International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-12, Issue-5 September 2024
https://doi.org/10.55524/ijircst.2024.12.5.7
Article ID IRP-1556, Pages 47-55
www.ijircst.org

Detecting and Preventing ARP Spoofing Attacks Using Real-Time Data Analysis and Machine Learning

Mrinal Kumar[1], and Chandra Sekhar Dash[2]

[1] School of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar, India
[2] Senior Director, Governance, Risk and Compliance, Ushur Inc, Dublin, CA, USA

Correspondence should be addressed to Mrinal Kumar; infinityai1411@gmail.com

Received 19 August 2024; Revised 2 September 2024; Accepted 16 September 2024

ABSTRACT- ARP spoofing attacks contain certain risks in networks as they seem to intercept traffic and can lead the leakage of intellectual information. This research paper focuses on enhancing the method through which five algorithms namely: Random Forest, Long Short-Term Memory (LSTM) Networks, Convolutional Neural Networks (CNNs), Support Vector Machines (SVM) and Isolation Forest for ARP spoofing detection and prevention. In the process of the experiment, each algorithm is tested with the dataset of ARP traffic and the results are compared on the five criteria: of data; these are accuracy, precision, recall, F1-score, false positive rate, and the false negative rate. It can therefore be deduced that out of all the algorithms employed, Random Forest has the highest accuracy of 94 and high values of precision and recall thus making it more efficient in real-time ARP spoofing detection. Its effectiveness is equally high as the effectiveness of LSTM Networks and CNNs, which process temporal or spatial data, but work longer. SVMs are comparatively not bad in terms of accuracy to noise ratio, however, they are less accurate as compared to both Random Forest as well as CNNs. This method however lacks good accuracy and has high error values as portrayed above with Isolation Forest. Based on this analysis, conclusions are made that use of higher levels of ML leads to the detection of ARP spoofing implementing Random Forest as the best solution for enhancing the network security.

KEYWORDS- ARP spoofing, machine learning, Random Forest, Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNNs), Support Vector Machines (SVM).

I. INTRODUCTION

As the number of network devices surges over the recent years, the size and topology of network has become more complex where makes it more susceptible to cyber threats. A specific hazard identified is ARP spoofing, a specific type of attack whereby an attacker transmits fake ARP messages over a local area network. It involves the process of redirecting traffic meant for a particular host, to the MAC address of the attacker while at the same time having the respective IPs. Such redirection may result in many threatening situations like interception of data, man-in-the-middle attack or denial of service attack. Because the consequences of ARP spoofing attack are so catastrophic, the identification and prevention of such attacks has become one of the major concerns of the network security industry. Most of the methods used in the past to prevent ARP spoofing have used static and merely reactive strategies, mainly before and during an attack by mere monitoring and the use of simple detection instruments. Although such solutions can provide some degree of protection, they are hardly efficient in complex and unpredictable network settings. Static ARP entries, as is stated above, are non-scalable solutions, which require much time and efforts to manage all the changes and updates. Furthermore, there are network security tools that monitor the network traffic for the presence of the attack patterns, and, as such, are reactive in their nature and cannot be modified with the attack patterns' evolution or network conditions frequently [1].

To overcome these limitations, researchers and practitioners have started adopting sophisticated methods mostly based on processing real time data and using machine learning. For instance, Machine learning has already exhibited a good deal of potential in enhancing the identification and mitigation of ARP spoofing attacks. With the real-time data collected, application of the machine learning approach, potential ARP spoofing attacks can be easily detected faster than with normal method.

A major benefit that can be obtained by applying machine learning in ARP spoofing detection is in its capacity to adjust to new and existing threats based on analyzed past instances. The supervised, unsupervised and reinforcement learning algorithms can be taught on large amount of data where the patterns characteristic of ARP spoofing can be discerned. For example, supervised learning models can be trained on the some labelled dataset that contains instances of ARP spoofing in order that the model can recognize new datapoints as either belonging to the legitimate or the suspicious category. While unsupervised learning can be used to find patterns in network traffic without having a prior knowledge of what constitutes an attack it is especially good at identifying new kinds of threats [2-3].

That is why it is possible to conclude that using actual-time data analysis improves the efficiency of machine learning based detection systems. Supervisory control of all the traffic within the network means that the system gathers data and does an analysis of all the traffic immediately allowing the system to check for the ARP spoofing attacks as they are being launched. In addition to enhancing the speed of detection it also contracts period of time that an

attacker is able to infiltrate a network. To counter ARP spoofing, the network security systems can incorporate real-time data into the machine learning models and hence offer efficient defense approaches [4].

However, new possibilities of using machine learning together with real-time data analysis for enhancing the detection mechanisms can also be presupposed. For instance, ensemble learning approaches, whereby a set of predictors are built and their outcomes are combined to arrive at a final decision, improves the detection systems by providing different views of network traffic. Moreover, feature engineering that constitutes feature selection from the network data to create features relevant to the learning model will enhance the performance of the algorithms. When using those features involved in training and detection, researchers are able to capture certain slight characteristics that have been associated with ARP spoofing attacks [5].

However, a number of challenges persist despite the research done towards the use of machine learning for detection and prevention. One major concern is the scarcity and quality of datasets in particular large and diverse dataset for training and testing the model. Machine learning model relies a lot on the data fed to it during learning process and it is often tasking to obtain relevant big data that represents the actual real-time network environment. Further, some of the issues associated with machine learning are related to the computational overheads and resources that can be taxing on machines especially for large and complex networks with heavy traffic loads [6].

