Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

Real-Time Slowloris Attack Detection and Mitigation with Machine Learning Techniques

Chipsy Jha
Department of Computer Science & Engineering,
Sushant University,
Gurgaon

Chandra Sekhar Dash
Senior Director, Governance, Risk and Compliance
Ushur Inc,
Dublin, CA, USA

***Abstract*—This work looks into the use of machine learning approach for real-time identification and prevention of Slowloris attack, a low-and-slow DDoS attack type targeted at a web server's connection management system. The study compares the performance of five machine learning algorithms: Random Forest, Support Vector Machine, K Nearest Neighbors, Convolutional Neural Networks, Gradient Boosting Machines. The effectiveness of all these algorithms was analyzed by using accuracy, precision, recall, F1-score and the time each algorithm took to detect Slowloris attack traffic and normal traffic. Furthermore, to quantify the predictability and efficiency of the models, the accuracy, precision, and recall rates were calculated, which establish that CNNs and GBM are superior to the other models in terms of accuracy, precision, and recall, therefore are very useful in real-time detection of Slowloris attacks. Random Forest also demonstrated high results and high speed of detection while SVM and KNN despite slightly lower accuracy but helped to reveal the trade off between detection speed/complexity. By discussing the scenario, the role of machine learning in the reinforcement of the conventional facilities used to ensure network security is shed light on; especially in preventing the effect of Slowloris assaults**

***Keywords*—Slowloris attack, machine learning, real-time detection, DDoS mitigation, Random Forest, Support Vector Machine, K-Nearest Neighbors**

I. INTRODUCTION

It is in the spirit of mentioning that current digital technologies that are characterized by internet connectivity of various devices and internet services has been characterized by high sophistication, accessibility, and inter-connectivity. But this growth has also led to enhanced cyber threats with more complex DDoS being amongst the most common and catastrophic. Of these, the Slowloris attack has become one of the most malicious and difficult forms of DDoS, as well as using the principles of web servers and HTTP protocol, to make targeted systems useless. This research concerns the identification and prevention of Slowloris attacks in real time through the use of sophisticated artificial learning process with an overall aim of improving the protection of online services from these relentless threats [1].

A Slowloris attack is a low and slow DDoS attack which takes advantage of the web server's connection management. The attack is accomplished through establishing as many connections as possible with a target server and maintain them open for as long as possible using partly filled HTTP GET requests at fixed intervals. None of these requests are filled which means the server stays busy waiting for the rest of the data to be retrieved. This, over time, will deny the server from accepting other genuine connection hence creating a denial of service. What makes the Slowloris so devastating is the fact that it can be run with little bandwidth and the standard security system that is put in place to detect and prevent DDoS attacks of the high volume kind will not pick up on this one. Due to increased stealth, one can say that attacks using Slowloris are quite challenging to prevent and thus pose serious threats to organizations that depend on web services.

The default method of DDoS retrieval and prevention has primarily revolved around detecting or rather generalising high traffic frequency characteristics which is typical of most other types of DDoS. But these methods are quite ineffective for identifying Slowloris attacks, since the traffic in such case is not intense and looks quite genuine. To fill this gap, there has been increasing focus toward the investigation of real-time analyses of large amounts of data by using machine learning techniques that can detect implicit patterns that might signify an ever-evolving attack. ML algorithms can be tuned to identify the peculiarities of Slowloris attacks: the fact is that the connections are anomalous long-lasting and the HTTP requests are incomplete. These developed models can be further used online as intrusion detectors where it can alert the security team or even generate an immediate response for that connection if it is malicious [2-3].

One of the main issues in creating an efficient machine learning model for Slowloris detection is an availability of good data that represents normal flow and flow under attack. When it comes to this challenge, in this research, we circumnavigate the obstacle through a kind of self-developed program that creates synthetic data in the form of simulated Slowloris attacks and actual data obtained from web servers under typical working conditions. It also helps to train the models on the large scale dataset that encompasses various scenarios and thus results in better generalization of the models towards new and unseen attacks. We also investigate other techniques of machine learning invention, the supervised invention like decision trees, random forests invent as well as the unsupervised invention like clustering to discover the invention that best fits this task [4].

