Cyber Attack Detection in Wireless Adhoc Network using Artificial Intelligence

Mahmoud A. Zaher[1]*, Nabil M. Eldakhly[2]

[1] Faculty of Artificial Intelligence, Egyptian Russian University (ERU), Cairo, Egypt
[2] Faculty of Computers and Information, Sadat Academy for Management Sciences, Cairo, Egypt & French University in Cairo, Egypt
Email: mahmoud.zaher@eru.edu.eg; nabil.omr@sadatacademy.edu.eg

Abstract

A wireless sensor network, also known as a WSN, is made up of thousands of minuscule sensor nodes that are connected to one another in order to monitor, track, and organize data collected in an unattended environment in the most prominent location. Due to its one-of-a-kind qualities, it has, the wireless sensor network is gaining traction in a variety of sectors and put to use in a wide range of applications, including surveillance, healthcare, and industry. These networks exposed to a variety of security flaws and major threats because of their dynamic design and deployment in an unsupervised environment. Cybercriminals prey on individuals who utilize the internet as well as organizations in order to get sensitive information. The hackers were able to access critical data on the company's systems, such as login information, credit card details, and bank account numbers. Phishing attacks are a sort of cyberattack in which hackers trick internet users into believing their websites are authentic in order to collect the users' private information. The purpose of these attacks is to steal this information. Malware assaults begin with the covert installation of malicious software on corporate servers or user PCs via the use of the internet. The attackers then continue to steal every piece of information that kept on the targeted server or computer. Malware used in an ever-increasing number of attacks these days. An incursion into a network is a kind of attack in which the perpetrator seeks to take possession of all of the network's resources. Approaches based on heuristic analysis and visual resemblance used, regardless of whether they are blacklisted or whitelisted.

Keywords: Cyber-Attacks; Intrusion Detection System; HTTP Sites; Attackers.

1. Introduction

The infrastructure-based networks will each have their own set of fixed base stations, and each of those fixed base stations will have its own set of fixed access points that are arranged according to a particular zone. These base stations may serve as an access points for mobile stations, allowing them to connect to wire backbone networks. The execution of the duties associated with these network control services falls on the shoulders of the base stations. Base stations are often linked to one another in order to permit synchronized controllers [1], and there is a substantial difference between the form of an ad hoc network and that of an infrastructure network.

It is not necessary to have a permanent infrastructure in an ad hoc network of the kind known as a MANET since the nodes in the network are able to regulate themselves and operate together as a group while yet being mobile. This eliminates the requirement for infrastructure. While this kind of system and its nodes are able to make bonds at any given time and are free to disseminate

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

themselves over the network at any given moment. Because mobile ad hoc networks have this one-of-a-kind feature, the statistics of the data that are stated by mobile equipment have the propensity to change on a relatively regular basis. Additionally, both locating the network and the mobile equipment [2] make it more difficult to participate in the network. In order to advance the performance of mobile ad hoc type networks, there are two key aspects that will be improved: the station frequency, as well as the amount of time that batteries may be used before, they need to be replaced. The life of the batteries and the life of the device itself both count as key aspects. Other important features include: In addition, the network of this mobile ad-hoc learns that the effect of fluctuating transmission power levels is really important and plays a very big role. This is something that the network discovers through experience. The performance of these ad hoc networks [3] will continue to be impacted by the criteria that include frame sizes, the length of a slot, channel capacity, channel utilization, and the number of transmissions that are happening at the same time. When it comes to deciding whether transmission can take place, the data rates, and the range of transmission that the network has, as well as the distance that separates the nodes, all play important roles. The Media Access control, or MAC, protocol [4] has a standard that contains the rules that dictate how a collection of nodes may utilize a common media in order to allow reliable data transmission. [MAC] stands for "Media Access Control." This is accomplished via the use of a mechanism for controlling media access. In addition to this, it will attempt to attain the maximum possible channel utilization and will provide an equitable entry point into the medium.

The result of this direct influence will be the death or falling of nodes because of the let down and discouragement of energy. The lifespan of the batteries that provide power to the active nodes that participate in mobile ad hoc network communication would be shortened. After then, the most important aim of the ad hoc network [5] is to be able to enable communication approximately, and this purpose is expected. In an environment such as an ad hoc network, there will be a need for energy maintenance management approaches, whose primary function will be to monitor the effect. This is crucial since the operational message will be present, and it is important to make sure that the particular failures of that node are effective. In addition to this, more information will be offered in the form of a representation of life's network in order to enable an abundantly the subsequent anticipated message. This is done in order to facilitate an abundantly subsequent the expected message.