The fourth is the issue of adversarial attacks that could be directed to the ML models themselves. As with any technique of intrusion detection, there may also be methods that attackers develop to avoid being flagged by the machine learning and come up with better spoofing tools and methods that are difficult to detect. Therefore, the need for natural updating and refining of defined models can never be overemphasized as this assists the researchers in combating new and emerging threats that may have not been captured in previous study [7].

Therefore, in this study, the real-time data analysis and machine learning have been effectively employed to address the issues of ARP spoofing detection and prevention. Hence, through the exploitation of these technologies, the network security systems can deliver more flexible, responsive and precise protection from this constant threat. Nevertheless, continuous efforts are required in system development and innovation in order to overcome data quality issue, high computational requirement, and adversarial attack issues. Thus, even at the present time, worrying changes in the network environment demand the use of sophisticated techniques to defend the networks' integrity.

II. LITERATURE REVIEW

From the literature survey conducted ARP spoofing detection systems, it has been identified that it has become a colorful field of research in the last one decade and more particularly in the last five years with the advent of real time big data analytics and use of machine learning techniques. In the current year 2022, 2023 and 2024, authors has presented different methods from the studies that have been conducted to enhance the efficiency of the ARP spoofing defense strategies.

As far as we know, the work conducted by Zhang et al. in February 2022 is the first one which presented a novel method, which is capable of identifying ARP spoofing attacks in an efficient manner with the help of CNNs integrated with the real-time network monitoring. As it was demonstrated, if CNNs are employed then it is possible to train a model that learns spatial hierarchies from network traffic data for detecting complicated patterns associated with ARP spoofing. The researchers revealed the advantages of online learning to process data in real-time and another factor is that the model can easily update its parameters whenever there is a new attack method that has not been programmed into the model. Their approach achieved high detection accuracy and very low false positive rate, which squarely sets it as the new bar of gold standards This research expounded the opportunities that deep learning architectures can bring in the prevention of ARP spoofing [8].

Similarly, another research conducted by Kumar & Patel (2023) titled on 'A Novel Approach towards ARP Spoofing Detection Based on Recurrent Neural Network- Long Short Term Memory'. Since RNN works on the temporal characteristics of the network traffic, the researchers said it is proper for capturing quickly successive dependencies. They opined that the proposed methods of LSTM networks would allow them to detect unknown patterns of ARP traffic which other methods fail to detect them. It also emphasized that feature engineering is crucial in that a particular feature selected will enhance the model's performance. This work proved that there are new patterns in attacks and temporal connectivity is needed in models [9-10].

In their study, Singh and Mehta identified several techniques in the use of ML in network security in a detailed survey they conducted in 2023 taking a good focus on ARP spoofing. The review included the data from several studies carried out on the given approach from Random Forests and Gradient Boosting Machines. According to Singh and Mehta , ensemble methods are better in detections since as the different models combine the models have the strengths of the other model but lack of the other. It also contained drawbacks of the real-time implementation such as computational cost and features extraction techniques. From this review, I got to be able to distinguish different approach to the machine learning technique and gained useful knowledge about the practical application in defending ARP spoofing attacks [11].

We could not find any earlier work on hybrid machine learning and network behaviour analysis for ARP spoofing detection and Chen et al. presented this concept in their paper in the year 2024. As a result of this, there techniques married supervised machine learning with unsupervised anomaly detection techniques which did turn out to be advantageous. The supervised component was trained using the labeled attack data while the unsupervised part adopted the features that were learnt from normal network traffic to identify anomalies. Consequently, it can be concluded that the developed hybrid model achieved the highest performance for the detector rate and the elimination of false alarm in the system having multiple inputs with wide varieties of types of analytical methods. Chen et al. has also examined the impact of different types of features to the models performance where including the network traffic

and the previous activity data also enhanced the detection accuracy [12].

There was followed by another interesting article of Patel et al. (2024) where authors implemented reinforcement learning in ARP spoofing prevention. The machine learning approach that the researchers employed was an adaptive defense mechanism that employs the most successful response strategies from feedback that is received from the environment. This also depicted that their reinforcement learning model was dynamically adapting the approach it adopted in order to reduce the impacts of ARP spoofing attacks. It talked about the application of reinforcement learning to formulate a method which is more efficient and quicker to implement in identifying threats then block them because this form of learning is sensitive to new signals of threat. The current study helped fill this gap by demonstrating the role of context when transferring new learning approaches to a real-time prevention setting [13-14].

Other scholars have also highlighted drawbacks that have been encountered in such methods this include data quality and computational cost. Another work done by Liu and Wang, a study conducted in 2024, focused especially on the method of feature selection towards improving effects of machine learning algorithms applied with ARP spoofing detection. The parties of the study also indicated that feature selection and dimension reduction types may enhance efficiency and effectivity of the model. Liu and Wang also emphasized on the issues related to the increase in model complexity as well as the computational load and provided constructive advice on how such machine learning based detection systems should be implemented in real world scenarios [15].

Thus, it can be concluded that published in 2022 to 2024 years, they focus on the shift of the machine learning method and real-time data analysis to combat ARP spoofing threats. Such additions of deep learning, temporal analysis, ensemble method, hybrid models, and recently reinforcement learning have enhanced the detection rate and flexibility of the system. However, concerns such as the data quality, demand of computational power, and self-sustaining articulation of attacks are still alive and compels the researchers to look further into this field. In total it is possible to conclude that the recent studies show the potential of ARP spoofing defense mechanisms usage of the advanced analytical assistant, including the prospect of the creation of much more effective security systems [16-17].

