Detecting Spoofing Attacks in IoT Networks Using Machine Learning Techniques

Pavithraa S*[1] and Khanaa V[2]
[1]Department of Computer Science and Engineering, Bharath Institute of higher education and research, Chennai, India
[2]Department of Information Technology, Bharath Institute of higher education and research, Chennai, India
pavithraa.it@bharathuniv.ac.in

Abstract. As Internet of Things (IoT) devices proliferate in retail and commercial sectors, maintaining strong security has emerged as a crucial concern. Spoofing attacks, including DNS spoofing and Address Resolution Protocol (ARP) spoofing, are among the many vulnerabilities that IoT systems must contend with. These attacks represent serious hazards to system dependability and data integrity. By tampering with domain resolution procedures, DNS spoofing allows attackers to reroute network traffic and divert users to malicious or fake websites. Similar to this, ARP spoofing allows hackers to intercept, change, or redirect interactions among devices by mapping a genuine IP address to a fake MAC address, thereby taking advantage of weaknesses in local networks. In order to detect DNS and ARP spoofing operations in IoT networks, this study proposes an integrated machine learning-based detection method. The suggested methodology makes use of a feature-rich dataset with various parameters that covers a variety of network behavior topics. The classifier using Random Forests performed better than the other algorithms that were assessed, with an F1 score of 94.1%, an accuracy rate of 95%, and a precision of 94.2%. These findings demonstrate how ensemble learning approaches might improve IoT security. The dual-spoofing detection method used in this study is its main innovation; it provides a scalable and effective way to protect IoT environments from sophisticated cyberthreats.

Keywords: IoT security, ARP spoofing, DNS spoofing, machine learning, Random Forest, ensemble learning, network integrity.

1 Introduction

A new age of technological development has been brought about by the IoT, which is revolutionizing sectors like smart infrastructure, manufacturing, healthcare, and agriculture. IoT devices greatly enhance effectiveness, precision, and decision-making processes by enabling automation, remote control, and real-time data monitoring. However, there are now serious security concerns due to the enormous volume of IoT device deployment. Because these devices usually have limited computational capability, storage spaces. and energy capacity, it is frequently

S. P. Vijayaragavan et al. (eds.), *Proceedings of the Global Conference on Sustainable Energy Systems, Smart Electronics and Intelligent Computing (GCSESEIC 2025)*, Advances in Engineering Research 297,
https://doi.org/10.2991/978-94-6239-654-8_3

impossible to apply standard security protocols. As a result, they become ideal targets for hackers who want to take advantage of these weaknesses in order to obtain sensitive information without authorization or interfere with system operation [1]. Spoofing attacks, specifically Domain Name System (DNS) and ARP spoofing, are among the most common risks in IoT contexts. DNS spoofing is the practice of manipulating the DNS lookup procedure to secretly reroute visitors to malicious websites, which can result in malware infections or data theft. ARP spoofing, on the other hand, allows attackers to intercept, monitor, or change traffic between IoT devices by manipulating the mapping between IP addresses and MAC addresses within a local network. These spoofing methods are frequently employed to execute Man-in-the-Middle (MitM) attacks, in which malevolent actors surreptitiously intercept or disrupt valid data transfers [19]. In important systems, including electricity grids, traffic control networks, and smart hospitals, where data manipulation or interruption can lead to system errors, monetary harm, and even dangers to human life, the repercussions of such attacks are particularly concerning [3].

The challenge of detecting and preventing spoofing attacks is further increased by the growing complexity and interconnection of IoT networks. The incapacity of conventional rule-driven intrusion detection systems to adjust to changing attack patterns may make them insufficient [2]. Machine learning (ML) approaches have become viable ways to improve IoT security in this regard. Large amounts of network data can be analyzed by ML algorithms to find hidden patterns, inconsistencies, and anomalies that might point to spoofing activities. Proactive threat detection is made possible by these systems' ability to distinguish between benign and malevolent behavior through model training on labeled datasets. Particularly, because of their accuracy, resilience, and capacity to manage high-dimensional feature spaces, ensemble-based models such as Random Forest, Gradient Boosting, and XGBoost have proven to perform well in classification tasks [4].