The phrase "network lifespan" may have a few distinct meanings depending on the context, including the following:

• The amount of time that must pass before the cumulative delivery rate of distribution may fall below the threshold

• The amount of time needed for the network to divide • the amount of time needed once a problem has been detected in the first node

In most cases, the processing unit (microcontroller) is accompanied by a minuscule memory device, which is responsible for carrying out instructions regarding detection, [6] communication, and self-organization. The microcontroller unit is required for the execution of communication protocols, the control of the sensors, the execution of the signal processing algorithm on the information obtained from the sensors, and the provision of the information to the sensor node. The transceiver device allows for a wireless connection to be established with the node that is nearby. A radio transceiver is used here for the purpose of communication. Both a transmitter and a receiver are included in its construction. Depending on the requirements of the application, an appropriate mode of communication, such as infrared, optical, or radio communication, will be used. The sensor node's power unit is an essential component of the node itself. The battery provides the energy that the sensor node as a whole requires, and as a result, it plays a significant role in determining how long the sensor node will remain operational. In the field, the primary responsibility of a sensor node is to detect events, complete a quick analysis of particular information, and relay the information. The nodes that make up the WSN are able to send data to one another, and the most important concern of the WSN [7] is data security. An intruder is able to attack an individual node in a Wireless Sensor Network, and the intruder's ability to change the basic characteristics of an individual node is also possible. This targeted node will then behave as a malicious node, producing transmissions that are undesirable and of no utility to the network as a whole, and distributing the information across the

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

whole network area. The WSN vulnerability might be exploited in a variety of ways, including floods, wormholes, black holes, and so on. The degree of danger posed by a breach in security could be proportional to the kind of assault that was launched against the wireless network.

2. Related Work

Cross-layer assault tactics [8], These strategies may either dramatically increase the attackers' power or decrease the likelihood that they would be detected. As part of the process of developing a cross-layer trust protection system, an uncommon PHY and MAC identification system as well as a cross-layer trust manager was established. To combat the jamming that occurs in the physical layer, it is standard practice to apply techniques that vary based on the targeted packet delivery ratio (PDR) [9]. Jamming is an additional tool that can be used to disrupt the characteristics of another layer; nevertheless, it is possible that these approaches cannot be used to defend against assaults that target many layers.

This system was designed in order to effectively detect persistent attacks [10]. In addition, a mitigation function was designed in order to achieve the greatest possible balance between security and productivity. A security mechanism that protects against cross-layer assaults is produced by the concurrent operation of detection and mitigation systems. Numerous layer attacks have been discovered in the following generation, each of which makes use of very few alterations made to one layer of the network in order to covertly restrict access to another target layer [11]. A new security approach based on the Bayesian learning method was suggested. Within this approach, the attack detection component builds a model of recorded data in order to identify covert attack actions. Existing methods of attack detection frequently believe that attacks are always carried out in the same way and always have the same goal and that large-scale attacks must be carried out in order to achieve significant results, [12] suggested that the primary importance of developing a detection and mitigation method capable of detecting and counteracting small scale vibrant cross-layer attacks [13].

This is because existing techniques of attack detection often believe that attacks are always carried out in the same way and always have the same goal. The use of data from several layers in the detection of assaults has garnered a significant amount of public attention. There is a series of functions inside an intrusion detection system (IDS) [14] that employ cross-layer characteristics for both single-layer assaults and cross-layer attacks. The idea is to monitor the features on several levels so that separate single-layer assaults (or simultaneous sub-attacks for cross-layer attacks) may be detected with higher accuracy. This will allow for better defense against cross-layer attacks. Using swarm intelligence as a countermeasure to avoid cross-layer assaults [15] like Sybil and collision attacks at the data link and network layer is a novel technique that was developed.

This new approach integrates swarm intelligence as a countermeasure. As the primary debatable elements, the DOS 17 attack, the number of hops, the distance, and the amount of energy are all taken into consideration. The effectiveness of the network is impacted by the weights that are assigned to its various factors. An evolutionary algorithm aids in preserving the performance of the network [16] by discovering an alternate solution when an invader blocks a node. This helps keep the network running smoothly. In order to arrive at the best possible resolution, the ant agents engage with one another via the process of distributed problem solving.

When it comes to anti-jamming strategies, the decision-making process is heavily influenced by performance characteristics such as hops, energy, distance, packet loss, and packet delivery. However, before the agents understand the network, there is a significant initial investment in both time and computing resources. When the integrity of the node itself has been compromised, the likelihood of the data packet being tampered with is increased. Bayesian learning is a type of machine learning technique that is used to train multilayer classifiers. These classifiers are used to identify and mitigate harmful activities that occur in the helping layer. A novel detection scheme was proposed [17], and it relies on this type of machine-learning technique. In order to identify assaults on a network, Bayesian learning [18] was another technique that was often utilized. Combining the Bayesian Algorithm with the Swarm Intelligence (SI) technique was the unique detection method [19] that was developed. This method was designed to identify the Sybil assault.

