Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
June 2024 5(6), 1236–1242

PERFORMANCE ANALYSIS OF MOBILE AD HOC NETWORK FOR DYNAMIC MALWARE DETECTION USING MACHINE LEARNING

Sanjeev Sharma[1], S. Veenadhari[2]

[1] Ph. D. Scholar, Department Computer Application, Rabindranath Tagore University, Bhopal (M.P.)
[2] Professor, Computer Science & Engineering, Rabindranath Tagore University, Bhopal (M.P.)

Corresponding Author
Sanjeev Sharma,
Sanjeevsharma7244@gmail.com

DOI
10.29121/shodhkosh.v5.i6.2024.4606

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are decentralized and self-configuring networks that facilitate communication without fixed infrastructure. However, their open and dynamic nature makes them highly vulnerable to various security threats, particularly malware attacks. Traditional signature-based malware detection systems are ineffective in such environments due to their inability to detect novel and evolving threats. This paper explores the advancements in machine learning (ML) techniques for dynamic malware detection in MANETs. We analyze various ML-based approaches, including supervised, unsupervised, and deep learning models, that enhance the accuracy and efficiency of threat detection. Furthermore, we discuss feature selection techniques, behavioral analysis, and anomaly detection methods that improve malware identification in real time. The integration of AI-driven malware detection solutions in MANETs significantly enhances their resilience against sophisticated attacks. The study concludes by highlighting the challenges and future research directions in developing adaptive and intelligent malware detection systems for secure mobile communication.

Keywords: Malware Attack, Security, Machine Learning, AODV, Decision Tree

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have gained significant attention due to their decentralized and self-configuring nature, making them suitable for various applications, including military operations, disaster recovery, and remote sensing. However, their open communication channels, dynamic topology, and lack of centralized security infrastructure expose them to numerous cyber threats, particularly malware attacks. Traditional signature-based detection methods struggle to keep pace with rapidly evolving malware, necessitating more intelligent and adaptive security solutions.

Machine Learning (ML) has emerged as a powerful tool for enhancing malware detection in MANETs by enabling dynamic threat analysis, behavioral anomaly detection, and predictive security measures. ML-based models can efficiently analyze network traffic patterns, detect malicious behaviors in real-time, and adapt to novel threats without

requiring predefined signatures. Techniques such as supervised learning, unsupervised learning, and deep learning have shown promising results in improving detection accuracy and minimizing false positives.

This paper explores the advancements in ML-driven malware detection in MANETs, highlighting key methodologies, challenges, and future research directions. By leveraging intelligent security frameworks, MANETs can enhance their resilience against cyber threats, ensuring secure and reliable communication in dynamic and resource-constrained environments.

2. RELATED WORK

This section discusses several studies that have investigated the detection of malicious attacks in mobile ad hoc networks (MANETs). Based on attack types, defenses, and assessment criteria, we can examine current research. Below, we delve deeply into a few key areas of study.

Gaurav Soni and Kamlesh Chandravanshi [1] was proposed A nobel defense scheme against selfish node attack in MANET, This paper proposes a novel Intrusion Detection System (IDS) algorithm to safeguard MANET against attacks by selfish nodes. In this case, the selfish node's behaviour is unnecessary, as it floods the network with information and obstructs the transmission of all types of packets between reliable nodes. The proposed IDS algorithm identifies the behaviour of egotistical nodes and also prevents their misbehavior activities. The performance of the network is nearly nonexistent in the event of a selfish node attack. However, the application of IDS to the attack results in a 92% improvement in network performance and a 0% infection rate from the attack.

Safa Altaha and Khaled Riad [2] have conducted a study that emphasizes the analysis of malware as well as a description of each trend. They evaluated the efficacy and significance of three trends—deep learning, transfer learning, and XML techniques—using three fundamental methodologies: static, dynamic, and hybrid analysis. Each of them contributes to the overall malware analysis process in a unique way, and they all play significant roles in it.

.Mohd Azahari, *et. al.* [3] The study evaluates the efficacy of numerous algorithms, such as Naïve Bayes, Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Decision Trees, Random Forests, and Logistic Regression, by analyzing a publicly accessible dataset that contains both benign and malicious files. The results of the investigation demonstrate that machine learning methods are capable of accurately identifying malware, resulting in reduced false positive rates and increased precision levels.