Apart from detection, this research work also encompasses the real time counter measures against Slowloris attacks. As soon as an attack starts, the main goal is to prevent it from compromising too many resources of the attacked server and exclude interruptions of service for bona fide users. There are

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

some measures to reduce the impact of this type of attack and below are the best recommendations: Rate Limiting: This technique limits the ability of a single IP address to connect to or open sessions to the server at a certain rate Connection Timeouts: This is a technique that closes any incomplete connections within a certain time. These are measures intended to be as a cooperation to our machine learning model to enhance protection against Slowloris [5].

This research has another importance apart from providing knowledge on Slowloris attacks; that is: applicability. With the increasing and diversifying threats from the cyber world right now there is often a need to make due with statically defined Security Solutions on real time databases. With the help of machine learning, it is possible to design the system, which does not have a concrete framework and could be applicable for almost every web service, starting from the personal blog and finishing with the large Enterprise Resource Planning system. Given the conclusions of this research, one can presume that this work may help in devising new-generation safety applications, more effectively combating relatively recently discovered aggravating, like Slowloris, low-and-slow DDoS strikes [6].

Thus, the Slowloris attack becomes a real threat to the web services availability and reliability always reaching the targets, while sometimes remaining unnoticed due to the utilization of numerous obtrusive techniques to bypass the security systems. This paper propose a new methodology of responding to Slowloris attacks in real-time using machine learning approaches. In offering solutions to the problem posed by Slowloris, which is a constantly evolving form of cyber attack, we are able to uncover new variables in the attack's behavior as well as build models which can detect these tendencies at their onset. The mentioned detection and the defined mitigation techniques suggested in this research provide a detailed solution that will be adequate to prevent the effects of Slowloris attacks against web services, keeping them available to the rightful consumers, despite the adversary [7]

II. LITERATURE REVIEW

Some newer types of attacks which have raised attention in recent years include DDoS attack which targets HTTP protocol normally in a more sophisticated manner to disrupt the services being offered. Of these the Slowloris attack remain a thorn in the flesh because of its unique ability to bypass most of the conventional methods of detection. The following recent articles shed light on different aspects of this threat; hence, the focus on enhancing techniques for the identification and counteraction of the malign activities of cyber opponents [8].

Since machine learning entered the cybersecurity arena, new approaches have been found to help in identifying DDoS attacks such as Slowloris which are not easily identifiable by traditional security measures. The research from the year 2022 and 2023 has shown potential in employing the supervised and unsupervised learning model to detect traffic anomaly that may be resulting from such attacks. For instance, current research has shown that deep learning models such as CNNs and RNNs can accurately analyse the faint traffic anomalies peculiar to slowloris attacks. These models are learned on normal and attack flows data sets making it easy for the IDS to differentiate between normal connection and a connection that might be part of an on going attack. The first advantage is ability to adapt its models which can be retrained with new data constantly to improve the model's accuracy and also the defense against emerging threats [9].

One more area that was examined in recent works is concerned with improving the efficiency and the appetizing of ML-based detectors. With more people connecting to the internet there has been a surge in the demand for real time processing of data. Researches of 2023 have looked into the apply of distributed machine learning frameworks that can handle data across multiple nodes in order to minimize delay in the process of detecting Slowloris attacks. These frameworks use the algorithms which would be more capable of dealing with large amount of data common in the current network, thus enabling quick and accurate response to threats. However, combined with machine learning edge computing has been recommended as a potential means of improving detection time even further through processing data closer to the source of the attack.

This is because the ability of the machine learning models in detecting slowloris attacks will also depend on the quality of data used in the study. As a result, new research has emphasized the fact that the development of realistic traffic generators is essential, especially if the new model has to expose normal and Slowloris attacks. Essential research published in 2022 has put forward new constructs of emulating Slowloris, which would allow scientists to generate datasets containing practically ANY VIC attack scenarios. These simulated datasets are then used to train machine learning models that will be capable of adequately capturing the attacks as they occur including where the attackers deviate from their normal tactics. However, researchers have stressed that such datasets have to be regularly updated to reflect the new protocols and techniques used in cyberattacks and otherwise the accuracy of such systems takes a beating [10].