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

The swarm agents gather the performance characteristics such as energy, packet delivery rate, packet loss rate, and so on. The information that is acquired is then utilized as training data for a Bayesian Network, which infers the knowledge to detect malicious nodes. It has been stated that in the future, a combination of DOS assaults may potentially be something to consider. It has been determined, after taking into consideration the suggestions for future work that were cited in the preceding literature review, that the Bayesian Network based machine learning technique can be used effectively to design a model that can monitor the features on multiple layers in order to make decisions in an actual world setting. In this work, the Bayesian learning method, which is a technique for machine learning, is used to train the classifier. The classifier monitors all of the abnormal changes that take place in the network, and a classifier is used for classification and to overcome the attacks based on the observed features. For detecting jamming in the physical layer and poisoning in the MAC layer [20], posterior distribution, which is a conditional probability assigned after taking into account the relevant information, is used. In order to identify and categorize the DOS assault in the physical and network layers, which deal with large amounts of data, the machine learning approach known as machine 18 was used.

[21] Suggested a detection approach that increases the accuracy of detection by employing cross-layer characteristics and a two-phase mobile agent-based strategy. This method was published in the journal Communications of the ACM. [22] Concentrated their efforts on mobile agents that make advantage of a three-way manoeuvre including sensor stations and the mobile agent to be aware of every node's dependable neighbour. As a result, the node does not listen to the traffic coming from the enemy, and the level of safety is increased since the mobile agent also delivers the information directly to the base station. An alternate method for the detection of intrusions in ad hoc networks is presented in [23] Mobile agent approach is how the contemporary method is characterized. Before transferring the data, the mobile agent will first follow the adjacent node and then gather the information around them in order to determine the link between the anomalous models that have been found. This tactic ensures the protection of the currently active node, as well as the nearby node and the global network.

The primary advantage of the strategy that has been described is that it makes optimum use of the resources provided by sensor networks, which enables it to provide two levels of protection. When compared to the way that is currently being used, this solution offers the benefit of reducing the amount of cluster head resources that are used. Another benefit is a decrease in the required infrastructure, which results in an increased lifespan for the sensor network. [24] Concentrate their attention largely on the creation of a combined security solution that makes use of mobile agents. The proposed security solution makes use of mobile agents in order to provide fundamental security services and to defend against [25] multiple attacks, including Denial of Service attacks, HELLO Flood attacks, Traffic Analysis, cloning attacks, Sink Hole attacks, Black hole attacks, and Selective Forwarding attack, while requiring the same amount of energy as would be required to address a single Attack. Through the use of Wireless Node Agent, this research investigates the detection and prevention of cross-layer assaults in the application and network layers. WNA is the shorthand for Wireless Node Agent, which is a server that works with each node to detect network intrusion.

The two-ensemble learning algorithms that are used most often are known as Adaboost and Bagging. The ensemble's learning method can be broken down into three distinct phases: the generation phase, during which a set of candidate models is induced; the pruning phase, during which a subset of those models is selected; and the integration phase, during which the model outputs are combined to produce a prediction.

3. Proposed work

Incorporating new characteristics with machine learning algorithms may help reduce the number of false positives that occur while trying to identify cyberattacks. An effort was undertaken to identify the most effective machine learning algorithms, with the goal of detecting cyber threats with a higher level of precision than is now possible using these techniques. There are five ways to use machine learning to differentiate between legitimate and counterfeit websites: KNN, Decision Tree, Support Vector Machine, and Random Forest are some of the statistical methods that may be used.

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

Advantages of the Proposed System

The proposed system is comprised of a dataset that provides detailed information on a variety of cyber-attacks. This information may be used for the purpose of attack detection and prediction. The accuracy of the findings is taken into consideration when selecting which one to employ in the proposed technique, which makes use of a number of different machine-learning algorithms. For each method, metric values are created that may be regarded as the predicted results. When comparing the models, the Voting Classifier, which is an ensemble method, is used to provide results that are very accurate and error-free.

