dealing with continually incoming data, we use gaussian naive bayes. Bayesian hypothesis derived is generalised for evidence and nodes. This section also explains Decision Tree that is used for comparison in the results section.

- ***Bayes hypothesis:***

Given the evidence

$$E = (e_1, e_2, \dots e_n), \tag{1}$$

the Bayes theorem provides the posterior probability An-node (where A1-the node is an attack, A2-the node is not an assault). Thus, the formula is as follows:

$$P\left(\frac{An}{E}\right) = \frac{P\left(\frac{E}{An}\right).P(An)}{P(E)} \tag{2}$$

replace An with A1 if node is an attack or A2 if the node is not an attack

$$P\left(\frac{E}{A_n}\right)\text{-is conditional probability} \tag{3}$$

P(An)-is the prior belief, P(E) -Probability that gives suspicious events

- ***Naïve Bayes***

In naïve bayes two events are independent of each other, hence the formula can be rewritten as:

$$P\left(\frac{A1}{(e_1,e_2,\dots e_n}\right) = \frac{P(e1/A1).P(e2/A1)\dots.P(en/A1)..P(A1)}{P(e1).P(e2)\dots..P(en)} \tag{4}$$

This can be written as

$$P\left(\frac{A1}{(e_1,e_2,\dots e_n}\right) = \frac{P(A1)\prod_{i=1}^{n} e_i/A1}{P(e1).P(e2)\dots..P(en)} \tag{5}$$

As the denominator is constant it can be changed to:

$$P\left(\frac{A1}{(e_1,e_2,\dots e_n}\right) \alpha\ P(A1)\prod_{i=1}^{n} e_i/A1 \tag{6}$$

For a classifier model the formula will be

$$A1 = argmax_{a1}\, P(A1)\ \prod_{i=1}^{n} e_i/A1 \tag{7}$$

- ***Gaussian Na ïve bayes:***

Is each feature's continuous value, which must be distributed using a Gaussian distribution. If yes then the probability is gaussian.

Currently, the conditional probability is:

$$\mathrm{P}(\frac{e_i}{A1}) = \frac{1}{\sqrt{2\pi\sigma_{a1}^2}} \exp(-\frac{(e_i - \mu_{A1})^2}{2\sigma_{a1}^2}) \tag{8}$$

3.2 Decision Tree method to classify detected attacks:

The predictions are organised into a tree-like structure that begins at the root and finishes at the leaf. Let's examine the terminology frequently used in decision trees.

The tree begins with a root node, from which decision nodes are produced. Leaf nodes mark the end of the tree and the point at which further splitting ceases.

Information gain=1-entropy

Creating a tree using information gain

- Calculate the entropy of all positive and negative datapoints
- Calculate weighted average entropy of every datapoint
- Take the datapoint with less entropy of high information gain as the root

3.3 After classifying data using gaussian naive bayes and a decision tree, it becomes necessary to identify intrusion:

The first step in stopping the assault is to find the incursion. "Prevention is better than cure," says the adage. Many overheads can be eliminated if the calculation can manage the heavy flow and identify the assault. The biggest difficulty is detecting behaviour of the stream data due to the enormous number of data following the epidemic in 2019. Therefore, stronger intrusion detection systems are required.

There is a good likelihood of identifying an attacker if they are not aware of the actions of the authorised user. several methods of spotting cancerous activity

Not invasive but yet interfering This is a false negative because the intrusion happens but the system is unable to identify the assault. The system for detecting the attack has failed and needs a careful study.

Negative intrusion and Negative interference: Despite the attack's anomalous nature, the system mistakenly registers it as non-invasive, making it a real negative.

The system senses an assault, but it's simply a false alert, or obtrusive negative interference.

The system detects invasive and interfering activity. Attacks of this nature should be documented and responded to as true positives.

The attack should be tracked by a competent system, which won't record false positives, false negatives, or genuine negatives. A real negative will have an impact on the system's overall performance, but a fake negative is still OK. To avoid being detected by the system, the attackers adopt different tactics.

The study employs the supervised machine learning approach to identify anomalies since the output labels are included in the dataset.