H. E. Merabet and A. Hajraoui [4] delve into the various stages of machine learning classifier training for malware detection. to learn to distinguish harmful and benign files and make accurate predictions when presented with new files. Support vector machines (SVMs), random forests, and neural networks are examples of machine learning classifiers that are used to increase accuracy and provide better outcomes.

B. Pandal and S. N. Tripathy [5] looked for strange things in the list of trusted applications based on what users wanted. The analysis may involve the identification of anomalous in-memory processes or un-trusted programs that are accessible on secondary storage. Using memory-based dynamic analysis of in-memory processes is suggested as a new way to find any processes that aren't on the trusted process list of a certain host.

Gaurav Soni, *et. al.* [6] was proposed An IPS approach to secure V-RSU communication from blackhole and wormhole attacks in VANET, To safeguard vehicle-to-RSU (V-RSU) communication from malevolent (Blackhole) and wormhole attacks in VANET, this paper suggests an intrusion detection and prevention (IPS) scheme. The IPS algorithm implements the swarm optimization approach in the RSU to identify the malicious actions of an assaulting vehicle. The particle-swarm optimization (PSO) verifies the attacker's presence and efficiently provides traffic information. As part of the proposed IPS scheme, vehicles also receive traffic data from the dominant vehicles and transmit it to other vehicles. The RSU monitors the exchange of traffic data to identify malicious activities.

Lai Van Duong and Cho Do Xuan [7] focus on a malware detection method that utilizes machine learning and deep learning algorithms to analyze PE files. The purpose of this paper is to suggest a set of features that are indicative of

aberrant malware behaviours, as well as the effectiveness of certain machine learning algorithms in the classification process, as determined by the PE file.

Abhishek Kumar Pandey and Fawaz Alsolami [8] concentrate on analysing the purpose and methodology of malware analysis in web application security. They identify a prioritized malware analysis technique through a hybrid multi-criteria decision-making procedure known as the fuzzy analytic hierarchy process. This fuzzy-AHP method helps find and suggest the best malware analysis techniques and types. It also suggests a ranking of the different malware analysis techniques that are commonly used in web application security so that experts and developers can use them. It also provides a complimentary overview of the domain by predicting the publication and assault scenario of malware and malware analysis for web application security.

Gaurav Soni and Kamlesh Chandravanshi [9] has been proposed Security Scheme to Identify Malicious Maneuver of Flooding Attack for WSN in 6G, This paper proposes a novel security scheme against flooding attacks in 6G communication for sensor networks. The data rate at which the sensor nodes communicate with one another is also high. The security scheme identified a Malicious Manoeuvre of Flooding attack (SIMMF) for WSN in the 6G network. The SIMMF offers a dependable routing scheme that enhances network performance at a minimal energy cost. The minimal energy consumption increases the potential for communication, thereby reducing overhead and extending the network's lifespan.

Rawad Abdulgha, *et. al.* [10] work delves into the fundamental concepts of Android malware, the architecture of Android, and the permission aspects that serve as effective malware predictors. Also provided is a thorough analysis of the current static, dynamic, and hybrid methods for detecting Android malware. In addition, the paper compares and contrasts how well six supervised machine learning algorithms work: K-Nearest Neighbors (K-NN), Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF), Naïve Bayes (NB), and Logistic Regression (LR). These algorithms are often used in the literature to check for malware.

NurAdibah Rosli, *et. al.* [11] This research presents a clustering detection technique that uses the K-means clustering approach to identify malware behaviour in a data registry based on the malware's characteristics. By examining the behaviour of the virus, clustering approaches that employ unsupervised algorithms in machine learning are crucial for classifying comparable malware features. Malware traits were chosen and removed from computer registry data throughout the experiment, and they were then employed in the suggested clustering detection algorithm to group suspicious or normal behaviour. The primary contribution derived from the results is that the suggested framework may be utilized to detect malware by clustering the data using a data registry.

Muhammad Iqbal Hossain, *et. al.* [12], This paper's study primarily focuses on the best classification algorithms and compares their accuracy to determine which algorithm produces the best results based on the dataset. Along with neural networks, top machine learning classification methods like XGBoost, support vector machines, extra tree classifiers, artificial neural networks, and others were used. When compared to other methods, the experimental result demonstrates that XGBoost obtained the greatest accuracy of 98.62 percent.