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

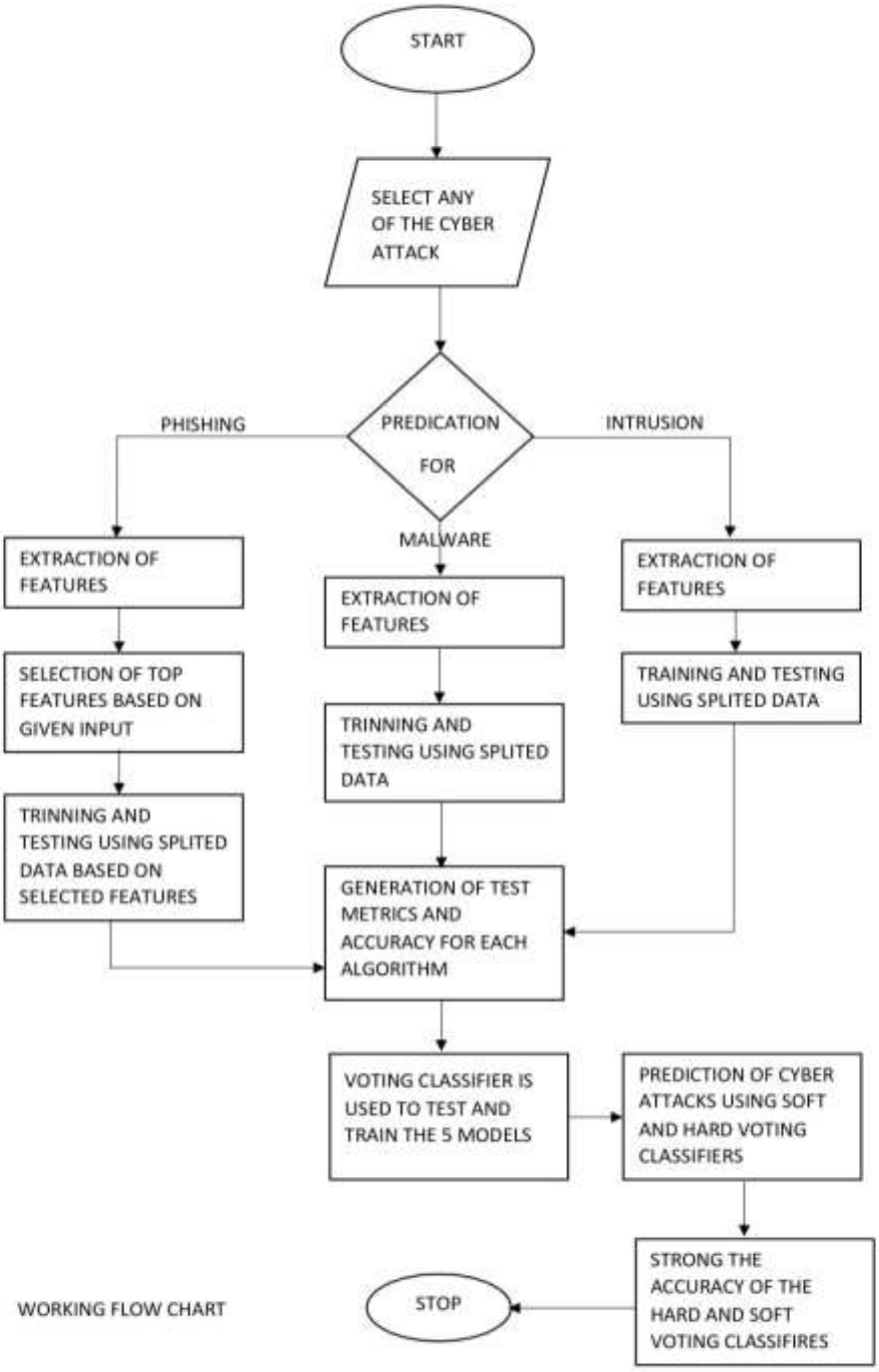

Figure 1: Flowchart

The system carries out the subsequent actions:

Step one: To begin the process, choose one of the cyber-attacks from the options, and it will go forward.

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

Step 2 requires the user to choose how many features to pick from in the event that the reported cyber-attack is an effort at phishing.
Step 3: The third step of the process involves the use of a predetermined dataset of cyber-attacks by the system in order to train and test a variety of machine learning algorithms and establish how accurate they are.
Step 4: The voting classifier is now being used with 5 models to compare all models in order to generate confidence.

DATASET PRE-PROCESSING

Any approach to machine learning that begins with some kind of data pre-processing either alters or encrypts the incoming data in order to make it easier for the computer to read and understand. To put it another way, the algorithm is able to quickly understand the characteristics of the input it is given. A collection of data items is referred to as a "dataset," however these objects may alternatively be referred to as "records," "points," "vectors," "patterns," "occurrences," "instances," "samples," "observations," or "entities." The word "dataset" refers to the grouping of these data objects. A number of features that characterize data items may capture the basic qualities of an object, such as its mass or the exact time at which an event took place. This is possible because a number of features defines data items. A feature may also be referred to as a variable, characteristic, field, attribute, or dimension. These are just some of the common synonyms. There are several of them. We will utilize the Feature Selection for the Phishing dataset in order to narrow down the available features in the given dataset to only the most important ones. The dataset comprises a big number of different characteristics. There will be a delay in the processing of the data because of the magnitude of the datasets that are involved in the identification of malware and intrusions. Because of this, feature scaling is used in order to translate the values of the dataset.