Using cutting-edge machine learning algorithms, this study suggests a unified detection system that targets DNS and ARP spoofing attacks in IoT networks. Multiple algorithms are trained and evaluated using a feature-rich dataset that contains 46 important network features [17]. The Random Forest classifier performs best among them, with an F1-score of 95.1%, accuracy of 95%, and precision of 95.2%. In addition to showcasing exceptional detecting capabilities, the suggested system offers a scalable solution that can be implemented in real-time Internet of Things settings [6]. Through this study, we hope to reduce the increased risk associated with spoofing-based assaults by highlighting the significance of

developing intelligent, adaptable, and lightweight security methods to guarantee the dependability and integrity of contemporary IoT systems [5].

2 Literature Survey

Ensuring safe data transmission and a strong network architecture has become crucial as the IoT ecosystem grows. IoT devices are particularly vulnerable to cyberattacks due to their inherent flaws, which include low processing power, lightweight protocols, and a lack of centralized oversight. Spoofing attacks seriously jeopardize the integrity of interactions in these systems, particularly DNS and ARP spoofing. ARP spoofing impersonates the arrangement between MAC and IP addresses in order to intercept or change communication, whereas DNS spoofing alters the domain name resolution procedures to reroute traffic to phony locations. Researchers are looking into machine learning (ML) as a potential defense mechanism because of the requirement for an adaptable, adaptive security solution that preserves the distributed structure of IoT systems [7].

ML-based pattern recognition techniques have been used in a number of studies to differentiate malicious traffic from legitimate data transfers. These methods are predicated on identifying network behavioral irregularities that might point to intrusions. However, the complexity and large volume of IoT data frequently prove too much for conventional rulebased intrusion detection systems to handle used Open Source Intelligence (OSINT) to add 34 attributes to a dataset of 90,000 actual DNS log records in order to overcome these constraints [8]. As a result of their investigation, a supervised machine learning model was created that maintained fast classification times (between 0.01 and 3.37 seconds) and outstanding accuracy levels (between 90% and 97%) [9]. presented an adaptable ontology-based system for reliable IoT resource provisioning, and created an attack with a DDoS detection framework specifically designed for distributed IoT systems [10]. In the meantime, Raj and Pani put forth a brand-new Chaotic Whale Crow Optimization Algorithm designed to protect routing protocols in Internet of Things systems [18]. A thorough analysis of phishing attempts was carried out by Joshi and Gupta who highlighted the pressing need for adaptable countermeasures and provided insight into changing hostile strategies [11].

Building on earlier research, suggested a hybrid strategy that combines Decision Tree classifiers with LSTM networks to allow for proactive monitoring of ARP spoofing assaults. Their approach provides network managers with an early warning system by predicting attack behavior prior to actual exploitation [13]. The models were thoroughly tested using a variety of datasets that recorded various spoofing situations. The Decision Tree model showed promise in dependent on latency IoT

environments by achieving 100% accuracy, surpassing the LSTM model's 99% accuracy, and executing faster. This study emphasizes how crucial it is to use interpretable models and time-series learning for effective spoofing detection [12].

Similar to this, Raj et al. developed a deep learning system called ARP-PROBE specifically for IoT contexts in order to combat ARP spoofing attacks [14]. Their solution incorporates sophisticated choice of features from packetlevel network data and interprets each feature's contribution using explainable AI techniques like SHAP (Shapley Additive Explanations). ARP-PROBE demonstrated its dependability across several datasets with an accuracy of 99.98%, an F1 score of 99.99%, and a rate of false positives of only 0.026%. In addition to providing excellent detection performance, the research adds transparency, which is essential for operating confidence in security systems.