Notation for detecting malignant behaviour:

T+=true positive
F+=false negative
T-=true negative
F-=false negative

Precision is the T+ that are correctly classified

$$precision = \frac{T+}{(T+)+(F+)} \tag{9}$$

Recall is T+ that were successfully generated

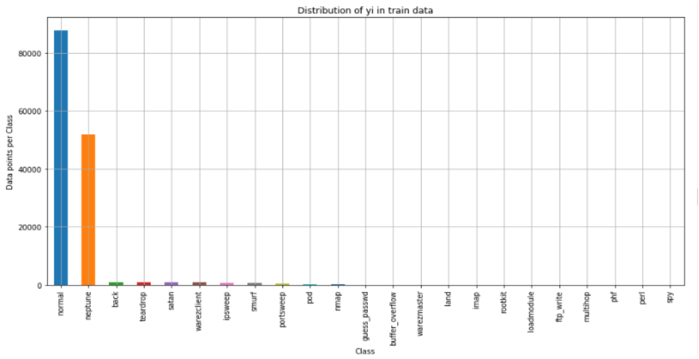
$$recall = \frac{T+}{(T+)+(F-)} \tag{10}$$

4. Implementation and Results

The outcomes of Gaussian naive bayes and decision trees for the dataset from [15] are discussed below. The dataset is executed, and 23 different output labels are produced. The paper uses these labels to train and evaluate the data and detect intrusion.

```
========================================
normal : 87831 ( 60.33 %)
neptune : 51820 ( 35.594 %)
back : 968 ( 0.665 %)
teardrop : 918 ( 0.631 %)
satan : 906 ( 0.622 %)
warezclient : 893 ( 0.613 %)
ipsweep : 651 ( 0.447 %)
smurf : 641 ( 0.44 %)
portsweep : 416 ( 0.286 %)
pod : 206 ( 0.141 %)
nmap : 158 ( 0.109 %)
guess_passwd : 53 ( 0.036 %)
buffer_overflow : 30 ( 0.021 %)
warezmaster : 20 ( 0.014 %)
land : 19 ( 0.013 %)
imap : 12 ( 0.008 %)
rootkit : 10 ( 0.007 %)
loadmodule : 9 ( 0.006 %)
ftp_write : 8 ( 0.005 %)
multihop : 7 ( 0.005 %)
phf : 4 ( 0.003 %)
perl : 3 ( 0.002 %)
spy : 2 ( 0.001 %)
========================================
```

(a)



(b)

Fig.4. (a). 23 different outputs (b): Graph of these 23 labels

After training and testing the dataset, the following outcome is generated.

```
Train data 70%
(101909, 116)
(101909, 1)
====================
Test data 30%
(43676, 116)
(43676, 1)
====================
```

The time taken, precision, recall and accuracy by the machine learning algorithm is generated as follows:

```
Time taken: 0:00:00.000414
The precision for GNB is  0.9736349467927717
The recall for GNB is  0.8717831303232897
The accuracy for GNB is 0.8717831303232897
```

```
Time taken: 0:00:03.987187
The precision for Tree is  0.9989732429978856
The recall for Tree is  0.9989466452942524
The accuracy for Tree is 0.9987178313032329
```

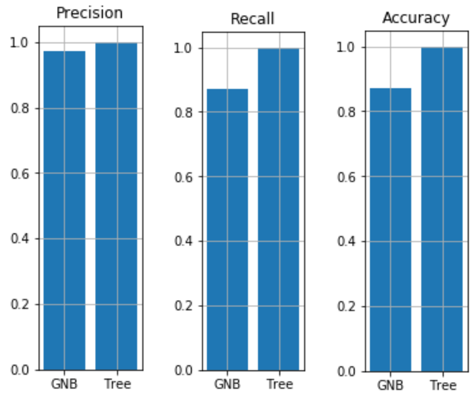


Fig.5. Precision recall and accuracy of GNB and DT

5. Inference and Future Work

After profiling the nodes, create logs: The report lists cybersecurity logs among the many types of logs. Because of the heavy traffic, it is impossible to profile every good or bad node active at any given time, the logs are useful in identifying assaults. Consequently, logs must be generated in order to check the assaults. The logs are produced using Cybernet profiling.

The logs should: Keep tabs on nodes constantly. Prevent unauthorised access by forbidding content modification. If the present logs have reached their maximum size, provide alternative logs. Keep track of system crashes, new service offerings, deleted user accounts, unsuccessful or failed login attempts, and changes to privileged users. Work on logs that you can identify. To establish the business case, risk associated with the business case, and use case check, a brainstorming session is helpful. Basically, pay attention to the little details of the log as you interpret it. There may be a requirement to identify the malware infection as a business case log.