PHISHING DETECTION
Once the data has been processed and the features have been selected, the next step is to test and train the most important characteristics using five different kinds of algorithms. To do this, we take 75% of the dataset and use it for training, and we use the remaining 25% for testing. Accuracy and standard value information are both produced and stored by algorithms.

INTRUSION & MALWARE DETECTION
Because of the quantity of the datasets that are required to identify viruses and incursions, the datasets are altered such that the values range from 0 to 1. In order to achieve this goal, the Feature Scaling approach is used. As soon as the values have been translated, the procedures of training and testing will get underway using 25% of the dataset for testing and 75% of the dataset for training respectively. As shown in Figure 3, each of the five algorithms is responsible for the generation, storage of metric, and accuracy data.

VOTING CLASSIFIER
Testing is carried out utilizing datasets, employing five distinct models, and a comparison of hard voting and soft voting based on probabilities is carried out.

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

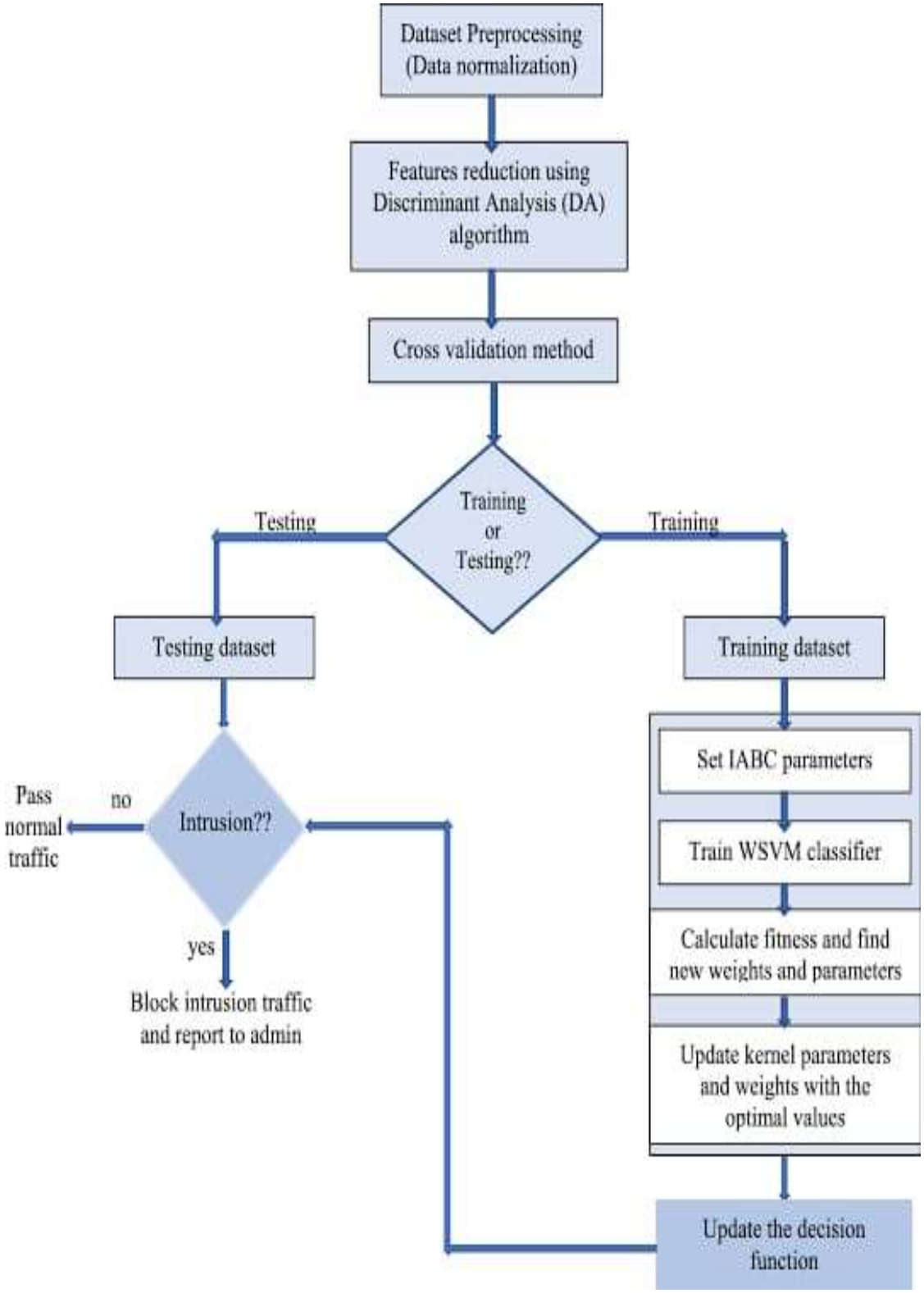