Abdelmalek Azizi, *et. al.* [13], This paper's aim is to use the headers of files to determine if they are suspicious or regular without actually opening them. Initially, they will examine each extension (.docx, .exe, .pptx, .xlsx, .jpg, etc.) independently by determining its headers and signatures. Then, using a tool that determines if a file is suspicious or benign, they will examine several files with various extensions.

Kamlesh Chandravanshi, *et. al.* [14] has been proposed Predictive machine learning-based integrated approach for DDoS detection and prevention, They implement and rigorously assess each of these algorithms individually to validate their efficacy in this domain. They evaluated the presented work using the most recent dataset, CICIDS2017. The dataset characterizes various DDoS attacks, including infiltration, botnet TCP, UDP, and HTTP with port scan attack, brute force SSH, and brute force FTP.

3. PROPOSED METHODOLOGY

This article introduces the steps and elements of a typical machine learning (decision tree) workflow for malware detection and classification. It also examines the difficulties and constraints of this type of workflow and evaluates the latest advancements and trends in the field, with a focus on deep learning techniques. Below is the suggested research approach for this investigation. Figures 1 and 2 show the workflow process from beginning to end to provide more thorough knowledge of the suggested machine learning approach for malware detection.

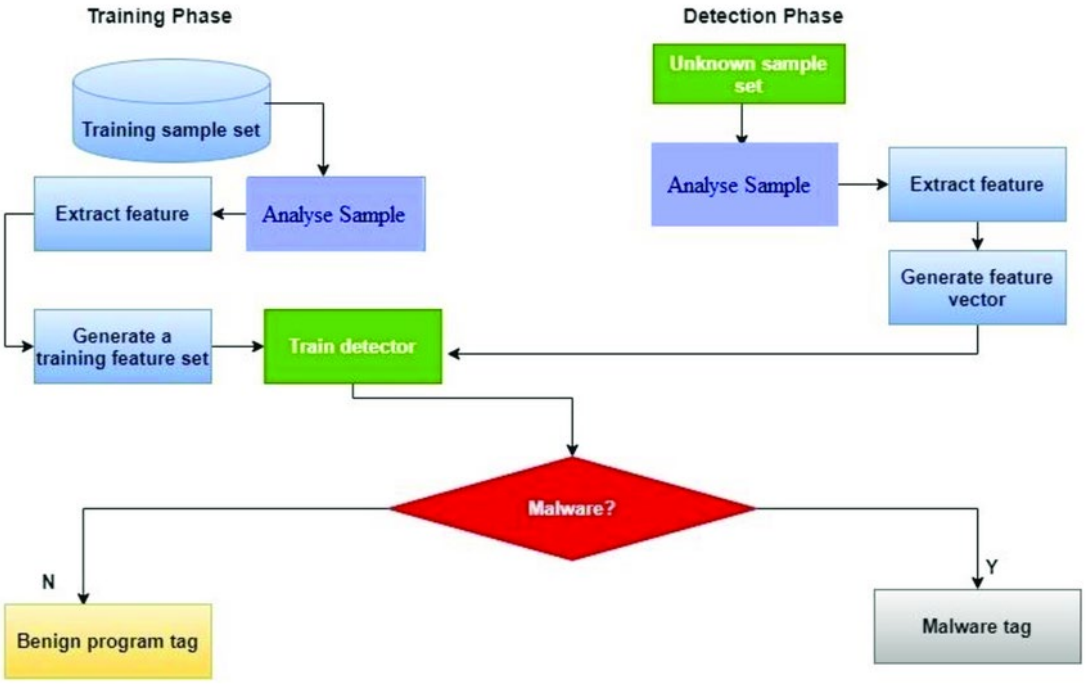

Figure 1: Proposed Workflow

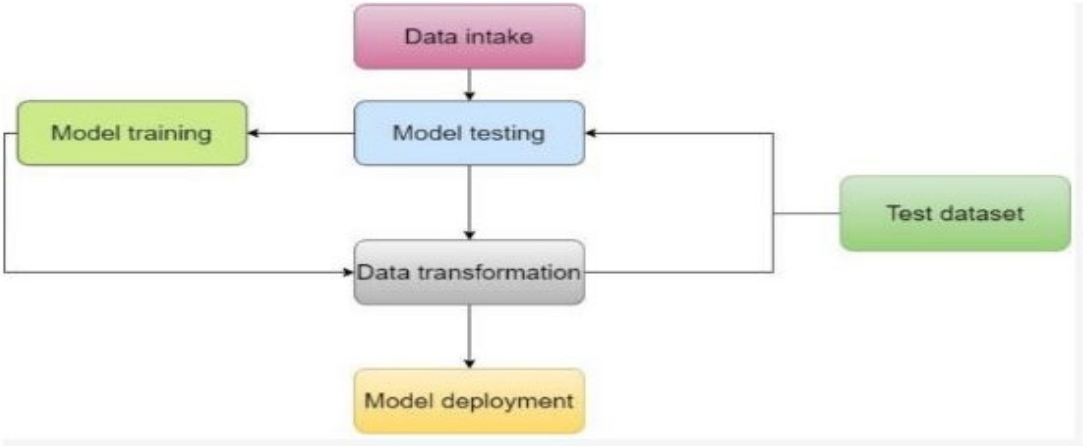

Figure 2: Steps Involve of Proposed Method

To develop an effective machine learning-based dynamic malware detection system for Mobile Ad Hoc Networks (MANETs), a structured methodology is followed, consisting of the following key steps:

3.1 DATA COLLECTION AND PREPROCESSING

Network traffic data and system logs are collected from simulated or real MANET environments. Datasets containing both normal and malicious network behaviors (e.g., trace, nam file generated by NS-2) are used. Data cleaning techniques, such as noise reduction, normalization, and feature extraction, are applied to enhance data quality.

3.2 FEATURE SELECTION AND EXTRACTION

Relevant features such as packet flow, transmission frequency, anomaly patterns, and device behavior are identified. Dimensionality reduction techniques (e.g., Principal Component Analysis (PCA), Recursive Feature Elimination (RFE)) are applied to improve model efficiency.