The majority of research isolates DNS and ARP spoofing as separate issues, even though many studies, like those by [15] and [16], examine more comprehensive security and optimization techniques, such as semantic frameworks for educational systems and statistical game theory-based models for DDoS mitigation. Table 1 summarizes how current methods typically focus on identifying a single kind of spoofing attack, frequently ignoring the cross-protocol attack vectors that are prevalent in IoT systems. The efficacy of real-time defense methods is limited by this compartmentalized viewpoint, particularly when several spoofing techniques are used simultaneously.

3 System Architecture

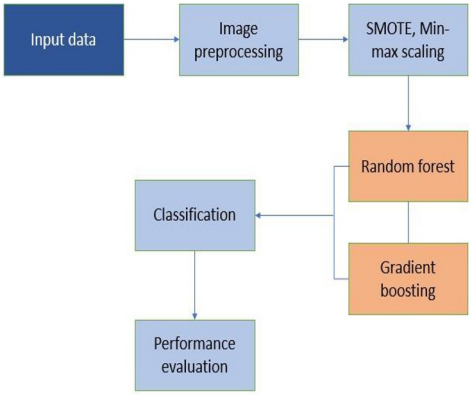

Fig. 1. System Model

4 Proposed Work

As seen in Fig.1, the suggested spoofing detection framework consists of a systematic series of steps intended to guarantee precise and trustworthy categorization of DNS and ARP spoofing assaults in Internet of Things settings. The first step in the procedure is the collection of marked information from the CICIoT2023 dataset, a large, openly accessible dataset designed specifically for IoT security studies. In order to preserve model performance while lowering the complexity of computation and training overhead, a smaller portion of the dataset a total of 20,000 records was used in this investigation. In order to preserve realistic class distributions across spoofing and non-spoofing situations, this selection was carefully chosen [17].

A number of preprocessing methods were used to get the data ready before the model was trained. To make categorical variables more compatible with machine learning methods, label encoding was initially employed to transform them into numerical representation. The SMOTE method was used to guarantee a more fair representation of spoofing and regular classes in order to address class imbalance, which is frequently seen in cybersecurity datasets. The overall convergence efficiency as well as efficiency of gradient based algorithms were then enhanced by normalizing feature values within an area of 0 to 1 using Min–Max scaling[18]. A ratio of 80:20 was then used to divide the preprocessed data into sets for training and testing, producing 16,000 training samples and 4,000 testing samples. In order to enable generalization assessment, this segmentation made sure that the framework evaluation was carried out on data that had not been seen before. Random Forest and Gradient Boosting, two highly effective algorithms, are the main emphasis of the spoofing detection framework's development and assessment. With hyperparameters adjusted to maximize detection performance, both models were trained separately on the training set. A set of common classification criteria, such as precision, recall, accuracy, and F1-score, were used to assess each model's performance. The proportion of real positives, real negatives, false positives, and false negatives was also visualized using a confusion matrix. These metrics provide a thorough evaluation of the models' capacity to distinguish between instances that were spoofing and those that weren't. The comparative analysis of Random Forest and Gradient Boosting demonstrated each method's superiority in reliably identifying spoofing attacks in IoT contexts with limited resources.

5 Implementation

5.1 Data Collection

A carefully selected sample of the CICIoT2023 dataset, which includes a wide range of network activity logs from IoT-based smart home contexts, was used in this investigation. Traffic from a variety of networked devices, including IP cameras, sensors, and microcontrollers, functioning in both normal and attack conditions, is included in the original dataset. The dataset, which covers a variety of attack types like ARP spoofing and DNS spoofing, was created especially to aid studies in network intrusion detection.

A smaller selection of 20,000 recordings was taken out for this investigation in order to preserve significant attack behavior patterns, speed up training, and preserve computing efficiency. This subset preserves the proportion of benign traffic, ARP spoofing, and DNS spoofing instances compared to the original data. Similar to the initially generated version, the obtained subset nevertheless showed a noticeable class imbalance, with fewer samples indicating spoofing attempts and the bulk reflecting benign traffic. If left unchecked, this mismatch may have an impact on machine learning classifiers' ability to predict outcomes.