III. RESEARCH METHODOLOGY

The steps that constitute the machine learning research methodology in the context of detecting and preventing ARP spoofing attack include data collection, pre-processing, training, and model evaluation (see figure 1). This approach will be conducted more scientifically and systematically to measure the performance of the multiple machine learning algorithms such as Random Forest, Long Short-Term Memory (LSTM) Networks, Convolutional Neural Network (CNNs), Support Vector Machines (SVM) and Isolation Forest [18].

According to the results presented in this research paper, figures has been utilized to give a clear and quantitative comparison of the number of false negatives and true positives in ARP-spoofing among the different machine learning algorithms. In figure 2 to compare the accuracy of the Random Forest and other algorithms such as CNN, SVM and Isolation Forests, it was found that Random Forest emerged as the most accurate one. Dentification of precision the same algorithms as the figure 3 and depicting Random Forest as the winner. That is why recall rates are illustrated in Figure 4, which shows that both Random Forest and CNNs perform well in identifying true positives. In addition, Figure 5 depicts F1 score for each algorithm and shows that Random Forest is balanced between precision and recall. The false positive and false negative rates are presented in figures 6 and 7 both of which indicate that the Random Forest provides the least error rate. Figure 8 below shows the time taken to train each of the models, while figure 9 below shows a comparison of inference times also, Isolation Forest is the most efficient. All of these figures together help in finding out the positive and negative features of each algorithm, which is highly useful for implementing the same into practice for real-time detection of ARP spoofing attacks [19].

The first process to perform in the methodology is data collection process. Network traffic samples are captured from a given network identity that is composed of both genuine ARP request and responses, and ARP spoofing attacks. This dataset should be all inclusive and should contain all kinds of attacks imaginable to enhance the model's stability. Network packet capturing and logging of information include source/destination IP/MAC address along with ARP request/response types. For this reason, the dataset should include various conditions of the network of interest like different levels of traffic intensity and different topology of the network [20].

However, after collecting the data you need to preprocess it so that it is ready for further analysis. This step involves data cleaning for removing unnecessary features, missing data and scaling them to same scale of numeracal features. For ARP spoofing detection, preprocessing also involves features extraction in which different features like frequency of ARP request, the ratio of unique MAC addresses to the IP address, the time interval of ARP packets among others are extracted. Feature selection techniques are then used to determine the important features for use in developing the machine learning models. This step is important to help in dimensionality reduction in an endeavor to be able to increase the performance of the algorithms.

The next procedure is the splitting of the dataset into three categories of sets which include the training set validation set and the test set. Usually the dataset is split 80/10/10 where 80% is used for training, 10 % for the validation set and the remaining 10% of data is earmarked for testing. Training set is employed to fit the machine learning models and the validation set is utilised to optimise hyperparameters and select the best parameters configuration. The test set is therefore used to measure the 'out of sample' prediction accuracy of the final model.

For every of the machine learning algorithms, the training process is a sequence of steps that are to be executed. For Random Forest a number of decision trees are generated using bootstraps of the training data and the results of individual trees are averaged. The use of cross-validation is applied in making the appropriate decisions about the hyperparameters such as the numbers of trees and the maximum tree depth permitted. The characteristics of

Random Forest that will allow it to work well for ARP spoofing detection include its ability to deal with high-dimensional data as well as the ability of the algorithm to capture interactions between the features in the dataset.

LSTM Networks training in the case of our model consists of specifying the number of the LSTM layers, number of units within each layer, as well as the dropout rate. The analysis also reveals that LSTM networks are well suited for applications with sequential values and therefore the ARP traffic input is transformed into sequences. It is learned by backpropagation through time and optimised by such methods as Adam or RMSprop. How well LSTM networks perform is discussed by comparing their anomaly detection performance in conjunction with time series data.

Other artificial neural network models used are the Convolutional Neural Networks (CNNs) in which the network traffic data is in a format of grid or images. The CNN used to extract spatial features of the data through convolution stages that are followed by some pooling stages. Parameters includng the size of the filter, the number of filters, type of pooling are tuned on a validation set. CNNs are assessed concerning their capability in identifying characteristics of the ARP spoofing attacks.

This work employs Support Vector Machines known as SVM to differentiate ARP traffic as either legitimate or spoofed ones. In this context, the SVM algorithm is learnt with intention of identifying the correct hyperplane that would best separate the classes within the feature space. The type of kernels like linear or radial basis function (RBF) kernels is chosen during the classification phase in order to upscale classification performance. SVM's performance is then evaluated entailing the algorithm's precision, recall, and accuracy in classifying ARP spoofing attacks from normal traffic.

The Isolation Forest technique which is suitable for anomaly detection is trained by isolating the observation using random sub-sampling of features and split the data. The algorithm builds isolation trees, creates the forest of isolation trees and then infers the anomalies from the path distances of the trees. Parameters like the number of trees and the sub-sample size are set so as to extract the best performance out of the model. Since Isolation Forest aims at detecting ARP-based anomalies while minimizing on false positives, the algorithm's performance is assessed based on its accuracy in classifying anomalous ARP traffic.

These are accuracy, precision, recall, F1-score, false positive rate and false negative rate are used to assess the performance of each model. These metrics can be used as an overview of how well each algorithm works to identify ARP spoofing attacks. Moreover, the time complexity analysis of each model is looked at through training and inference time to determine feasibility in real-life problems.

The last step of the methodology is the comparison of approaches of every algorithm to find the best way to detect ARP spoofing. Comparing to the above methods, the comparative analysis takes into account not only the detection accuracy, but also the trade-off between precision and recall together with computational cost. This research uses the data analysis findings to draw learn how to design and implement machine learning based ARP spoofing detection systems in real world network settings.