Use decision trees and Gaussian Naive Bayes to categorise nodes once they have been profiled to ensure that the attacks, they are producing are appropriate for the training dataset.

6. Conclusion

The research objectives outlined in the introductions is achieved through a systematic approach involving data collection, model development, experimentation, and evaluation.

Here's how each of the research objectives was achieved:

- *Developed a Bayesian-based method for profiling network nodes and use Gaussian Naive bayes for profiling:*

Data Collection: Gathered a diverse dataset that includes information about network nodes' normal behaviour. This data covers various network scenarios and conditions.

Model Development: Developed a Bayesian model that can analyse and profile network nodes based on the collected data and used Gaussian Naive Bayes as the data being used should be stream data. This model was able to adapt to changing network conditions and identify normal behaviour accurately.

Experimentation: Performed test using Bayesian-based profiling method on the collected dataset to ensure it accurately characterizes network node behaviour.

- *Classify cyber-attacks using Gaussian Naive Bayesian inference:*

Data Collection: This dataset includes instances of various cyber-attacks, with labelled data indicating the type of attack.

Model Development: Used Gaussian Bayesian inference-based classification model that can analyse network traffic data and classify it into different attack categories.

Experimentation: Evaluated the Bayesian inference model's performance by feeding it with network traffic data containing both normal and attack patterns. Measured the model's accuracy in classifying different types of cyber-attacks.

- *Evaluate the proposed approach's performance:*

Experimentation: Rigorous experiments were conducted using secondary network data to compare the performance of the Gaussian Bayes-based approach with existing methods and Decision Tree was used as a comparative measure.

Measure accuracy, precision, recall.

Statistical Analysis: Though statistical tests to prove Decision Tree performed better than Gaussian Bayes-based approach as it is secondary data. For primary stream data Gaussian Bayes is suitable as it updates incrementally as new data arrives without having to retrain the model from scratch.

- *Address limitations of existing solutions:*

Literature Review: Identified and thoroughly analysed the limitations of existing cyber-attack detection and classification methods. Understand the specific challenges they face.

Model Enhancements: Modified and refined the Gaussian Bayes-based approach to directly address the identified limitations. For example, Gaussian Naive Bayes: This algorithm has a relatively small memory footprint, as it only needs to maintain statistics (mean and variance) for each feature and class. It doesn't store the entire data, which can be essential when dealing with large streams of data. As data distribution shifts over time due to changes in underlying patterns or behaviours, Naive Bayes can adapt by updating its probability estimates. The Naive Bayes model is relatively simple and interpretable, which can be advantageous for understanding why certain predictions are made, especially in real-time scenarios where interpretability is crucial.

Comparative Analysis: As gaussian bayes updates incrementally as new data arrives, this property makes it efficient for handling continuously arriving data. Decision Trees typically require retraining the entire model when new data is introduced, which can be computationally expensive and time-consuming. This makes Decision Trees less suitable for stream data. Therefore, with the use of Gaussian bayes approach there is improved accuracy in node profiling, and enhanced cyber-attack classification

Additionally, the paper provides insights into the practical applicability of the Bayesian-based approach in the cybersecurity scenarios, showcasing its effectiveness in improving cyber-attack detection and classification.

In this paper, decision trees and Gaussian naive bayes are used. Before going ahead with intrusion detection and analysis find if it is necessary to carry out the exercise. First, determine if there is data backup accessible for the organization's job that involves large amounts of data. Then determine if it's necessary to detect the security system if data is compromised. In certain cases, the breach may not cause a significant loss to the company or the person whose data was exposed. It's similar to home upkeep in that some homes require immediate attention while others go years without any. Therefore, determine if a security system is necessary. Finally, once we have the data and feel the need to detect intrusion, check if it is necessary to determine whether the data accurately distinguishes between an attack and a non-attack as demonstrated in the findings using Gaussian na ïve bayes and decision tree. The accuracy for GNB is 0.8717831303232897. The accuracy for Tree is 0.9987178313032329. Though, Decision trees produce good results, the results are not always accurate. One may use supervised, unsupervised, and semi-supervised machine learning algorithms. It is recommended to utilise an unsupervised strategy while dealing with a live dataset since anomalies are constantly evolving and need to be found. Unsupervised will make it easier to create various anomaly clusters that may be utilised to more accurately categorise the abnormalities.