Figure 2: Methodology of Intrusion Flowchart

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

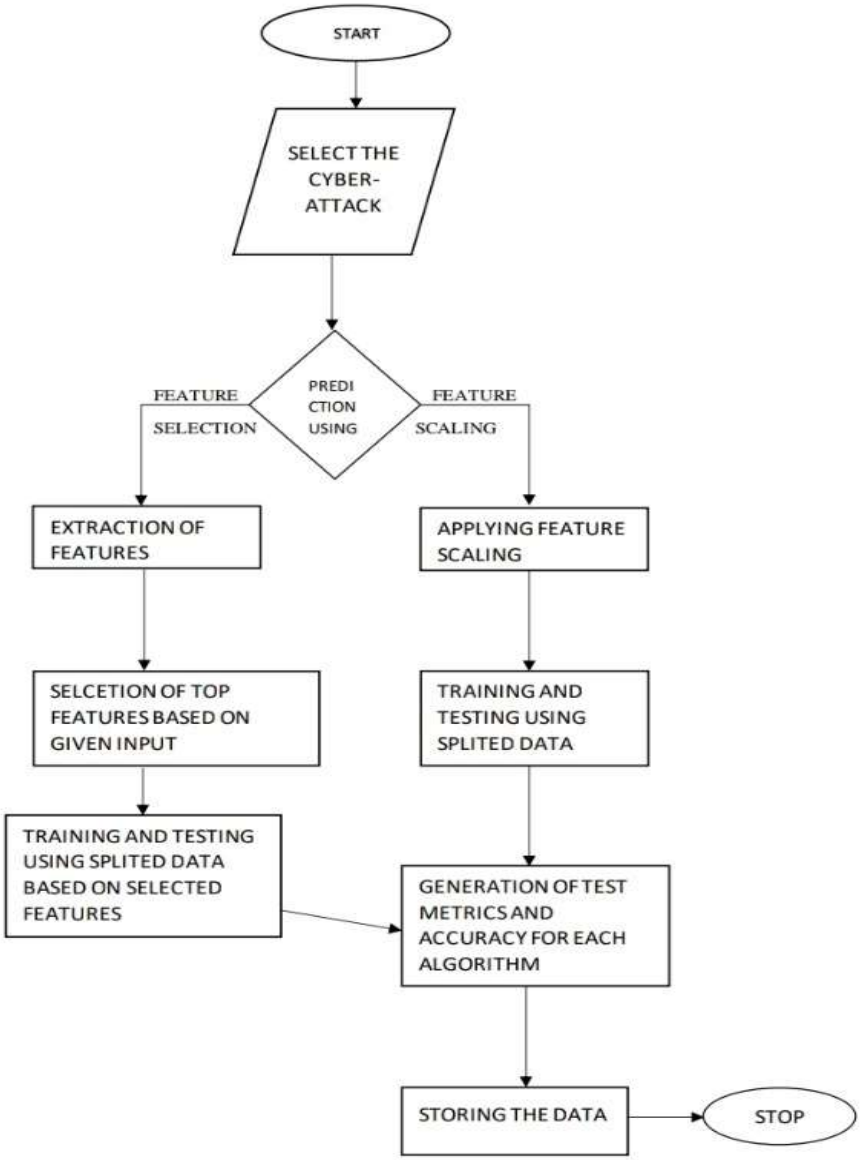

Figure 3: Flowchart of Malware and Intrusion

Upon recognizing the threat, the suggested mitigation scheme will be applied further. Since several attacks can be used collectively, the mitigation element is confronted with the problem of the lower strategy area. The simple protection process that targets one of the subs – attacks may drop into another's purse, and thus suffer in either safety or achievement. As there is a possibility that the attack plan can degrade the network's usual activity and degrade the performance of the network, it is necessary to optimize the security & effectiveness of the network. To deal with this, we have allowed the attack reduction component to determine strategy R, which optimizes the compromise between the efforts made by the defendant and the desired security level. We identify the security feature for this purpose.

$$h(R_k, T_k) = \alpha E[U(M_k)] - \beta E[G(M_k)]$$
$$h(R_k, T_k) = \alpha E\left[U\left(q(R_k, T_k)\right)\right] - \beta E\left[G\left(q(R_k, T_k)\right)\right]$$

Where R and T are strategies for defenders and attackers like power allocation, next hop selection, etc.