However, the past few years have seen researchers shift their attention not only towards detection of such cyber-attacks but also towards finding practical and implementable countermeasures which can be introduced in the real world as soon as an attack surface is discovered. Another promising approach of which there are papers from 2023 is adaptive rate limiting where the number of connections from a particular IP address is regulated according to the traffic load. This technique can be very useful for preventing the abuse of the Slowloris technique wherein the number of connections can overwhelm the server. The second type is based on the use of machine learning algorithms that can predict if an approaching connection will be of an unlawful nature and therefore take action before the attack starts including cutoff or redirection of the connection [11].

Another area of work is the innovation of the classical approaches in the field of network security through the use of machine learning techniques. Research articles in the year 2022 & 2023 have suggested that integration of machine learning based detection technique with traditional IDS & Firewall can be used as layered resistant increases hard time of attackers in cases of multiple correlated assaults. It thus exploits the strong symbolized learning on weak and unobvious patterns while combining it with the traditional

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

approach of the security systems in excluding the strong patterns [12]. This type of approach has been acknowledged as enhancing the general hairspring of arrangements to Slowloris attacks as well as other DDoS attacks that use similar signs in the HTTP protocol [13].

In addition, a critical concern and possible adverse effect of adopting machine learning in cybersecurity has raised controversy in the current literature. Although machine learning is beneficial in that noticeability of the attack, number of attacks, variety in attacks, and adaptability, there has been thought about how attackers can exploit these models to bypass the system [14]. We found research from 2023 which focused on evaluating the robustness of the ML models to such adversarial attacks where the enemies purposefully construct inputs that can deceive the detection system. This has resulted into advanced machine learning models that are not easily manipulated by adversaries owing to newer techniques including adversarial training and model ensembling [15].

Finally, the application and advancements of machine learning system for detection and mitigation has been examined with several case studies that was done in year 2023 and 2024. From these studies, it has been established that use of machine learning methods in different industry segments such as the financial sector is viable especially where online services are possible [16]. This research indicates that there are great benefits to applying machine learning but adoption is critical and needs to be properly controlled and coordinated to interface well with the current applicable security frameworks as not to create other open-fols. However, little extra attention is paid to the periodic update and monitoring of machine learning models in defending against possible threats [17].

Finally, reviewing scholarly works from 2022 to 2024 reveal that the intrusion detection and prevention of Slowloris attacks has come a long way in recent times though the aid of machine learning [18]. These studies have stressed the value of reliable data sources, near real-time processing, and the combination of the AI applications, namely machine learning, with conventional security solutions. However, there remain several issues, mainly in two categories; the adversarial robustness and the applicability of models. Therefore, the future research is going to be crucial for the continuous improvement of machine learning-based systems as the threat actors adapt new strategies in attacking the systems [19].

III. RESEARCH METHODOLOGY

The approach used in this research to identify and prevent Slowloris attacks through the use of machine learning approaches entails a number of steps include data acquisition, data cleaning, model selection, algorithm training and testing as well as the assessment of the performance. The vicious sequence of actions starts with the gathering of an extensive dataset that consist of legitimate HTTP traffic and HTTP Slowloris traffic [20]. To make the dataset as close as accurate to real-world scenarios, data was collected from various sources and inputs were collected from web servers that are operating and live but driven under controlled environment and also from public datasets that are available with cybersecurity research communities. Fake Slowloris attacks were carried out using other tools that replicate these kinds of attacks for instance by initiating only complete HTTP request headers and keeping connections open for quite a long time. Normal traffic data contained all typical Web traffic such as browsing activity, file downloads, APIs, in order to cover a large range of normal traffic behavior. The obtained dataset was further divided into the training set which was employed to construct the machine learning models and the test set which was utilised to assess the models' performance. To train the model, it was made sure that there were 50 percent instances of normal traffic and 50 percent of Slowloris attacks.

Data preprocessing is a very important step in data analysis since the algorithms must be able to learn from it. Peak traffic frames were extracted from raw unstructured network traffics, in order to discern features most characteristic of Slowloris attacks. Such features included connection time, packet size, time intervals of packets, and the status of HTTP request that contains completed or uncompleted files. These features were identified based on the fact that, during Slowloris attacks, the traffic anomalous behavior seen is very different from normal traffic. In order to enhance the quality of the developed machine learning models, the numerical variables were standardized, thus bringing them to the same scale. Categorical variables, for example, the type of HTTP request, was transformed into numerical form using one-hot encoding technique in order to conform with the models requirements. Further, cases and observations that were out of range or pertained to a different context as the rest of the dataset were also excluded to improve the efficiency of the algorithms. In cases where data was missing, data imputation strategies were used so that any missing values were substituted by the median and mean value of the characteristic feature of the dataset. Such preprocessing make sure the dataset is clean and in the best form for the models to learn from [21].