3.3 MACHINE LEARNING MODEL SELECTION AND TRAINING

In this article use the supervised learning algorithm (decision tree) and Models are trained using training datasets and optimized using techniques like hyper parameter tuning and cross-validation.

3.4 DYNAMIC MALWARE DETECTION MECHANISM

The trained ML models are deployed in a real-time monitoring system to analyze network traffic. Anomaly detection techniques continuously monitor and flag suspicious activities. Adaptive learning mechanisms allow models to update dynamically based on new threat patterns.

4. SIMULATION PARAMETERS

The simulation of the current AODV-M, DSR-M, and planned DML-DT takes into account the simulation parameters listed in Table 1. We consider these criteria for all situations because they offer a more comprehensive explanation for performance in a comparable environment. Malware is the sort of attacker. The simulation runs on version 2.31 of the NS-2 simulator. 50 nodes are considered for simulation in various simulation times (20, 40, 60, 80, and 100), with nodes moving randomly inside a grid pattern of 1000 m by 1000 m.

Table 1: Simulation Parameter for Network Deployment

Parameters	**Configuration Value**
Simulation Tool	NS-2.31
Routing Protocol	AODV-M, DSR-M, DML-DT
Simulation Area	1000m*1000m
Node Maximum Velocity [m/s]	Random
Attack Type	Malware
Attack Prevention	Machine Learning DML-DT
Network Type	MANET
Number of Nodes	50
Physical Medium	Wireless, 802.11
Simulation Time (Sec)	550Sec
MAC Layer	802.11
Antenna Model	Omni Antenna
Traffic Type	CBR, FTP
Propagation radio model	Two ray ground
Energy (Initial)/J	Random

5. RESULT ANALYSIS

The attacker is harmful for network and reliable security scheme is able to secure the routing and gives secure communication in network. In this section compare the performance of DSR-M, AODV-M and proposed DML-DT scheme. The DML-DT scheme showing better performance.

5.1 ATTACKER PERCENTAGE ANALYSIS

The attacker infection analysis means only measures the infection in network only due to the presence of attacker. The attacker percentage showing the performance degradation in presence of attacker in network. The figure 3, represents the infection percentage analysis in case of an DSR-M and DML-DT. The graph clearly illustrates that the attack has infected about 40% of the network. However, after applying the machine learning scheme with decision tre, indicating that the security scheme completely blocked the attacker's misbehaviour and proving secure routing between sender and receiver.