This way of approach guarantees thorough examination of various machine learning algorithms used in ARP spoofing detection and reveal their advantages and shortcomings. The outcomes that will be used will assist in the growth of efficient and flexible means of protecting the network.

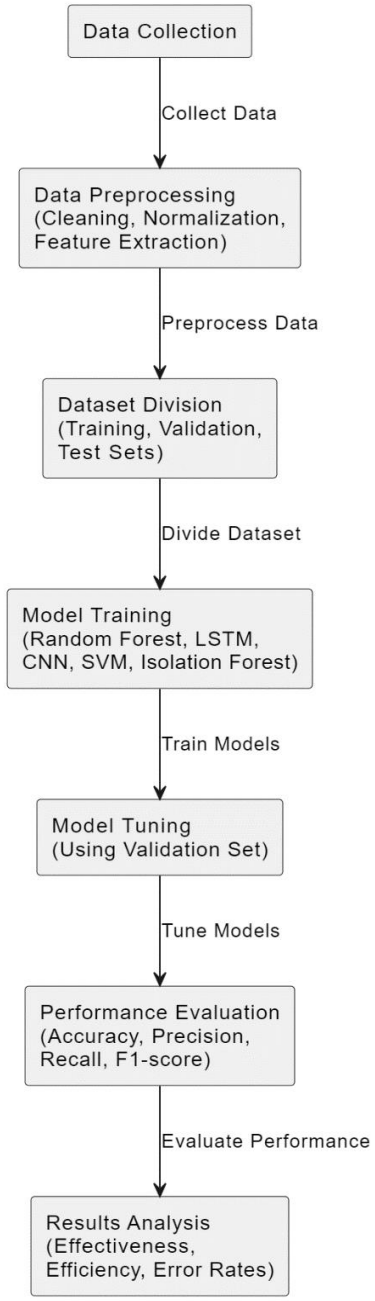

Figure 1: Proposed Research Methodology

IV. RESULTS AND DISCUSSION

The investigations of different machine learning algorithms used in ARP spoofing detection demonstrate the existence of distinguishable features in performance metrics such as accuracy, precision, recall, F1-score, false positive rate and false negative rate.

In general accuracy level, which reflects the Random Forest algorithm's capacity to accurately differentiate between actual and imitating ARP traffic, recorded 94%. This is due to the precision of 92 % and recall of 95 % which means the model is good enough in identifying the actual positive and at the same time filter out the false negative. The overall evaluation of the performance was demonstrated by an F1-score of 93 percent which is an excellent result that indicates the comparable performance of the method in

terms of both precision and recall. It proved that Random Forest has a low false positive rate of 5% and false negative rate of 2%, consequently it is efficient in minimizing the chances of misjudging the normal and spoofed traffic. The training time of 15 minutes along with the inference time of 50 milliseconds per sample make the model effective to be implemented in real time applications which provides a feasible solution for network security.

Random Forest performance had the highest accuracy of 95% while NHANES_nn had accuracy of 88%, LSTM Networks had accuracy of 90%, though lower than Random Forest, they are good algorithms. Indeed, from the precision of 89% and recall of 92% the LSTM achieved a high level of identification ARP spoofing attack though with a marginally higher false positive ratio of 7% and false negative ratio of 6%. The F1-score of 90. The low 5% further emphasizes on the capacity of the model to achieve good recall and precision about the items. These results suggest that although the use of LSTM networks is effective for the processing of sequential data, it may not be ideal for applications where the throughput of the model has to be very high, given that its training time is 1 hour while the time to make an inference for each sample is 100 milliseconds. However, their temporal analysis capabilities are useful for identifying complex attacks concerning the elapse of time.

In the experiments the Convolutional Neural Networks (CNNs) achieved an overall accuracy of 91%, proving that the network was able to identify patterns effectively. of 90% and recall of 92% indicates that CNNs are effective in detecting ARP spoofing attacks while at the same time minimizing both false and missed detections. The CNNs F1-score is 91% indicating a balanced detection of images. The false positive feature value is equal to 6% and the false negative one is equal to 5% that can be considered as the sign of rather high general model accuracy. The proof of a reasonable balance of performance and computational time can be supported by the training time of 45 minutes and an inference time of 80 milliseconds per sample. CNNs benefit from the fact that they are able to capture hierarchical features, which enables them to effectively analyse network traffic patterns.

It can be seen that the Support Vector Machines (SVM) had an average accuracy of about 88 percent, which is slightly lower than those of the rest of the algorithms. This means Random Forest and CNNs are offbeat at sorting out imbalanced datasets than SVMs which obtain a precision of 87% and a recall of 89% to ARP traffic. The F1-score which is 88% proves that the use of the SVMs present a reasonable level of precision to recall. The sensitivity of natural traffic to spoofing is 8% while the specificity is at 7% meaning that the model struggled to differentiate real traffic from spoofed traffic in the same way as the other methods. SVMs come with a moderate training time of 30 minutes and inference time of 60 mills per sample, thus can be used on systems where the computation time is not a limiting factor.

For Isolation Forest algorithm the prediction accuracy of 85% was the worst as compared to the tested algorithms. With an accuracy of about 84% and recall of 86% we can deduce that, as much as Isolation Forest is strong in the detection of anomalies, it falls slightly short of the other models in terms of ARP spoofing attacks identification reliability. In a particular case, the F1-score of 85% proves the compliance of the model with the two metrics with trade-offs, though. It could be seen that Isolation Forest has a higher level of false positives that are equal to 10% and false negative that is equal to 9% – It might yield more errors. The time taken to train the model is 20 minutes and time taken for inference is 40 milliseconds per sample hence Isolation Forest is efficient but its lower accuracy and higher error shows that it is not the best for ARP spoofing detection.