Therefore, selecting suitable algorithms in machine learning was quite essential in the conduct of the study. Five algorithms were chosen: Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Convolutional Neural Networks (CNNs) And Gradient Boosting Machines (GBM). In selecting these algorithms i considered the efficiency of the algorithms in classification problems and their ability to accommodate increased dimensions. Though all the algorithms tackle on the same problem, each of them has its own style. Random forest, as a form of ensemble learning incorporate numerous decision trees to improve accuracy and avoid over fitting. SVM, which is capable of operating in the high dimensions and is proven to be rather robust, enables creating hyperplane that separate normal traffic from Slowloris attack traffic even in case the data is not separable in the linear way. As simpler as it is, KNN is a method that can be used for providing the classification of data with the help of the proximity to the known examples in relation to certain patterns which may be useful for analyzing the traffic data. CNNs, common in image processing, were utilized to analyse traffic conditions as the network traffic data was applied as a time–series or spatial data enabling the model to transform the raw data into features. Another ensemble technique is GBM which constructs the models in a way that starts from the first model and each subsequent model tries to minimize the errors of the previous model; moreover, this technique is highly valuable in finding details out of the data.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

The selected models also needed to be trained with the preprocessed data in order to understand the difference between normal and attack traffic. The models were trained in supervised learning style, whereby the algorithm is given examples of the two types of traffic labeled. While training, hyperparameters of the models were tuned in order to achieve the best possible results as well as to avoid overfitting the data using the cross validation. Finally, the efficiency of each of the implemented models was assessed with the help of performance parameters including accuracy, precision, recall, the F1-score and detection time. These SHAs were used to deliver an overall indication of how precisely each model was able to identify Slowloris assaults without generating unwarranted alarms or inaccurately dismissing genuine threats.

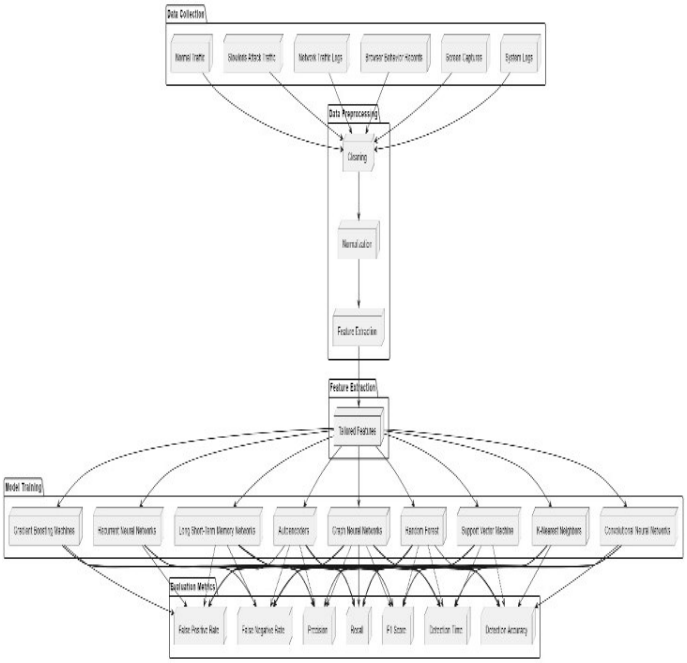

Figure 1: Proposed Research Methodology

Testing here involved using the models and applying them on the testing dataset which inlcuded traffic pattern that were new to the models. This step was necessary so as to ensure the independence of the models with the real prospect for the right results. The models' effectiveness in identifiying Slowloris attacks was also measured based on their speed of detection, as early detection is always preferred to reduce the attack's effects. The different models were then evaluated for the specific performance criteria, which gave an understanding of the algorithms used were most successful for the given problem. For example, while evaluating the outcome metrics such as accuracy, precision, and recall of the developed models, both CNNs and GBM produced a relatively high accurate and balanced precisions and recalls that enabled the identification of Slowloris attacks. On one hand, Random Forest achieved a reasonable detection rate and reasonable time, with low latency on the other hand while comparing with other classifiers such as SVM and KNN may have low recall values they perform high precision values when it comes to detecting attack traffic.