Authors' Contribution

Dr. Priyanka participated in every step of the writing of this paper. She developed the data selection, the entire paper's flow, and put the code into action.

References

[1] Alkhalil Zainab et.al,"Phishing Attacks: A Recent Comprehensive Study and a New Anatomy ",Frontiers in Computer Science,Vol-3, 2021, pp6, doi=10.3389/fcomp.2021.563060 .

[2] Steve Ursillo, Jr., Christopher Arnold,"Cybersecurity Is Critical for all Organizations – Large and Small",International Federation of accounts,| November 4, 2019.

[3] Cisco Annual Internet Report (2018–2023) White Paper,March 9, 2020.

[4] Julian Jang-Jaccard, Surya Nepal,"A survey of emerging threats in cybersecurity",Journal of Computer and System Sciences,Volume 80, Issue 5,2014,Pages 973-993,ISSN 0022-0000,https://doi.org/10.1016/j.jcss.2014.02.005.

[5] Julian Jang-Jaccard, Surya Nepal,"A survey of emerging threats in cybersecurity",Journal of Computer and System Sciences,Volume 80, Issue 5,2014,Pages 973-993,ISSN 0022-0000,https://doi.org/10.1016/j.jcss.2014.02.005.

[6] D. Gupta, P. S. Joshi, A. K. Bhattacharjee, and R. S. Mundada, ''IDS alerts classification using knowledge-based evaluation,'' in Proc. 4th Int. Conf. Commun. Syst. Netw. (COMSNETS), Jan. 2012, pp. 1–8, doi: 10.1109/COMSNETS.2012.6151339.

[7] M. A. Siddiqi, W. Pak, and M. A. Siddiqi, ''A study on the psychology of social engineering-based cyberattacks and existing countermeasures,'' Appl. Sci., vol. 12, no. 12, p. 6042, Jun. 2022.

[8] Meng, Y., Li, W., Kwok, Lf. (2013). Evaluation of Detecting Malicious Nodes Using Bayesian Model in Wireless Intrusion Detection. In: Lopez, J., Huang, X., Sandhu, R. (eds) Network and System Security. NSS 2013. Lecture Notes in Computer Science, vol 7873. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-38631-2_4 -

[9] Suleiman S. Fawzy, Abeer M. Yousif,2009,'Network Node Intrusion Detection System',Iraqi Journal of Science,Volume 50, Issue 3, Pages 396-402.

[10] Y. Huang, "Network Intrusion Detection Method Based on Naive Bayes Algorithm," 2022 6th Asian Conference on Artificial Intelligence Technology (ACAIT), Changzhou, China, 2022, pp. 1-10, doi: 10.1109/ACAIT56212.2022.10137846.

[11] K. Bajaj and A. Arora, ‘‘Dimension reduction in intrusion detection features using discriminative machine learning approach,’’ Int. J. omput. Sci. Issues, vol. 10, no. 4, p. 324, 2013.

[12] S. N. Murray, B. P. Walsh, D. Kelliher, and D. T. J. O’Sullivan, ‘‘Multi-variable optimization of thermal energy efficiency retrofitting of buildings using static modelling and genetic algorithms—A case study,’’ Building Environ., vol. 75, pp. 98–107, May 2014.

[13] S. Keele et al., ‘‘Guidelines for performing systematic literature reviews in software engineering,’’ Tech. Rep. EBSE 2007-001, Version 2.3, 2007.

[14] N. Kshetri and J. Voas, ‘‘Hacking power grids: A current problem,’’ Computer, vol. 50, no. 12, pp. 91–95, Dec. 2017.

[15] Joaquin Vanschoren," Intrusion detection datasets ACM KDD Cup",1999.

Author’s Profile

Dr. Priyanka Desai has approximately 20 years of experience as an Trainer, educator in Academia, Software Engineer and was a Data Scientist in a Fortune 500 company. Published/presented more than 12 papers in International/National Journals and Conferences.

Has handled Industry and academic projects and was a reviewer of International Conferences (IEEE) Mumbai and Bangalore chapters.

How to cite this paper: Priyanka Desai, "Enhancing Cybersecurity through Bayesian Node Profiling and Attack Classification", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.1, pp. 43-51, 2024. DOI:10.5815/ijwmt.2024.01.04