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

The expected utility $E[U(M_L)]$ reflects output and the negative gain $E[G(M_k)]$ is security. Note that $E[U(M_k)]$ is accessible as a defender can assess their own

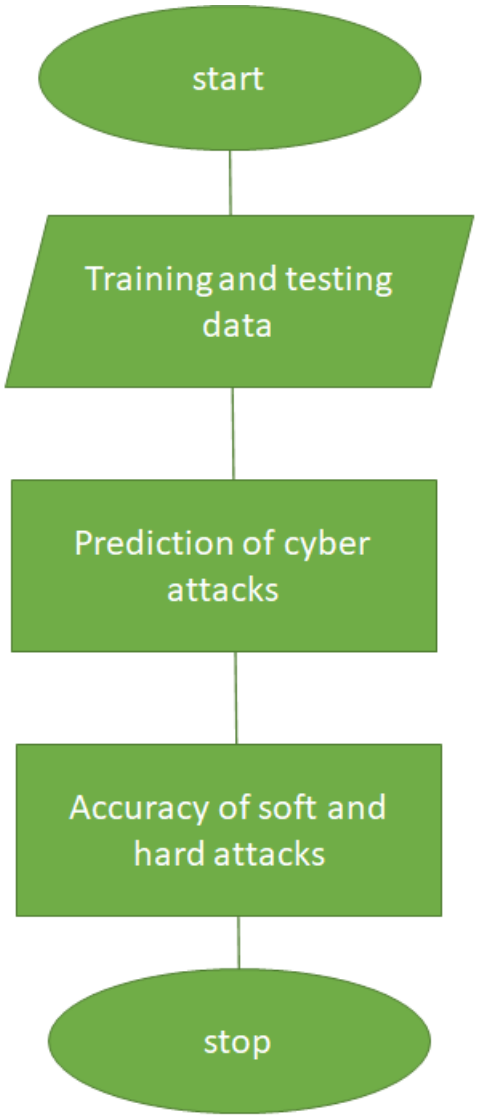

Figure 4: Flowchart of Voting Classifier.

E [G (M_k)] may not be measured immediately, but for a particular attack, an estimate can generally be made as soon as the model is obtained for attack operations. The maximal strategy is obtained from the below equation

$$\underset{R_k}{\text{Maximize}} \quad h(R_k, T_k)$$

Subject to

$$E[U(M_k)] \leq U_{th}$$
$$E[G(M_k)] \leq G_{th}$$

Where α and β are two variables, that must be controlled to compromise security and performance. The defender can control the required compromise between reliability and security by changing the value of α andβ. Based on the application, the value may vary. For instance, a video streaming application typically needs high performance, but a low level of safety while a wireless network of sensors that collects scientific data generally involves an elevated amount of safety, but can withstand a low data rate.

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

4. SIMULATION ENVIRONMENT

The performance of the proposed scheme was evaluated using network simulator NS2 and the performance is compared with malicious AODV and BLAD Protocol. The network deployed in the area of 500 m height and 500 m width is considered. 50, 100, 150, and 200 nodes were positioned randomly in the network area of 500m with a random topology. The Wi-Fi data rate is around 2Mps. Constant Bit Rate (CBR) with UDP source and sink is the simulated traffic with the size of the data payload of 512 bytes. Every single node in the wireless network system is set up with an Omni-directional antenna that transmits or gets the signals from the nodes around it. The MAC layer protocol is selected as IEEE 802.11 standard for the wireless LAN. The propagation and physical model are chosen as two ray ground and wireless pi respectively with the antenna model of Omni directional antenna.