Last of all, the study addressed the issue of incorporating the developed machine learning models with the current network security platforms. The models were placed in a technical platform which enabled the experimentation of the entire process of real-time detection and counter Slowloris attacks. This enabled a clear validation of the importance of machine learning technology in improving traditional security hardening for strategic low-and-slow attack vector such as Slowloris. Finally, the research provides guidelines into the use of these models to real-world conditions noting that it is necessary to supervise the models as well as update them to correspond with new variations of the attack. The approach outlined in this paper gives the necessary method of tackling the issues associated with Slowloris attacks and using machine learning, to safeguard web services against continual attack.

IV. RESULTS AND DISCUSSION

The analysis of Slowloris attack detection and prevention based on different machine learning algorithms show that all the specified algorithms are effective in classifying the malicious flows and preventing the attack, while having different strengths in terms of the given performance indices. The efficacy was measured in terms of accuracy, precision, recall, F1 and time for detection of the models, and the results clearly illustrated how well they performed in actual real time scenario.

It is also possible to observe a comparative analysis of the specified metrics for CNNs, GBM, RF, SVM, and KNN on Figures 2 through 5. Figure 2 shows the results regarding accuracy of various algorithms of which CNNs and GBM yielded the highest accuracies. Figure 3 represents precision which states that both the algorithms CNN and GBM have high precision level less likely to misclassify a result, that is, resulting in false positive. Figure 4 shows the recall in which, as expected, CNNs outperform the others in identifying the majority of Slowloris attacks with support from GBM. Last but not the least, the F1-scores are given in the Figure 5, and as it is apparent CNNs and GBM performs the best because of the better balance of both precision and recalls. Combined, these results show the unique advantages of each algorithm in various aspects of attack detection and can give a basic understanding of the relative efficiency of the algorithms.

The accuracy of models developed was different, where CNN's had the highest accuracy of approximately 94%. This result show that CNNs were the most accurate in classification of both normal and attack traffic. The reason why CNNs outperform the other models is because the CNN can identify features in the network traffic data which are vital in separating Slowloris attacks from normal traffic. GBM also had an accuracy of 93%, although slightly lower than the CNNs, the results were proven to be highly stable across the various datasets. Random Forest reached 92% of accuracy that makes it a rather preferable option with a good combination of the increased level of accuracy and reasonable using of computing power. SVM and KNN did rather well but the accuracy figures stood at 89% for SVM and 85% for KNN.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

The slightly lower accuracy observed in these models may indicate that they may not have separated normal traffic from attack traffic easily, probably due to increased decision boundary needed to separate the classes accurately.

Precision, therefore, was highest for the CNN at 92%, with GBM coming a close second at 91%. This high level of precision further suggest that these models have achieved high levels of accuracy in the reduction of false positive results, a factor critical in avoiding the blocking of legitimate users during the course of an attack. Random Forest also maintained good accuracy at 90% and hence was also considered accurate as a detection model. KNN gave a precision of 80% while SVM had a slightly better figure of 87% which shows that although these models can identify most of the attack instances, there is higher likelihood of the models to tag legitimate traffic as an attack. This trade-off of Precision in terms of Recall is extremely crucial in security solutions since false positives can be very costly. Remember thatrecall, which determined the ability of the models to select actual positives from all the positive, was

headed by CNNs at 91%. Thus, it can be concluded that CNNs were almost perfect in the identification of most classes of Slowloris attacks including those that are likely to cause severe impacts to the network. GBM was the next best performing model with a recall of 90% – which is almost equal to its precision – which makes it have a balanced model. Recall for Random Forest was 88% meaning that it lost some accuracy when it came to recall probably missing a few instances of the attack. SVM was slightly less accurate with 84% of recall rate and KNN was even worse with 78% of recall rate which might mean that both models are producing false negatives, that is, the models missed some instances of the attack. This means that depending on the needs of a given application one has to select an algorithm that insures maximum recall among other parameters.