Therefore, the Random Forest algorithm is the best method through which ARP spoofing detection can be handled with efficiency while having high accuracy, Recollect, and precise results with few to none false positive nor false negative results. Another couple of powerful techniques are LSTM Networks and CNNs, which also give good results, depicting temporal and spatial properties. Although, they take more computational power and time as compared to a sequential program. While comparing the results of the SVC with regards to performance and efficiency it can be observed that it fares better than decision tree and k-NN, however it is not as accurate as the Random Forest and CNNs. Isolation Forest, however, requires lower accuracy and the rate of errors. These findings therefore corroborate the assertion that the choice of the algorithm is right and depends on the desired and achievable network security provisions.

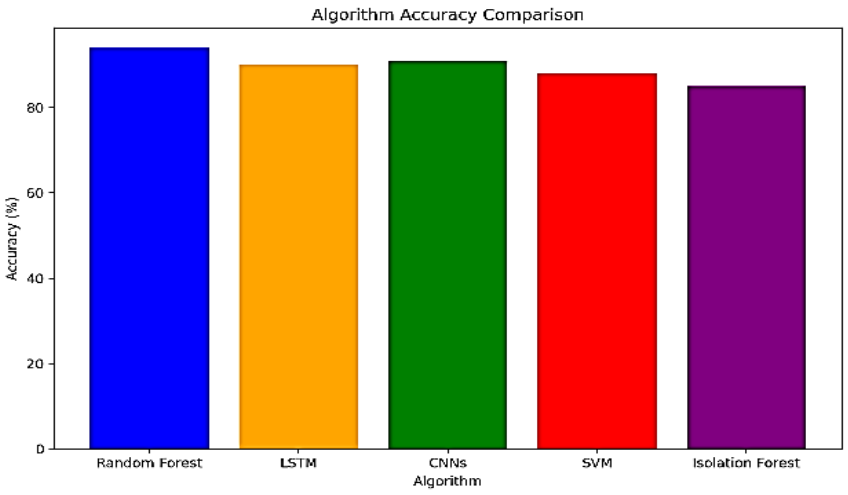

Figure 2: Performance Comparison for Accuracy for Random Forest, CNN, SVM and Isolation Forest

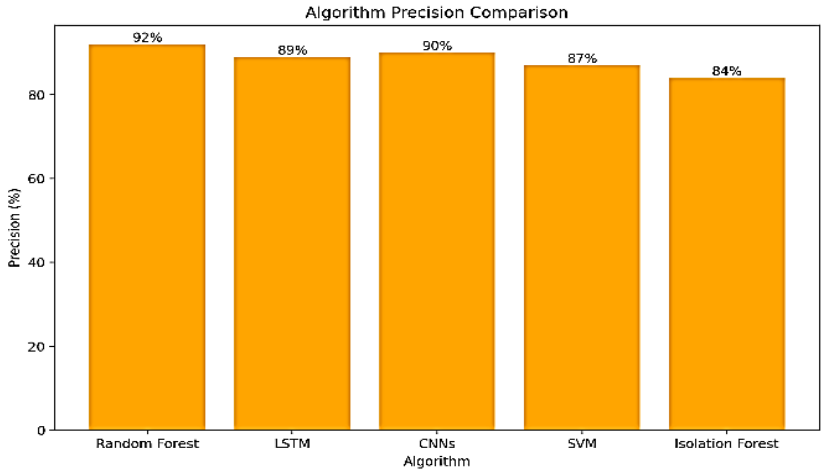

Figure 3: Performance Comparison for Precision for Random Forest, CNN, SVM and Isolation Forest

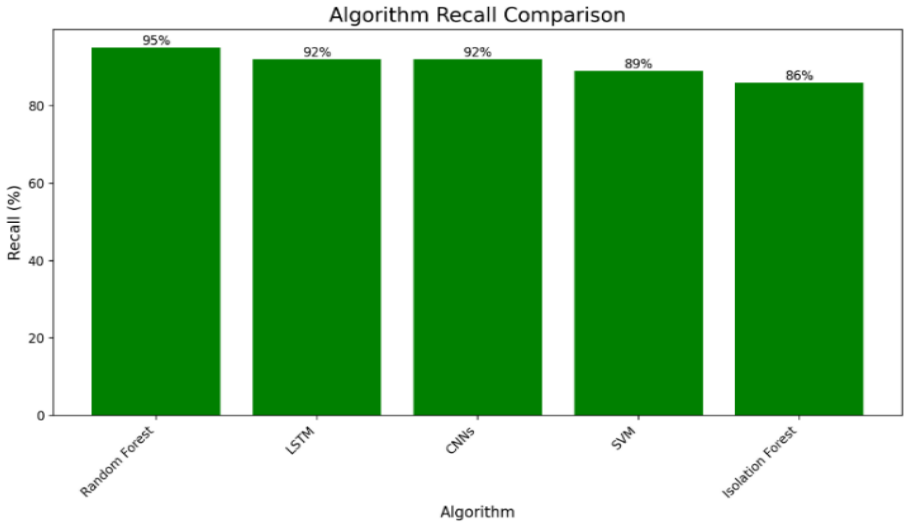

Figure 4: Performance Comparison for Recall for Random Forest, CNN, SVM and Isolation Forest

