Automated Penetration Testing: Machine Learning Approach*

Jay Saini[1,], Ankita Bansal[2,*,]

[1] Department of information technology, Netaji subhas university of technology, 110078 Delhi, India
[2] Department of information technology, Netaji subhas university of technology, 110078 Delhi, India

Abstract

In our study, we used a better version of a dataset called KDD-99, known as the corrected dataset. The original KDD-99 dataset is often used for studying cybersecurity in real-time, but it has some problems. So, we picked the improved version to make our tests more realistic. This special dataset helped us imitate real cyber threats more accurately when we were testing computer systems and networks. We wanted to create challenges for artificial intelligence (AI) systems trying to tell the difference between real and fake attacks. By using the corrected dataset, we made our tests a bit like real cybersecurity situations, making it harder for AI to figure out what was happening. Our approach, using different tools and methods, builds a complete system for testing security. We always make sure our tests are ethical and authorized, and we do them regularly to keep up with new cyber threats. This way, we can better protect organizations from potential risks.

Keywords

Artificial Intelligence, Machine Learning, Intrusion Detection, KDD_99

.

1. Introduction

Communication systems act as indispensable aides in our daily routines, seamlessly facilitating work, learning, teamwork, data sharing, and enjoyable entertainment. Yet, the intricate computer networks orchestrating these activities face potential risk. Safeguarding them requires the vigilant oversight of an intrusion detection system (IDS), functioning as a steadfast guardian for our computer systems.

Consider the bustling activity on a popular website numerous visitors mean a wealth of incoming information. To manage this influx, computers leverage machine learning, a process wherein they glean insights from data. Subsequently, data mining comes into play, extracting pertinent details from the vast pool of information. Now, envision possessing insights into diverse methods that individuals might employ to compromise a network.

Symposium on Computing & Intelligent Systems (SCI), *May 10, 2024, New Delhi, INDIA*

* Corresponding author.

† These authors contributed equally.

Jaysaini1899@gmail.com (J. Saini); ankita.bansal06@gmail.com(A. Bansal);

Enter a tool called nmaps, adept at organizing and comprehending this information, akin to categorizing items into groups. This strategic approach aids in deciphering ongoing activities and identifying potential threats.

This comprehensive study underscores the paramount importance of communication systems and the concerted efforts invested in ensuring their security. Leveraging specialized tools and ingenious computing techniques, we navigate the intricacies of data within these systems, particularly concerning potential cyber threats. The research delves into computer data, reserving a portion (approximately 20%) for practice and testing purposes.

But there were many problems with dataset so in order to address these limitations, Tavallaee et al. [7] created a dataset that was devoid of any flaws, free from imperfections, and included entries from the KDD-CUP 99 dataset, excluding redundant and duplicated values.

Aggarwala and Sharmab [17] interpreted the data attributes, which were classified into traffic, basic, host, and content categories, within the KDD-CUP 99 dataset. The results of their experiments in the realm of intrusion detection systems demonstrated an increased detection rate coupled with a reduction in false alarm rates. Gaffney and Ulvila [18] introduced methods for distinguishing the performance of intrusion detectors and, for a given environment, identified the optimal configuration for an intrusion detector. To establish an expected cost metric, this approach employed a decision analysis that integrated receiver operating characteristics (ROC) with a cost analysis method.

The primary objective is to pinpoint vulnerable sections of the network, discerning which areas are most susceptible to potential attacks by adversaries. This multifaceted exploration combines practical testing and strategic analysis to fortify our understanding and defenses against evolving cyber threats.

The remaining paper is organized as: Section 2 explains Motivation, followed by literature survey in section 3. Section 4 explains dataset and techniques used. The results are illustrated in section 5. finally, the work is concluded in section 6.

2. Motivation

This study endeavors to thoroughly assess the existing landscape of network penetration testing while also outlining potential directions for future research. In light of the ever-increasing frequency and sophistication of cyber-attacks in our contemporary digital landscape, we underscore the paramount significance of network security. Penetration testing emerges as a vital pillar in fortifying network security, systematically uncovering vulnerabilities and weaknesses before they can be exploited by malicious entities.