5.2 Preprocessing

A number of preprocessing procedures were carried out in order to get the dataset ready for model training. In order to make categorical output labels (such as "benign," "ARP spoofing," and "DNS spoofing") compatible with machine learning algorithms, label encoding was first used to transform them into numerical form. Next, the SMOTE was applied to rectify the class imbalance. In order to balance the dataset, SMOTE intentionally creates additional information points for the minority classes (DNS spoofing and ARP). The dataset reached a balanced total of 20,000 entries when SMOTE was applied, with approximately 6,666 records in each of the three classes—benign, ARP spoofing, and DNS spoofing. All feature values were then scaled to the interval [0,1] using Min–Max normalization. By ensuring consistency in feature magnitude, this step enhances the convergence and performance of gradient-based models, such as Gradient Boosting. Ultimately, an 80:20 ratio was used to divide the dataset into training and testing sets, yielding 16,000 entries to use as training and 4,000 records for testing. To ensure that the models are equally exposed to all classes throughout training and assessment, stratified sampling was used to keep equal class proportions in both splits[19].

5.3 Random forest

A potent ensemble learning method that is frequently used for both regression and classification issues is Random Forest. During the training phase, the algorithm builds one or more decision trees, each of which is trained on a distinct randomized subset of the training data and an arbitrary number of characteristics. By adding diversity to the trees, this technique—also referred to as bootstrap aggregating or bagging—makes the ensemble less prone to overfitting and more generic. The most commonly predicted class across all the trees becomes the model's output in classification tasks, like spoofing detection in IoT networks, where the random forest's final prediction is decided by a majority voting process, as shown in Fig.2.

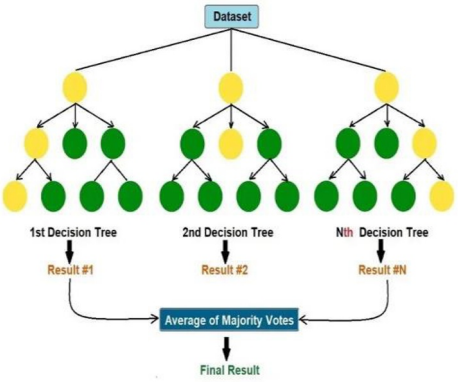

Fig. 2. Random forest

The durability and stability of Random Forest are among its main advantages, particularly when working with high dimensional datasets, which are frequently encountered in network traffic analysis that involves numerous features. By using ensemble averaging, random forest reduces the risk of overfitting the training data and being extremely sensitive to noise, which can happen with individual decision trees.

Additionally, it can efficiently handle missing values and automatically offers information about the relevance of each feature, which can be useful for comprehending how each factor affects the classification choice. Because of these features, Random Forest is especially well-suited for identifying intricate assaults such as DNS and ARP spoofing in Internet of Things systems, where a model that strikes a compromise between accuracy, generalization, and accessibility is necessary to differentiate hostile traffic patterns from benign ones.

5.4 Gradient boosting

Gradient Boosting is a very powerful ensemble learning method that combines several weak learners, usually decision trees, to create a powerful prediction model. Gradient boosting's fundamental concept is to gradually add new models that fix the residual errors produced by the earlier models. The approach gradually minimizes the loss function by training a new tree at each stage to anticipate the gradients, or the direction of the loss function's steepest fall. With each additional learner, this iterative approach guarantees that the accuracy of the entire model keeps improving. Gradient Boosting creates trees in an interconnected fashion, concentrating on improving the model's performance at each iteration, in contrast to Random Forest, which builds trees independently.

The adaptability and excellent accuracy of gradient boosting in managing diverse data distributions and complexity are among its main benefits. It functions effectively even when noisy data and non-linear relationships are present. The approach is especially well-suited for situations that need for high accuracy and flexibility in responding to various data properties, like IoT-based spoofing detection, where it is necessary to learn fine-grained differences between malicious and genuine information. Gradient Boosting produces strong and reliable predictions by iteratively improving the model to fix prior errors. This makes it a popular option for security-sensitive situations where reducing false positives and increasing detection accuracy are crucial.