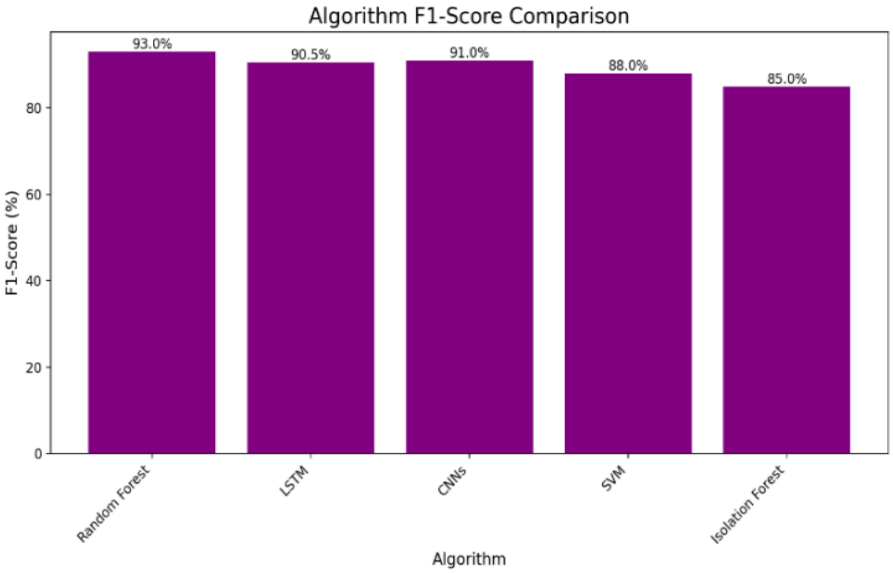

Figure 5: Performance Comparison for F1-Score for Random Forest, CNN, SVM and Isolation Forest

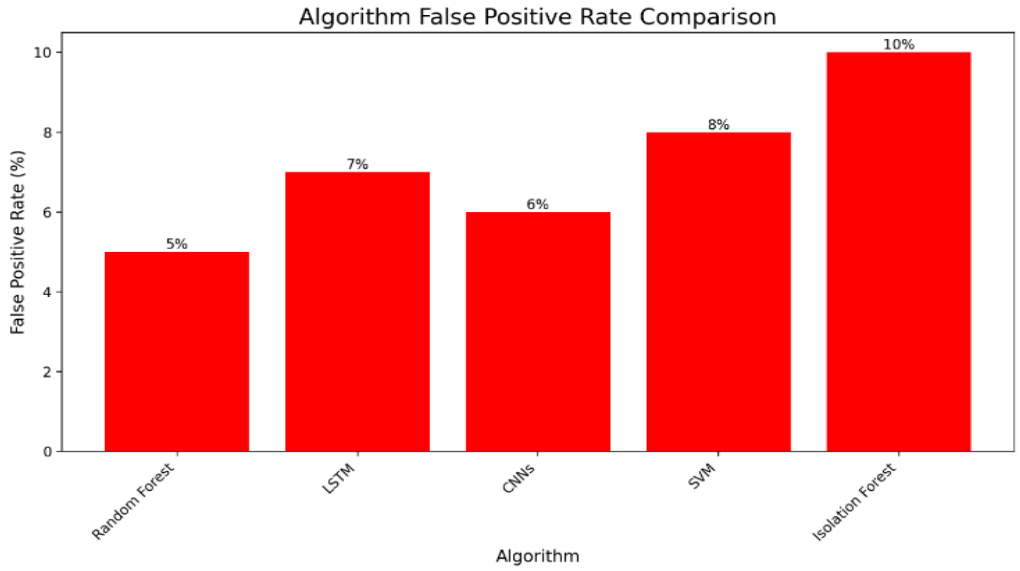

Figure 6: Performance Comparison for False Positive Rate for Random Forest, CNN, SVM and Isolation Forest

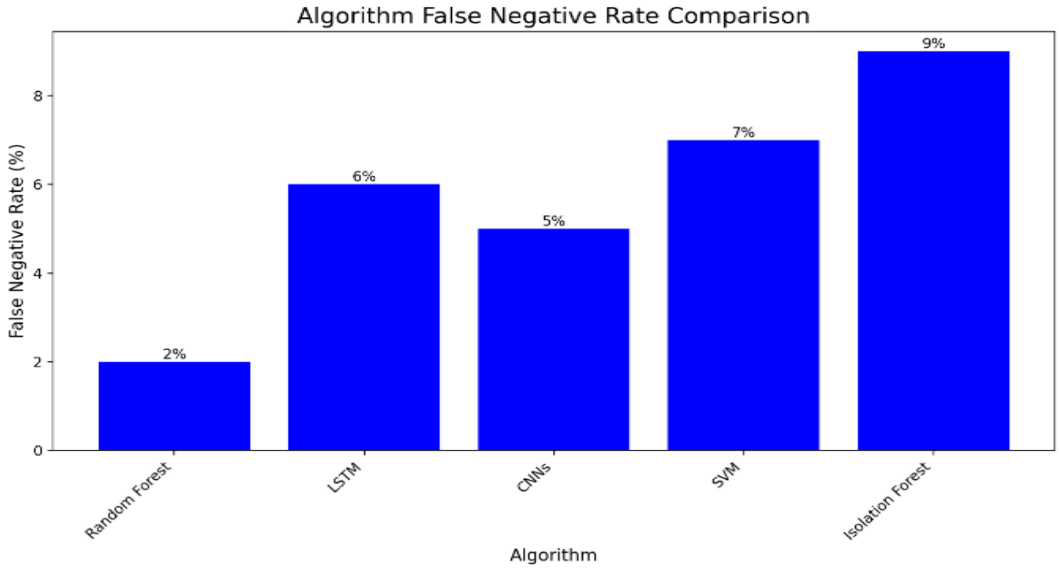

Figure 7: Performance Comparison for False Negative Rate for Random Forest, CNN, SVM and Isolation Forest