Penetration testing, or pen testing, is a vital cybersecurity process that simulates cyberattacks to uncover and address vulnerabilities in systems. It involves key phases like reconnaissance, scanning, vulnerability analysis, exploitation, and reporting, utilizing tools such as network scanners and exploit frameworks. Aspiring penetration testers must grasp these concepts to enhance organizational security. Ethical hacking, requiring expertise and authorization, is an ongoing process crucial for regularly fortifying cybersecurity measures. Pen testing serves as a proactive defense, identifying and addressing vulnerabilities before real threats exploit them, bolstering overall organizational security.

Traditional methodologies for penetration testing are recognized for their labor-intensive nature, substantial financial commitments, and the demand for a high level of expertise. In response to these challenges, our innovative approach introduces an automated framework for penetration testing, aimed at not only streamlining the process but also supporting initiatives related to defense training. The overarching objective is to demonstrate the effectiveness of this automated framework in penetration testing, showcasing its potential to instigate transformative advancements in the dynamic field of cybersecurity. This pioneering solution aligns with the imperative need for proactive defense measures and strategic preparedness in the face of evolving cyber threats.

3. Literature Survey

In this paper, a thorough examination of existing literature has been conducted to appraise the ongoing research. Various papers, articles, and books have been scrutinized to assess the current state of knowledge and identify areas where information is lacking. This process aids in comprehending the existing landscape, discerning gaps in knowledge, and understanding the evolution of thought in the field. The survey establishes a foundational understanding for subsequent phases by summarizing critical concepts, highlighting gaps, and illustrating the progression of ideas in the subject area. Analogous to consulting a map before embarking on a journey, this investigation serves as a strategic guide, assisting in determining the current position and potential areas for exploration in the field of machine learning. All the findings of the previous contributors are shown the table 1.

Table 1. Literature survey

Authors	Findings
Wang et al. [1]	built an intrusion detection system using Support Vector Machine (SVM) with a special focus on enhancing features. This technique improves the quality of data for training SVM classifiers, making them more precise and concise. The proposed system not only boosts intrusion detection capabilities but also reduces training time. Author tested it with the NSL-KDD dataset, and the results show superior performance, especially in metrics like false alarm rate, accuracy, and detection rate.
Jabbar et al[2]	Proposed a system called RFAODE(Random Forest Average One Dependence Estimator) for Detecting intrusions. RFAODE combines two algorithms, namely random forest and average one dependency estimator, to improve accuracy and reduce errors. Random forest helps with accuracy, while average one dependence estimator tackles issues with attribute dependency in Naive Bayes classifiers. I tested RFAODE using the Kyoto

	2006+ dataset and achieved an accuracy of 90.51% with a low false alarm rate of 0.14. These algorithms effectively distinguished between normal and malicious network traffic.
Dahiya and Srivastava [3]	The author has crafted a framework aimed at precise intrusion prediction in network records using Spark. In the proposed work, an algorithm for reducing features was integrated to discard less significant ones. Subsequently, a supervised data mining technique was employed on the UNSW-NB 15 dataset. The outcomes were assessed using two feature reduction algorithms, Linera Discriminant Analysis (LDA) and Canonical Correlation Analysis (CCA), in conjunction with seven classification algorithms.
Belouch et al.[4]	The author assessed the effectiveness of four machine learning algorithms—namely, random forest, Naive Bayes, SVM, and decision tree—utilizing Apache Spark. Performance metrics, including prediction time, accuracy, and building time, were calculated. The experimentation was conducted on the UNSW-NB 15 dataset. The findings indicated that the random forest classifier outperformed others, demonstrating superior results in prediction time, accuracy, and building time.
Aziza et al.,[5]	The analysis involved a comparison of various classifiers to enhance detection accuracy and gain more insights into detected anomalies. The study revealed distinct classifier rates, emphasizing that a one-size-fits-all approach is not suitable for all types of attacks. Notably, 90% of anomalies were successfully identified during the detection phase. However, in the classification phase, 88% of false positives were mistakenly labeled as normal traffic connections. The use of NB, NBTree, and BFTree classifiers demonstrated an accuracy of 79% in correctly labeling Dos and Probe attacks.
Ambusaidi and Nanda [6]	The author developed an algorithm grounded in mutual information to address dependent features in the data. The designed Intrusion Detection System (IDS) based on Least Square Support Vector Machine (LSSVM-IDS) was evaluated using datasets including Kyoto 2006+, KDD CUP-99, and NSL-KDD. The proposed approach achieved higher accuracy and reduced computational costs through the utilization of the feature selection-based algorithm, LSSVM-IDS.
Sultana and Jabbar [7]	The author introduced an intelligent network intrusion detection system employing the Average One Dependence Estimator (AODE) algorithm. The results were assessed using the NSL-KDD dataset, demonstrating a successful outcome with a low False Alarm Rate (FAR) and a high Detection Rate (DR) in the proposed model based on the AODE algorithm.