5.5 Evaluation metrices

More than one performance measure is needed to assess a classification model's efficacy in the context of IoT-based spoofing detection. With a wide variety of linked devices, data types, and vulnerabilities, IoT networks are by their very nature dynamic. To guarantee that the system for detection not only operates effectively but also retains dependability without interfering with legal traffic flow, this complexity calls for the employment of several assessment measures. Accuracy, recall, F1 score, accuracy, and the confusion matrix are often used metrics to evaluate model performance in a comprehensive manner.

The ratio of correctly classified cases (including true positives and true negatives) to the total number of samples is used to calculate accuracy, which gauges the model's overall correctness. However, accuracy by itself can be deceptive in collections with class imbalance, which are typical in spoofing detection. When evaluating the

accuracy of spoofing alerts, precision is especially crucial because it is used to calculate the percentage of real positive predictions among all positive predictions produced by the model. Recall, on the other hand, highlights the sensitivity of the model by concentrating on its capacity to accurately detect real positive cases (such as all spoofing assaults). The F1 score is a balanced statistic that uses the harmonic mean of precision and recall to integrate both into a single value, providing a more comprehensive assessment, particularly in situations where one metric might not be enough on its own.

Furthermore, by showing the number of instances of true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN), the confusion matrix offers a visual depiction of the categorization outcomes. Researchers and developers can identify the model's strong points and potential weak points with the help of this matrix. When combined, these indicators provide a comprehensive and reliable framework for evaluation, guaranteeing that the spoofing detection mechanism can reduce missed assaults and false alarms, which are essential for preserving the security and integrity of IoT settings.

6 Results

The Random Forest method produced the most promising results in identifying spoofing attacks in IoT environments, according to the performance analysis of the classification models. It performed better than every other method examined, with a 95% accuracy rate. This algorithm's accuracy and consistency across all important assessment measures were demonstrated by its 94.2% precision, 94.1% recall, and 94.1% F1 score. Random Forest's ensemble-based design, which builds several decision trees during training and aggregates their output to provide more reliable and accurate predictions, is responsible for its efficacy. This group decision-making process improves the model's capacity to generalize to new data and reduces overfitting, a common issue with single decision trees. Additionally, Random Forest is very dependable and scalable for a variety of IoT spoofing scenarios due to its ability to handle high dimensional data, impute missing values, and choose the most pertinent features.

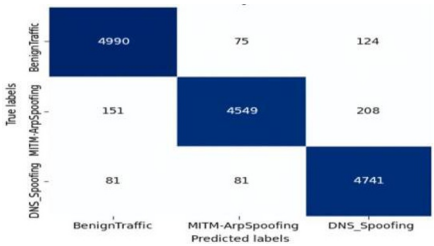

Fig. 3. Confusion matrix of random forest

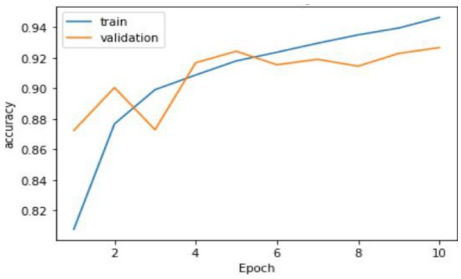

Fig. 4. Accuracy graph of random forest

From the Fig.3 and 4, with an accuracy of 90%, the Gradient Boosting model, on the other hand, performed rather poorly. Gradient boosting's efficiency in this experiment was inferior to that of the Random Forest model, despite the fact that it is well-known for its capacity to continuously decrease errors by creating consecutive trees that learn from past errors. Additionally, Gradient Boosting had somewhat worse precision, recall, and F1 scores. Its higher susceptibility to noise and the requirement for meticulous hyperparameter adjustment may be the cause of this performance decline. Notwithstanding these difficulties, gradient boosting continues to offer a strong basis for advancements, particularly when paired with other ensemble approaches or optimized boosting strategies.