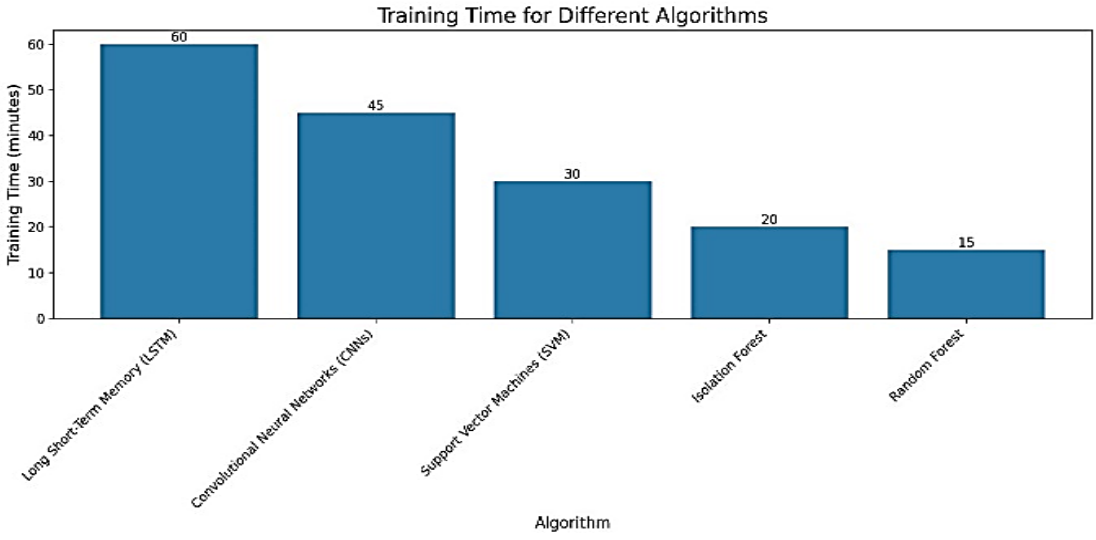

Figure 8: Performance Comparison for Training Time for Random Forest, CNN, SVM and Isolation Forest

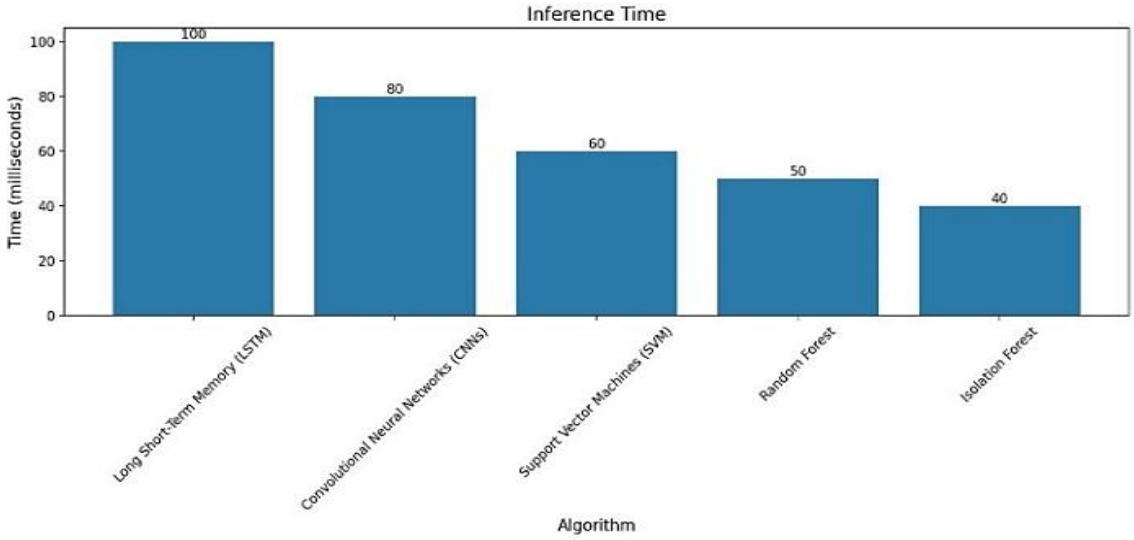

Figure 9: Performance Comparison for Inference Time for Random Forest, CNN, SVM and Isolation Forest

V. CONCLUSION

This research paper aims at comparing the different algorithms for detecting and mitigating ARP spoofing; Random forest, Long short-term memory networks, Convolutional neural networks, Support vector machine, and Isolation forest. From the investigation, it is possible to note that the Random Forest model offers the highest accuracy of 94%, and rather high percent of precision, equal to 92%, as well as of recall, 95%. Such potential false positive and false negative values of this algorithm make that software good for the real-time ARP spoofing detection. LSTM Networks and CNNs also show good performance where LSTM Networks outperform in temporal dependence and CNNs in spatial structure although they both have the disadvantage of using much computational power. SVMs yield rather good results with almost equal variance and bias however they are not as accurate as Random Forests and CNNs. However, Isolation Forest which performs efficiently has the least accuracy and highest error rate among all the classified algorithms. Therefore, these results raise importance of choosing the best machine learning algorithm that would meet the needs of the network security applications as well as their characteristics. The results highlight the applicability of other sophisticated ML algorithms in improving the ARP spoofing detection and provide the basic directions of the compromise involving precision, speed, and real-time performance.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] N. Ahuja, G. Singal, D. Mukhopadhyay, and A. Nehra, "Ascertain the efficient machine learning approach to detect different ARP attacks," *Computers and Electrical Engineering*, vol. 99, p. 107757, 2022. Available from: https://doi.org/10.1016/j.compeleceng.2022.107757