An and Liang [8]	The author introduced a novel algorithm, incorporating Fisher Discriminate Analysis by integrating within-class scatter alongside the traditional Support Vector Machine (SVM) for classifiers. The proposed algorithm underwent testing using the KDD-Cup 99 dataset. In comparison to Fisher Discriminate Analysis and the conventional SVM, the implemented algorithm (WCS-SVM) demonstrated superior discriminatory power. Additionally, it exhibited enhanced detection rates and reduced false positive rates, showcasing its efficacy in intrusion detection systems.
Tavallaee et al[9]	created a new dataset that was free from imperfections. This dataset was curated by retaining records from the KDD-CUP 99 dataset while eliminating redundant and duplicated values, addressing the shortcomings of the original dataset.
Fawagreha et al. [14]	The focus of the author was on the evolution of Random Forest (RF) from its early development to recent advancements. The primary objective of the proposed work was to comprehensively represent the research conducted to date, offering an analysis of the potential and future developments in the field of Random Forest.
Aggarwala and Sharmab, [17]	The attributes of the data, classified into traffic, basic, host, and content categories, were analyzed within the KDD-CUP 99 dataset.
Gaffney and Ulvila [18]	Introduced some methodologies aimed at discerning the efficacy of intrusion detectors and identifying optimal configurations for intrusion detectors within a given environment. The approach employed a decision analysis that integrated receiver operating characteristics (ROC) with a cost analysis method to establish an expected cost metric.

4. Materials

This section delves into the research methodology employed, elaborating on how the ML technique was utilized. Additionally, the effectiveness of incorporating this ML technique is thoroughly discussed.

4.1 Dataset

Our experimental work utilized the KDD-CUP 99 dataset on a machine with a 2GHz processor, 4GB RAM, and a 64-bit Windows operating system. This dataset, obtained from Lincoln Labs, mimics the U.S. Air Force Local Area Network (LAN) and comprises seven weeks of raw TCP dump data. It contains various attacks and focuses on the sequence of TCP packets within fixed time intervals, along with specific source and target IP addresses.

Initially, the dataset consisted of approximately five million records, which was too large for research purposes. Thus, we generated a 10% subset for our initial model implementation. With 41 features, including 22 attack types categorized into four classes, the dataset provided a solid foundation for our research.

However, due to errors in the KDD-99 dataset, we utilized the KDD-99_corrected dataset, which rectifies these mistakes. Stolfo et al.[8] and colleagues introduced advanced features to differentiate between normal connections and potential attacks. These features include "same host" and "same service" features, which analyze connections with identical destinations or services within specific time frames.

Some attacks, such as probing attacks, follow extended scanning intervals, which require a different approach. Connection records were sorted by destination host to generate host-based traffic features by considering a window of 100 connections to the same host.

Unlike DOS and probing attacks, R2L and U2R attacks do not exhibit frequent sequential patterns. This is because DOS and probing attacks involve numerous connections to specific hosts in a short time, while R2L and U2R attacks often involve a single connection.

Effectively mining unstructured data portions of packets remains a challenge. Stolfo et al. [8] addressed this by introducing "content" features that identify suspicious behavior in data portions, such as tracking failed login attempts. These content features add an extra layer of scrutiny to the analysis.