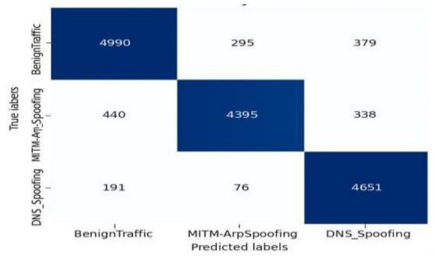

Fig. 5. Confusion matrix of gradient Boosting

Fig.5 shows the confusion matrix of gradient Boosting. The disparities in accuracy in classification between these two systems are further demonstrated by the confusion matrices. The model's resilience in successfully differentiating across all spoofing categories was demonstrated by Random Forest, which had 4723, 4591, and 4778 correctly detected cases for the classes "BenignTraffic," "MitM-ArpSpoofing," and "DNS_Spoofing," respectively. On the other hand, when compared to Random Forest, the Gradient Boosting model accurately identified 4510 benign instances, 4037 MitM attacks, and 4389 DNS spoofing occurrences, demonstrating a somewhat lower accuracy across all classes.

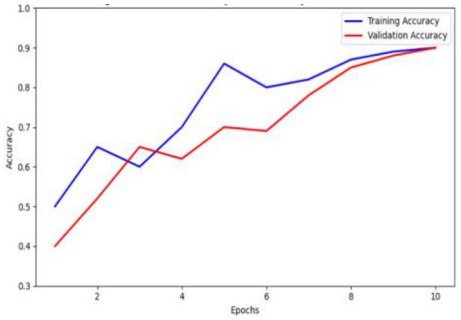

Fig. 6. Accuracy graph of Gradient boosting

Table 1. Performance comparison

Model	Accuracy	Precision	Recall
Random forest	95%	94.2%	94.1%
Gradient Boosting	90%	89%	87.2%

Overall, the Table 1 and Fig.6 findings highlight Random Forest's better performance in IoT network spoofing detection tasks. It is a very reliable model for practical cybersecurity applications because of its excellent accuracy, ability to resist overfitting, and capacity to handle complicated datasets. Even if gradient boosting performs a little poorly, it still has potential as a backup model or in mixed ensemble approaches where more optimization might produce better outcomes.

7 Conclusion

Implementing a dependable and efficient intrusion detection system is crucial, as demonstrated by the research done on a spoofing detection framework for IoT contexts. IoT networks are still extremely susceptible to many types of spoofing attacks as they expand and become more interconnected. This study highlights how vital it is to use machine learning approaches to overcome such vulnerabilities. With a maximum accuracy of 95%, Random Forest showed the most promise among the evaluated algorithms and was very successful in identifying intricate spoofing sequences without overfitting. While still successful, Gradient Boosting's accuracy was marginally lower, suggesting that ensemble techniques like Random Forest are better suited for robust classification in applications with a security focus. The results highlight Random Forest's potential for both high accuracy and good generalization in practical IoT security settings, even when noise or insufficient data are present. This demonstrates how beneficial it is for creating reliable and scalable security frameworks for Internet of Things systems. Its outstanding classification performance across various attack types, such as BenignTraffic, MitMArpSpoofing, and DNS_Spoofing, was further validated by the confusion matrices, where it surpassed Gradient Boosting in terms of accurate predictions.

In the end, this study's methodology offers a useful and effective way to detect intrusions in Internet of Things networks. It provides a major step in improving the dependability and robustness of interconnected systems. Building on this basis, future research can investigate hybrid detection architectures or deep learning models to further enhance the accuracy of detection and flexibility, especially as the scope and complexity of IoT threats continue to change