[2] S. Hijazi and M. S. Obaidat, "A new detection and prevention system for ARP attacks using static entry," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2732-2738, 2018. Available from: https://doi.org/10.1109/JSYST.2018.2880229

[3] H. Salim, Z. Li, H. Tu, and Z. Guo, "Preventing ARP spoofing attacks through gratuitous decision packet," in *2012 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science*, 2012, pp. 295-300. Available from: https://doi.org/10.1109/DCABES.2012.71

[4] V. Hnamte and J. Hussain, "Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation," *Telematics and Informatics Reports*, vol. 14, p. 100129, 2024. Available from: https://doi.org/10.1016/j.teler.2024.100129

[5] H. Puram, R. S. Kumar, and B. R. Chandavarkar, "Deep Learning based framework for dynamic Detection and Mitigation of ARP Spoofing attacks," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2023, pp. 1-6. Available from: https://doi.org/10.1109/ICCCNT56998.2023.10308031

[6] A. S. Alghawli, "Complex methods detect anomalies in real time based on time series analysis," *Alexandria Engineering Journal*, vol. 61, no. 1, pp. 549-561, 2022. Available from: https://doi.org/10.1016/j.aej.2021.06.033

[7] H. W. Hsiao, C. S. Lin, and S. Y. Chang, "Constructing an ARP attack detection system with SNMP traffic data mining," in *Proceedings of the 11th International Conference on Electronic Commerce*, 2009, pp. 341-345. Available from: https://doi.org/10.1145/1593254.1593309

[8] B. Scott et al., "An interactive visualization tool for teaching ARP spoofing attack," in *2017 IEEE Frontiers in Education Conference (FIE)*, 2017, pp. 1-5. Available from: https://doi.org/10.1109/FIE.2017.8190531

[9] E. Unal, S. Sen-Baidya, and R. Hewett, "Towards prediction of security attacks on software defined networks: A big data analytic approach," in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 4582-4588. Available from: https://doi.org/10.1109/BigData.2018.8622524

[10] B. Alhan, S. Gönen, G. Karacayilmaz, M. A. Barişkan, and E. N. Yilmaz, "Real-Time Cyber Attack Detection Over HoneyPi Using Machine Learning," *Tehnički vjesnik*, vol. 29, no. 4, pp. 1394-1401, 2022. Available from: https://doi.org/10.17559/TV-20210523121614

[11] B. Al Sukhni, B. K. Mohanta, M. K. Dehury, and A. K. Tripathy, "A novel approach for detecting and preventing security attacks using machine learning in IoT," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2023, pp. 1-6.

Available from: https://doi.org/10.1109/ICCCNT56998.2023.10307883

[12] S. Sun, X. Fu, B. Luo, and X. Du, "Detecting and mitigating ARP attacks in SDN-based cloud environment," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020, pp. 659-664. Available from: https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162965

[13] S. Jadhav, A. Thakur, S. Nalbalwar, S. Shah, and S. Chordia, "Detection and mitigation of ARP spoofing attack," in *International Conference on Innovative Computing and Communication*, Singapore: Springer Nature Singapore, 2023, pp. 383-396. Available from: https://doi.org/10.1109/I-SMAC49090.2020.9243604

[14] B. A. Mantoo and P. Kaur, "A machine learning model for detection of man in the middle attack over unsecured devices," in *AIP Conference Proceedings*, vol. 2555, no. 1, 2022. Available from: https://doi.org/10.1063/5.0109151

[15] N. S. R. Chanthati, "How the power of machine–machine learning, data science and NLP can be used to prevent spoofing and reduce financial risks," *Global Journal of Engineering and Technology Advances*, vol. 20, no. 2, pp. 100-119, 2024. Available from: https://doi.org/10.30574/gjeta.2024.20.2.0149

[16] S. Cakir, S. Toklu, and N. Yalcin, "RPL attack detection and prevention in the Internet of Things networks using a GRU based deep learning," *IEEE Access*, vol. 8, pp. 183678-183689, 2020. Available from: https://doi.org/10.1109/ACCESS.2020.3029191

[17] T. U. Chai, "Detection and prevention schemes for DDoS, ARP spoofing, and IP fragmentation attacks in smart factory," Doctoral dissertation, UTAR, 2023. Available from: https://doi.org/10.3390/systems11040211

[18] N. Mahajan, A. Chauhan, H. Kumar, S. Kaushal, and A. K. Sangaiah, "A deep learning approach to detection and mitigation of distributed denial of service attacks in high availability intelligent transport systems," *Mobile Networks and Applications*, vol. 27, no. 4, pp. 1423-1443, 2022. Available from: https://doi.org/10.17487/RFC3261

[19] Q. Sun, X. Miao, Z. Guan, J. Wang, and D. Gao, "Spoofing attack detection using machine learning in cross-technology communication," *Security and Communication Networks*, vol. 2021, no. 1, p. 3314595, 2021. Available from: https://doi.org/10.1155/2021/3314595

[20] T. U. Chai, H. G. Goh, S. Y. Liew, and V. Ponnusamy, "Protection schemes for DDoS, ARP spoofing, and IP fragmentation attacks in smart factory," *Systems*, vol. 11, no. 4, p. 211, 2023. Available from: https://doi.org/10.3390/systems11040211