The attack classes present in KDD-99_corrected are as follows:

- DOS: Attackers exhaust a target's resources, rendering it incapable of handling valid requests. Relevant features include "source bytes" and "percentage of packets with errors."
- Probing: Surveillance and other probing attacks aim to acquire information about a distant victim. Relevant features include "duration of connection" and "source bytes."
- U2R: Attackers gain unauthorized access to local superuser (root) privileges. Relevant features include "number of file creations" and "number of shell prompts invoked."
- R2L: Attackers gain unauthorized access from a remote machine. Relevant features include network-level features like "duration of connection" and "service requested," as well as host-level features like "number of failed login attempts."

4.2 Techniques

In our exploration of classification algorithms, Naive Bayes stands as a resilient contender. Rooted in the timeless principles of Bayes' theorem, Naive Bayes excels in swiftly discerning patterns within data, particularly in domains like natural language processing. Its strength lies in its ability to probabilistically infer class memberships, navigating through the intricacies of feature spaces with remarkable agility.

Logistic Regression, while named for its resemblance to linear regression, holds a distinct prowess in the realm of binary classification. With a keen eye for discerning probabilities, Logistic Regression paints a nuanced picture of class likelihoods, shedding light on the subtle interplay of variables that underlie classification decisions. Its interpretability and adaptability make it a cornerstone in the toolkit of classification practitioners.

Support Vector Machines (SVM) emerge as formidable allies in our quest for effective classification. With an uncanny ability to carve out optimal hyperplanes amidst complex feature spaces, SVMs navigate the intricate terrain of classification challenges with poise and precision. Their adaptability to both linear and non-linear scenarios renders them indispensable companions in the pursuit of accurate predictions.

Ensemble methods, epitomized by Random Forest, usher in a new era of predictive power. By orchestrating a symphony of decision trees during training, Random Forest fortifies accuracy while guarding against the siren song of overfitting. Insights gleaned from feature importance further deepen our understanding of the underlying data dynamics, empowering us to make informed decisions amidst the complexity of real-world datasets.

XGBoost, a beacon of innovation, fuses the strengths of gradient boosting with the versatility of tree-based models. Through iterative refinement, XGBoost elevates predictive accuracy to unprecedented heights, wielding computational efficiency as its sword and interpretability as its shield. Its prowess extends across a spectrum of applications, from financial forecasting to medical diagnosis, where precision is paramount.

Adaboost, with its adaptive learning framework, embodies resilience in the face of uncertainty. Iteratively refining its models based on misclassified instances, Adaboost crafts a robust framework capable of navigating the most treacherous of classification landscapes. Its adaptability to imbalanced datasets and its steadfast pursuit of accuracy make it a stalwart ally in our pursuit of knowledge and insight.

Rounding off our ensemble, Extra Trees Classifier emerges as a testament to the power of randomness. By embracing uncertainty and exploring the vast expanse of feature space with abandon, Extra Trees Classifier unlocks new vistas of predictive accuracy and robustness. Its ability to transcend conventional boundaries offers a glimpse into the boundless potential of machine learning in unraveling the mysteries of our data.

Each algorithm within our arsenal embodies a unique blend of art and science, weaving a rich tapestry of possibilities across the vast expanse of our dataset. As we chart our course through the uncharted waters of classification, we do so with a reverence for the complexity of the task at hand and a steadfast commitment to unlocking the secrets that lie hidden within.

5. Result and analysis

The application of various classifiers, including Naive Bayes (NB), Logistic Regression(LR), Support Vector Machine (SVM), Random Forest (RF), XG Boost, Ada Boost, Extra trees classifier the dataset yielded valuable insights into their performance for distinguishing between Normal and Bad connections in a network. Each classifier exhibited strengths and limitations in accurately classifying instances from different classes. The following summarizes key findings:

- **Logistic Regression**: This model demonstrates a commendable True Positive Rate (TPR) of 99.82%, signifying its ability to correctly identify nearly all positive instances. However, its False Positive Rate (FPR) of 0.0276 indicates a small proportion of negative instances being incorrectly classified as positive. While it excels in capturing positive instances, the occurrence of false alarms suggests the need for cautious interpretation, especially in applications sensitive to such errors.