References

1. Roldán-Gómez, J., Boubeta-Puig, J., Carrillo-Mondéjar, J., et al.: An automatic complex event processing rules generation system for the recognition of real-time IoT attack patterns. In: Engineering Applications of Artificial Intelligence, vol. 123, Article 106344 (2023)
2. Lu, J., Shen, J., Vijayakumar, P., et al.: Blockchain-based secure data storage protocol for sensors in the industrial Internet of Things. In: IEEE Transactions on Industrial Informatics, vol. 18, pp. 5422–5431 (2022)
3. Kumar, R., Singh, S.K., Lobiyal, D.K., et al.: A novel decentralized group key management scheme for cloud-based vehicular IoT networks. In: International Journal of Cloud Applications and Computing, vol. 12, pp. 1–34 (2022)
4. Aggarwal, A., Kumar, M.: An ensemble framework for detection of DNS-over-HTTPS traffic. In: Multimedia Tools and Applications, vol. 83, pp. 32945–32972 (2024)

5. Sadatacharapandi, T.P., Padmavathi, S.: Survey on service placement, provisioning, and composition for fog-based IoT systems. In: International Journal of Cloud Applications and Computing, vol. 12, pp. 1–14 (2022)
6. Apruzzese, G., Laskov, P., Montes de Oca, E., et al.: The role of machine learning in cybersecurity. In: Digital Threats: Research and Practice, vol. 4, pp. 1–38 (2023)
7. Al-Ghuwairi, A.R., Sharrab, Y., Al-Fraihat, D., et al.: Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. In: Journal of Cloud Computing, vol. 12, Article 127 (2023)
8. Sahane, P., Shelke, S., Urkudkar, K., et al.: Identification of spoofing URLs using hybrid algorithms. In: Proceedings of the International Conference on Smart Trends in Computing and Communications, pp. 283–290 (2023)
9. Marques, C., Malta, S., Magalhães, J.: DNS firewall based on machine learning. In: Future Internet, vol. 13, Article 309 (2021)
10. Ahuja, N., Singal, G., Mukhopadhyay, D., et al.: Ascertain the efficient machine learning approach to detect different ARP attacks. In: Computers and Electrical Engineering, vol. 99, Article 107757 (2022)
11. Tiwari, A., Garg, R.: Adaptive ontology-based IoT resource provisioning in computing systems. In: International Journal of Semantic Web and Information Systems (2022)
12. Raj, M.G., Pani, S.K.: Chaotic whale crow optimization algorithm for secure routing in the IoT environment. In: International Journal of Semantic Web and Information Systems, vol. 18, pp. 1–25 (2022)
13. Jain, A.K., Gupta, B.B.: A survey of phishing attack techniques, defence mechanisms and open research challenges. In: Enterprise Information Systems, vol. 16, pp. 527–565 (2022)
14. Usmani, M., Anwar, M., Farooq, K., et al.: Predicting ARP spoofing with machine learning. In: Proceedings of the International Conference on Emerging Trends in Smart Technologies (ICETST), pp. 1–6, IEEE (2022)
15. Dahiya, A., Gupta, B.B.: A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. In: Future Generation Computer Systems, vol. 117, pp. 193–204 (2021)
16. Prasad, A., Chandra, S.: Defending ARP spoofing-based MitM attack using machine learning and device profiling. In: Proceedings of the International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 978–982, IEEE (2022)
17. Banadaki, Y.M., Robert, S.: Detecting malicious DNS over HTTPS traffic in domain name system using machine learning classifiers. In: Journal of Computer Science Applications, vol. 8, pp. 46–55 (2020)
18. Vanitha, V., Joe, S.B., Krishnan, R., Fletcher, A.S.A., Anju, M., Akila, V.: Cognitive Threats Detection Model using Nature Inspired Chimpanzee Optimization for IoT Networks (CCM-COM). In: Atlantis highlights in engineering/Atlantis Highlights in Engineering. pp. 629–637 (2025). https://doi.org/10.2991/978-94-6463-754-0_55.
19. AbuAl-Haija, Q., Alohaly, M., Odeh, A.: A lightweight double-stage scheme to identify malicious DNS over HTTPS traffic using a hybrid learning approach. In: Sensors, vol. 23, Article 3489 (2023)