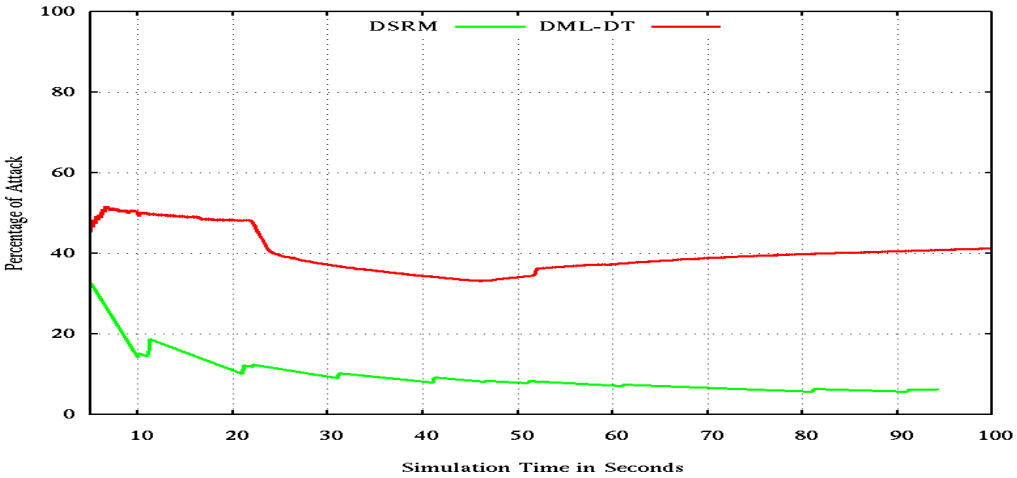

Figure 3: Percentage of Attack Analysis

5.2 DATA RECEIVING ANALYSIS

The attacker presence in network always affects the data packets receiving and only focus on the data packets dropping in network. The data packets receiving percentage measures the packets' percentage performance. In the figure 4,shows the PDF analysis in DSR-M, AODV-M and DML-DT for . We only evaluate the normal routing performance after applying the proposed security scheme. The effect of a malware attack in a network is showing the degradation in performance. In DSR-M, only 6% data received, In AODV-M only 11% data received but after applying DML-DT 88% data received in network. The proposed decision tree based approch improves the network performance and provides secure routing. After applying a security scheme against anmalware attack, the network performance improves 78%. The proposed security scheme improves performance in the presence of DML-DT.