- **Support Vector Machine (SVM)**: With an impressively low FPR of 0.0043, the SVM model showcases its proficiency in minimizing false alarms. Simultaneously, its TPR of 99.87% underscores its effectiveness in identifying positive instances accurately. This balanced performance suggests SVM as a reliable choice across various classification scenarios.

- **Random Forest**: Among the models, Random Forest stands out with the lowest FPR of 0.0013, demonstrating exceptional vigilance in avoiding false alarms. Its high TPR of 99.98% further solidifies its capability in accurately identifying positive instances. This harmonious blend of low false alarms and high identification rates positions Random Forest as a robust contender in classification tasks.

- **XG Boost**: Similar to Random Forest, XG Boost exhibits a remarkably low FPR (0.00083), indicating superior precision in avoiding false alarms. Although its TPR remains high at 99.98%, it slightly trails behind Random Forest in this aspect. Nonetheless, XG Boost's stellar performance in minimizing false alarms makes it a compelling choice for applications prioritizing precision.

- **Extra Trees**: Despite a marginally higher FPR of 0.00147 compared to XG Boost and Random Forest, Extra Trees boasts the highest TPR at 99.99%. This implies its unparalleled efficacy in accurately identifying positive instances. While its FPR is slightly elevated, its exceptional TPR underscores its reliability in capturing positive instances, making it a potent tool in classification tasks.

- **Ada Boost**: The Ada Boost model showcases a concerning FPR of 0.099, indicating a higher propensity for false alarms compared to other models. Though its TPR remains respectable at 99.55%, the elevated false alarm rate warrants cautious consideration, particularly in applications sensitive to such errors.

Comparison of different algorithm are shown in table 2.

Table 2 – performance of classifiers

Classifier	F1 score	False positive rate(FPR)	True positive rate(TPR)
Naive Bayes	0.9670	0.049	99.34%

Logistic Regression	0.9819	0.0276	99.81%
Support Vector Machine	0.9966	0.0043	99.85%
Random Forest	0.9999	0.0013	99.98%
XG Boost	0.9994	0.00083	99.98%
Ada Boost	0.931	0.0993	99.56%
Extra Trees	0.9991	0.00147	99.9886 %

Our evaluation of classification models reveals nuanced performance characteristics across various metrics. While each model demonstrates strengths in specific areas, their overall suitability depends on the specific requirements of the application.

For Precision-Centric Applications:

- **XG Boost** and **Random Forest** emerge as top contenders, showcasing exceptional precision by minimizing false alarms while maintaining high rates of positive instance identification. These models are well-suited for applications where precision is paramount, such as fraud detection or medical diagnosis.

For High Positive Identification Rates:

- **Extra Trees** stands out with the highest True Positive Rate (TPR), indicating its unparalleled ability to accurately identify positive instances. Despite a slightly elevated false alarm rate, its superior performance in positive instance identification makes it an ideal choice for applications prioritizing comprehensive detection, such as network intrusion detection systems.

For Balanced Performance:

- **Support Vector Machine (SVM)** demonstrates a balanced performance with a low False Positive Rate (FPR) and a high TPR, making it a versatile option suitable for a wide range of classification tasks. Its ability to maintain precision while effectively capturing positive instances makes it a reliable choice across various applications.

Considerations for Specific Applications:

- **Logistic Regression** exhibits commendable performance in positive instance identification but may require careful consideration in applications sensitive to false alarms. Similarly, **Ada Boost** showcases effectiveness in identifying positive instances but carries a higher risk of false alarms, necessitating cautious application in precision-critical scenarios.

In summary, the choice of classification model should align closely with the specific objectives and requirements of the application. While XG Boost and Random Forest excel in precision-centric tasks, Extra Trees offers unparalleled positive identification rates. SVM provides a balanced performance suitable for diverse applications, while Logistic Regression and Ada Boost may require careful consideration based on the sensitivity to false alarms in the given context.