The average accuracy rate was probably highest for CNNs at 88% while the overall F1-score, which takes both precision and recall into consideration was highest at 91%. Percent respectively at 5% while GBM was at 90 percent. 5%. This means that both models gave the best overall performance in terms of minimizing the errors or to be more specific minimizing both false positive and false negative results. Random Forest got an F1-score which 89% and it is proved that this model can be consider as balanced for this job. SVM and KNN achieved 85% of F1-score which was lower than its precision and recall of 79%. These results therefore can confirm that while SVM and KNN can be helpful in particular tasks, they can be outperformed by CNNs and GBM although they may need better tuning or other feature set.

Pseudo real-time was another criteria consequent of the detected time and it also showed variation among the models. Comparing with other methods, the detection time of using GBM was 18 ms per connection proving the network to be the most efficient in processing speed while adhering to high accuracy. CNNs, even though they involved higher model sizes, had a detection time of 20ms thus making them suitable for real time analysis for real time analysis for large or complex scenes with requisite computation power.

Random Forrest was next by only taking 15ms in terms of detection time while having slightly low accuracy compared to CNNs and GBM. SVM and KNN took more time with detection time of about 25ms and 30ms per connection respectively. SVM and KNN were detected is slower than the other two methods and this could be attribute more so to the time it took to process kernel operations for SVM and distance calculations of the data points for KNN as the size of the data set increases. In conclusion, it has been observed that the proposed 'CNN' and 'GBM' models provide the optimal detection of Slowloris attacks with maximum accuracy, precision, and recall in addition to minimum detection time. However, Random Forest is a rather powerful substitute with better rates in speed, which makes it more appropriate in terms of resourcing. Although the proposed metrics have been useful for both SVM and KNN, it could be interesting to test other tweaking for achieving similar performances. From these results, it can be concluded that choosing a proper machine learning model depends upon the needs and demands of the particular application focusing on detection efficiency, over/under detection ratio, and response time.