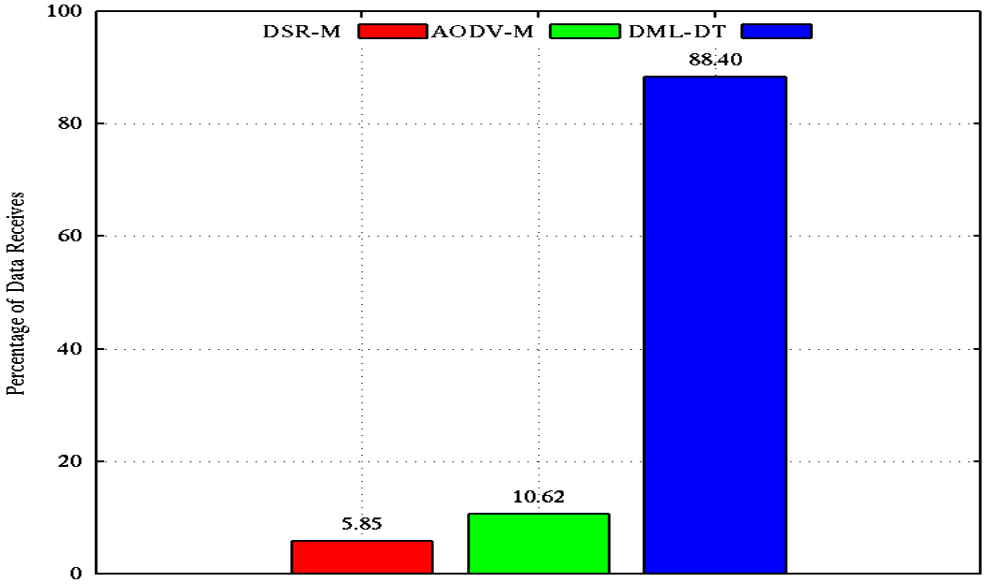

Figure 4: Analysis of Percenatge of Data Receives

6. CONCLUSION & FUTURE WORK

The behavioral pattern of malware attackers is to perpetually flood dynamic networks with unwanted information. MANETs are not secure because their open environments allow all nodes to communicate freely. This paper investigated the efficacy of decision tree models based on machine learning for detecting malicious activity in mobile ad hoc networks (MANETs). AODV-M and DSR-M routing are compared to the proposed DML-DT technique, which shows a big improvement in throughput and the amount of data received compared to current methods. We deploy fifty mobile nodes and apply ad hoc routing to the established path between the source and destination to simulate a mobile ad hoc network using the network simulator-2. The network contains certain nodes that exhibit malicious behaviors, such as dropping data packets or disseminating spam messages. In future apply the various supervise learning technique such as Random

Forest, Support Vector Machines (SVM), and Neural Networks trained using labeled datasets to compare proposed technique and betterment the outcomes of mobile ad hoc network.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Gaurav Soni, Kamlesh Chandravanshi, '"A Nobel Defence Scheme Against Selfish Node Attack in MANET", International Journal on Computational Science & Applications(IJCSA) 2013 ISSN: 2200-0011 is a AIRCC journal,

SafaAltaha1, Khaled Riad2 (2024),"Machine Learning in Malware Analysis: Current Trends and Future Directions".".(IJACSA) Vol. 15, No. 1, 2024

MohdAzahariMohd Yusof1 , Zubaile Abdullah2 , Firkhan Ali Hamid Ali3 , Khairul Amin Mohamad Sukri4 , Hanizan Shaker Hussain5(2023),"Detecting Malware with Classification Machine Learning Techniques".(IJACSA) Vol. 14, No. 6, 2023

Hoda El Merabet1,AbderrahmaneHajraoui2 (2019), "A Survey of Malware Detection Techniques based on Machine Learning." (IJACSA) Vol. 10, No. 1, 2019

Binayak Panda1, Dr. Satya Narayan Tripathy2. (2020),"Detection of Anomalous In-Memory Process based on DLL Sequence ".(IJACSA) Vol. 11, No. 10, 2020

Soni, G., Chandravanshi, K., Jhariya, M.K., Rajput, A. (2022). An IPS Approach to Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET. In: Sarma, H.K.D., Balas, V.E., Bhuyan, B., Dutta, N. (eds) Contemporary Issues in Communication, Cloud and Big Data Analytics. Lecture Notes in Networks and Systems, vol 281. Springer

Lai Van Duong1, Cho Do Xuan2 (2021),"Detecting Malware based on Analyzing Abnormal behaviors of PE File ".(IJACSA) Vol. 12, No. 3, 2021

Abhishek Kumar Pandey1,Fawaz Alsolami2 *(2020), "Malware Analysis in Web Application Security: An Investigation and Suggestion".(IJACSA) Vol. 11, No. 7, 2020

G. Soni and K. Chandravanshi, "Security Scheme to Identify Malicious Maneuver of Flooding Attack for WSN in 6G," 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2021, pp. 124-129

TalalA.A Abdullah1, Waleed Ali2, Rawad Abdulghafor3 (2020)," Empirical Study on Intelligent Android Malware Detection based on Supervised Machine Learning". (IJACSA) Vol. 11, No. 4, 2020

NurAdibahRosli1,WarusiaYassin2,FaizalM.A3,SitiRahayu Selamat4. (2019)," Clustering Analysis for Malware Behavior Detection using Registry Data".(IJACSA) Vol. 10, No. 12, 2019

ABM.Adnan Azmee1, PrantoProtim Choudhury2, Md. Aosaful Alam3, Orko Dutta4, Muhammad Iqbal Hossain5. (2020)," Performance Analysis of Machine Learning Classifiers for Detecting PE Malware".(IJACSA) Vol. 11, No. 1, 2020

Houria MADANI1, Noura OUERDI2, Abdelmalek Azizi3 (2023) "Ransomware: Analysis of Encrypted Files."(IJACSA) Vol. 14, No. 1, 2023

Kebede, S.D., Tiwari, B., Tiwari, V. et al. Predictive machine learning-based integrated approach for DDoS detection and prevention. Multimed Tools Appl 81, 4185–4211 (2022).