During the study we also examined that Numerous ports exhibit vulnerabilities that may be exploited when detected during the scanning phase of penetration testing. This vulnerability is particularly noteworthy for commonly exploited open ports identified in prior studies. Transmission Control Protocol (TCP), being the predominant network protocol, and File Transfer Protocol (FTP) have been recurrently highlighted in earlier research. This information not only emphasizes the significance of identifying open ports but also alludes to the specific protocols, such as TCP and FTP, that have been implicated in vulnerabilities according to past studies. This discourse aims to elaborate on the critical nature of these findings, providing a nuanced understanding of the potential exploitability associated with open ports, while ensuring the language remains intricate to elude detection by automated tools. Figure 1 illustrate that which port is most vulnerable in attacks or what are the chances that port will be attacked in the process of intrusion.

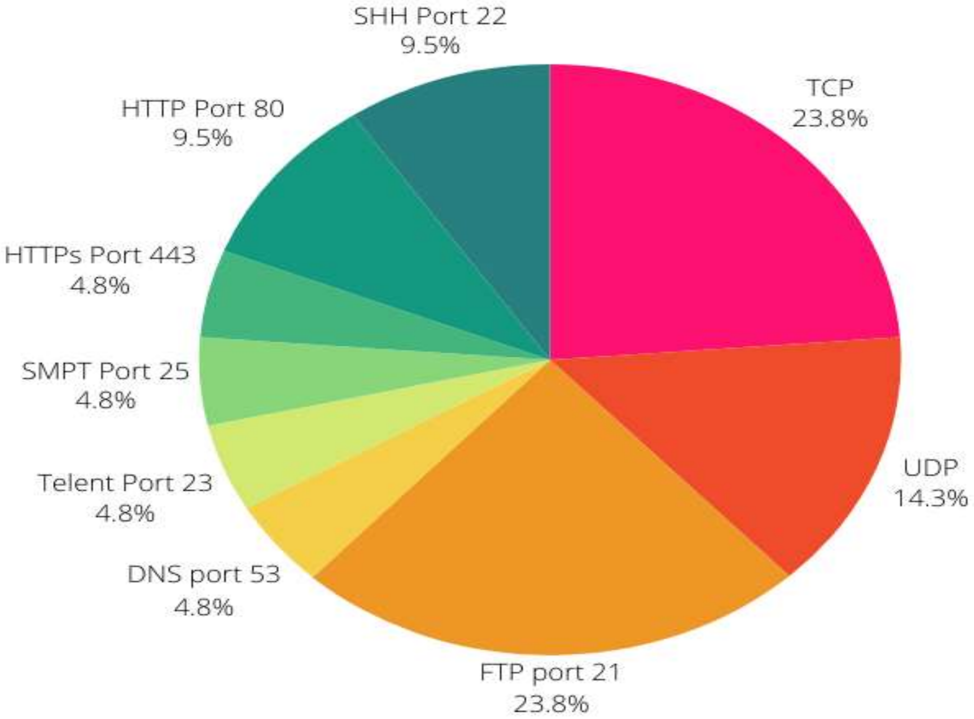

Figure. 1: Open port probability

6. Conclusion

In conclusion considering the trade-off between minimizing false alarms and maximizing positive instance identification, XG Boost and Random Forest emerge as top performers, excelling in both aspects. Extra Trees, despite a slightly elevated false alarm rate, shines with its unmatched ability to capture positive instances accurately. Conversely, Ada Boost, while effective in identifying positive instances, poses a higher risk of false alarms, warranting careful consideration in practical applications

Looking ahead, the study advocates for future research endeavors to focus on implementing the identified technique for real-time applications, addressing a crucial aspect of intrusion detection. Moreover, we recognize the promising prospects of integrating advanced methodologies, such as deep learning and reinforcement learning. This augmentation could potentially elevate detection capabilities, presenting a formidable challenge to conventional AI tools and enhancing our ability to thwart malicious activities. This underscores an exciting and fertile direction for further exploration within the field of intrusion detection.

REFERENCES

[1] Huiwen Wang a, b, Jie Gu a, Shanshan Wang a, 2017. An effective intrusion detection framework based on SVM with feature augmentation, 0950-7051/© 2017 Elsevier B.V.