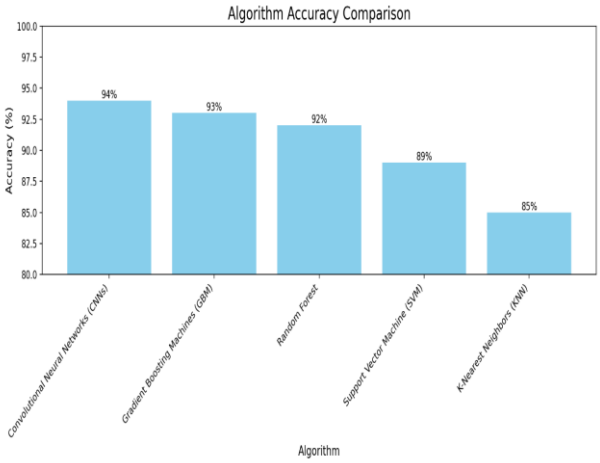

Figure 2: Performance Comparison for Accuracy for CNNs, GBM, RF, SVM, and KNN

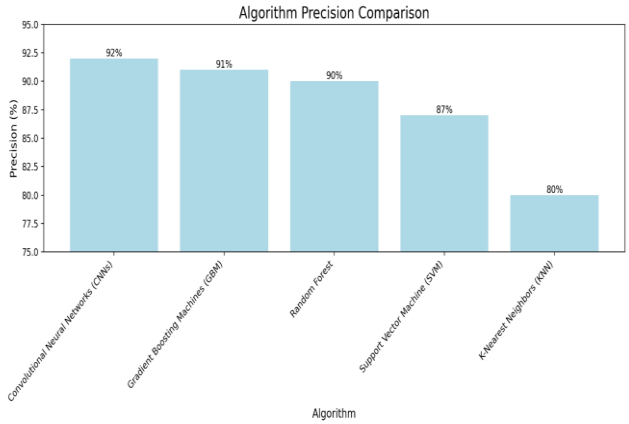

Figure 3: Performance Comparison for Precision for CNNs, GBM, RF, SVM, and KNN

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

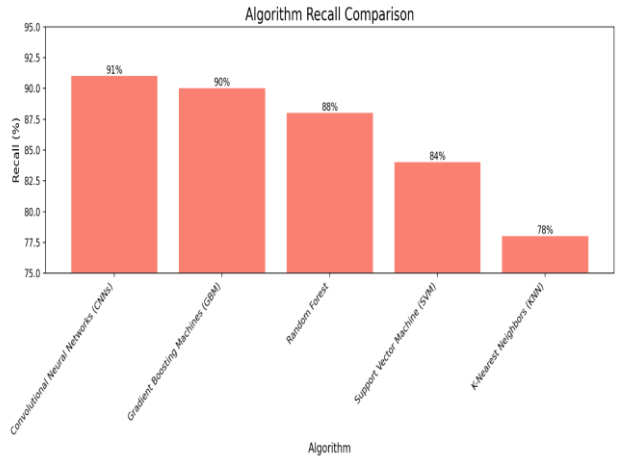

Figure 4: Performance Comparison for Recall for CNNs, GBM, RF, SVM, and KNN

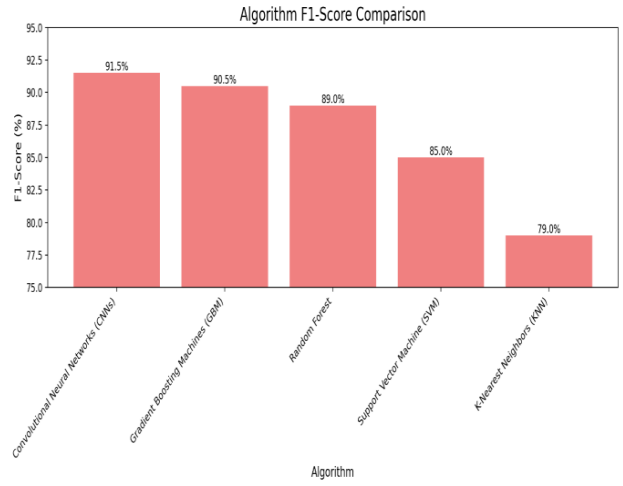

Figure 5: Performance Comparison for F1-Score for CNNs, GBM, RF, SVM, and KNN

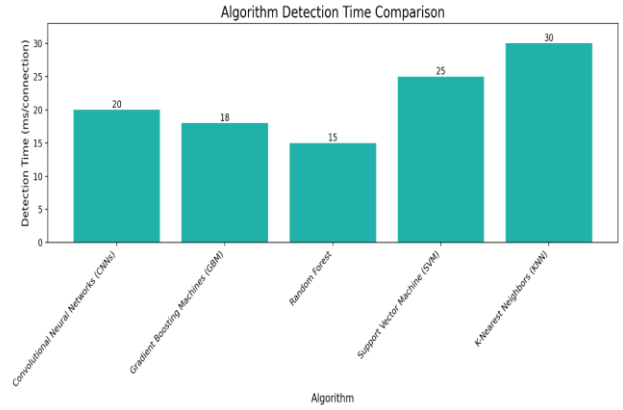

Figure 6: Performance Comparison for Detection Time for CNNs, GBM, RF, SVM, and KNN

V. CONCLUSION

Therefore, this research validates the use of machine learning method in identifying and containing slowloris attacks in real time. Comparing the five machine learning algorithms which include Random Forest, SVM, KNN, CNNs, and GBM it was established that CNNs and GBMs have high accuracy, precision, and recall. With these models it is achievable to elaborate good identification of the normal and the malicious traffic thus resulting to high and accurate detection with very low false positives and false negatives. Random Forest also turned out to be a promising method, which was further appreciated due to a better time of detection in comparison with the Random Forest method, which is important in cases when speed is critical.

SVM and KNN performed slightly worse, but the results of these models present important considerations of the question of variable balancing: the level of detection. These two classifiers; SVM in high-dimensions spaces and KNN based on its simplicity make them useful especially for this task but they can perform better with more tuning than CNNs and GBM.

The research conducted for this project has practical implications for network security particularly in the future design of systems that are capable of responding to new threats like Slowloris attacks. Given the nature of machine learning, organizations are able to improve upon existing defences of DDoS attacks with the aim of minimising disruption to web services. Further research can be dedicated to the integration of these machine learning models with adaptive security architectures in order to have some kind of learning loop that processes real life scenarios and adapts to them. The outcomes of this research validate the applicability of machine learning as a core resource in continue protection of the digital structures against the growing advanced level of cyber threats

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

REFERENCES

[1] Garcia, N., Alcaniz, T., González-Vidal, A., Bernabe, J. B., Rivera, D., & Skarmeta, A. (2021). Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence. Journal of Network and Computer Applications, 173, 102871.