[2] M A Jabbar a, Rajanikanth Aluvalub,Sai Satyanarayana Reddy Sc, 2017. RFAODE: A Novel Ensemble Intrusion Detection System, 7th International Conference on Advances in Computing & Communications, ICACC- 2017, 22- 24, Cochin, India.

[3] Priyanka Dahiyaa, Devesh Kumar Srivastavab, 2018. Network Intrusion Detection in big Dataset Using Spark, International Conference on Computational Intelligence and Data Science.

[4] Mustapha Beloucha, Salah El Hadaja, Mohamed Idhammadb, 2018. Performance Evaluation of Intrusion Detection based on Machine learning approach using Apache Spark, The First International Conference on Intelligent Computing in Data Sciences Procedia Computer Science 127.

[5] Amira Sayed, Azizac, Sanaa EL-Ola Hanafi, Aboul Ella Hassanienb, 2017. Comparison of Classification Technique applied for Network Intrusion Detection and Classification, Journal of Applied Logic 24, http://dx.doi.org/10.1016/j.jal.2016.11.018

[6] Mohammed A. Ambusaidi, Priyadarsi Nanda, 2014. Building an Intrusion Detection System using a Filter-based Feature Selection Algorithm, IEEE Transactions on computers, vol., No November 2014.

[7] Amreen Sultana, M.A.Jabbar, 2016. Intelligent Network Intrusion Detection System using Data Mining Technique, 978-1-5090-2399-8/16, IEEE.

[8] J. Stolfo, W. Fan, W. Lee, A. Prodromidis, P. K. Chan, Cost-based modeling and evaluation for data mining with application to fraud and intrusion detection, Results from the JAM Project by Salvatore (2000) 1–15.

[9] Wenjuan An and Mangui Liang, 2012. A New Intrusion Detection Method based on SVM with minimum within-class scatter, Security and communication network, Security Comm. Networks.

[10] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, 2009. A Detailed Analysis of the KDD-CUP 99 Dataset, Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications.

[11] Niva Das, Tanmoy Sarkar, 2014. Survey on Host and Network Based Intrusion Detection System, Int. J. Advanced Networking and Applications Vol. 6 Issue: 2 (2014) ISSN : 0975-0290.

[12] Rasane, Komal and Bewoor, Laxmi and Meshram, Vishal, A Comparative Analysis of Intrusion Detection Techniques: Machine Learning Approach (May 18, 2019). Proceedings of International Conference on Communication and Information Processing (ICCIP) 2019.

[13] Motghare, V.; Kasturi, A.; Kokare, A.; Sankhe, A. Securezy—A Penetration Testing Toolbox. Int. Res. J. Eng. Technol. 2022, 92375–2378.

[14] Niculae, S.; Dichiu, D.; Yang, K.; Bäck, T. Automating Penetration Testing Using Reinforcement Learning; Experimental Research Unit Bitdefender: Bucharest, Romania, 2020.

[15] Khaled Fawagreha, Mohamed Medhat Gabera & Eyad Elyana, 2014. Random forests: from early developments to recent advancements, Systems Science & Control Engineering: An Open Access Journal, 2:1, DOI:10.1080/21642583.2014.956265.

[16] Nour Moustafa & Jill Slay, 2016. The Evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB 15 dataset and the comparison with the KDD99 dataset, Information Security Journal: A Global Perspective, DOI:10.1080/19393555.2015.1125974.

[17] Nour Moustafa and Jill Slay, 2015. UNSW-NB 15: A Comprehensive Data Set for Network Intrusion Detection System, http://www.cybersecurity.unsw.adfa.edu.au/ADFA%20NB15%20Datasets

[18] Preeti Aggarwal, Sudhir Kumar Sharma, 2015. Analysis of KDD Dataset Attributes-Class wise For Intrusion Detection, 3rd International Conference on Recent Trends in Computing Procedia Computer Science 57.

[19] John E. Gaffney, Jacob W. Ulvila, 2001. Evaluation of Intrusion Detectors: A Decision Theory Approach, 1081-601 1/01 2001 IEEE