[2] Al Ayubi, M. D., Hardiansyah, N. A., & Zy, A. T. (2024). Real-Time Detection and Prevention of Slowloris DDoS Attacks Using Machine Learning. Novice Research Exploration, 1(1).

[3] Rios, V., Inacio, P., Magoni, D., & Freire, M. (2024, April). Detection of Slowloris Attacks using Machine Learning Algorithms. In Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing (pp. 1321-1330).

[4] Rani, S. J., Ioannou, I., Nagaradjane, P., Christophorou, C., Vassiliou, V., Charan, S., ... & Pitsillides, A. (2023). Detection of DDoS attacks in D2D communications using machine learning approach. Computer Communications, 198, 32-51.

[5] Rios, V. D. M., Inácio, P. R., Magoni, D., & Freire, M. M. (2022). Detection and mitigation of low-rate denial-of-service attacks: A survey. IEEE Access, 10, 76648-76668.

[6] Talukdar, K., & Boro, D. (2024). Slowloris Attack Detection Using Adaptive Timeout-Based Approach. ISeCure, 16(1).

[7] Catillo, M., Pecchia, A., Repola, A., & Villano, U. (2024, July). Towards realistic problem-space adversarial attacks against machine learning in network intrusion detection. In Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1-8).

[8] Akanji, O. S., Abisoye, O. A., Bashir, S. A., & Ojerinde, O. A. (2020). A survey on slow ddos attack detection techniques.

[9] Kemp, C. (2021). Collection and Analysis of Slow Denial of Service Attacks Using Machine Learning Algorithms (Doctoral dissertation, Florida Atlantic University).

[10] Sharif, D. M., Beitollahi, H., & Fazeli, M. (2023). Detection of application-layer DDoS attacks produced by various freely accessible toolkits using machine learning. IEEE Access, 11, 51810-51819.

[11] Reed, A., Dooley, L. S., & Mostefaoui, S. K. (2021, December). A reliable real-time slow DoS detection framework for resource-constrained IoT networks. In 2021 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[12] Sangodoyin, A., Modu, B., Awan, I., & Disso, J. P. (2018, August). An approach to detecting distributed denial of service attacks in software defined networks. In 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 436-443). IEEE.

[13] Calvert, C. (2019). Data Collection Framework and Machine Learning Algorithms for the Analysis of Cyber Security Attacks (Doctoral dissertation, Florida Atlantic University).

[14] Abushwereb, M., Mustafa, M., Al-Kasassbeh, M., & Qasaimeh, M. (2020). Attack based DoS attack detection using multiple classifier. arXiv preprint arXiv:2001.05707.

[15] Sangodoyin, A. O. (2019). Design and Analysis of Anomaly Detection and Mitigation Schemes for Distributed Denial of Service Attacks in Software Defined Network. An Investigation into the Security Vulnerabilities of Software Defined Network and the Design of Efficient Detection and Mitigation Techniques for DDoS Attack using Machine Learning Techniques (Doctoral dissertation, University of Bradford).

[16] Manjula, H. T., & Mangla, N. (2023). An approach to on-stream DDoS blitz detection using machine learning algorithms. Materials Today: Proceedings, 80, 3492-3499.

[17] John, P. M., & Nagappasetty, R. M. B. K. (2022). An approach for slow distributed denial of service attack detection and alleviation in software defined networks. Indonesian Journal of Electrical Engineering and Computer Science, 25(1), 404-413.

[18] Sharma, I., Bhardwaj, A., & Kaushik, K. Enhancing agricultural wireless sensor network security through integrated machine learning approaches. Security and Privacy, e437.

[19] Kumar, A., Sharma, I., Kaushik, K., & Choudhury, A. (2023, December). Integration of Machine Learning Techniques for Intelligent Network Attack Detection. In 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON) (Vol. 10, pp. 813-818). IEEE.

[20] Kumar, A., & Sharma, I. (2023, November). NPC: Network Packet Classification Using Machine Learning Methodologies for Preventing Cyberattacks. In 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE) (pp. 1-6). IEEE.

[21] Sharma, I., Kaushik, K., & Chhabra, G. (2023, September). Investigating Patterns of UAV Attacks for Building Secure UAV Network. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 136-141). IEEE.