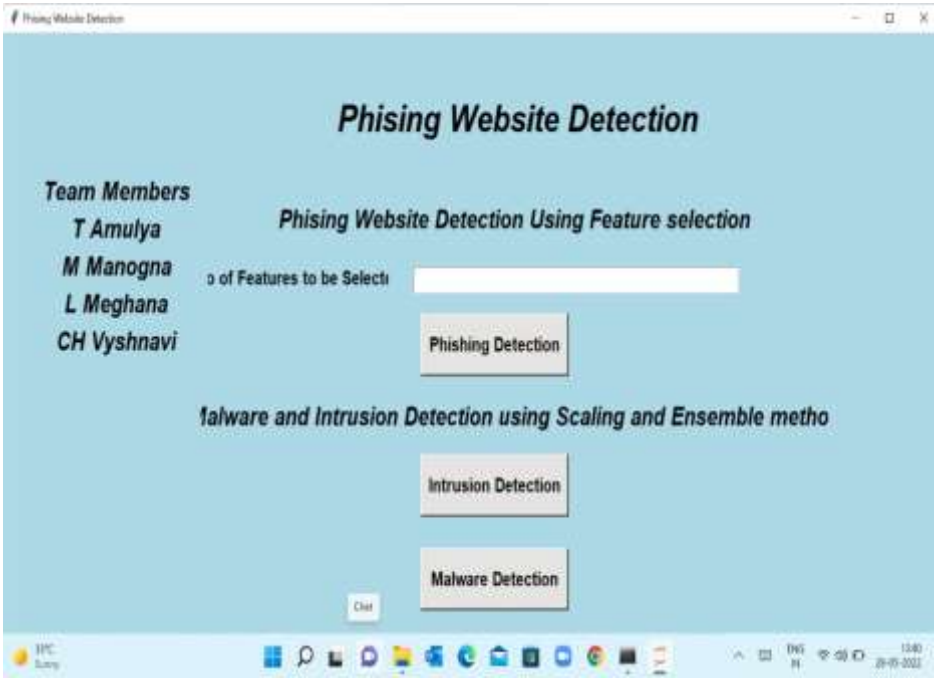

Figure 5: phishing Website Detection first page

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

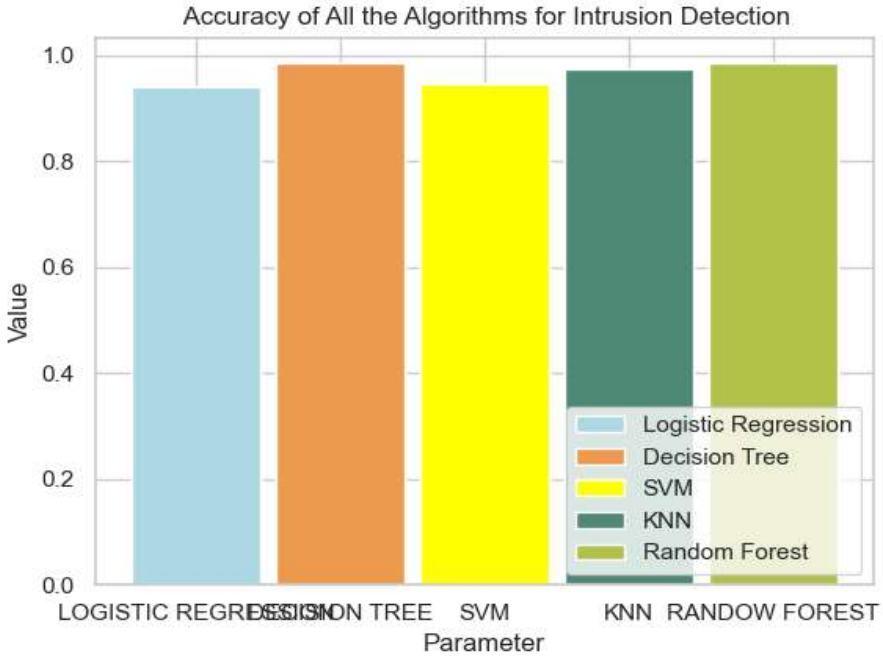

Figure 6: Average accuracy for Intrusion detection

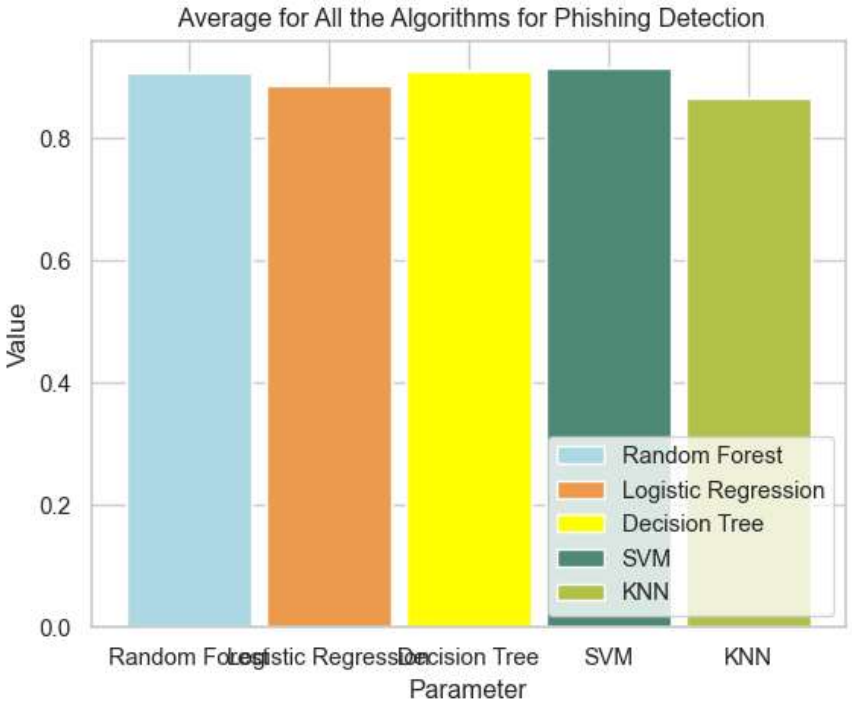

Figure 7: Average phishing detection accuracy

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

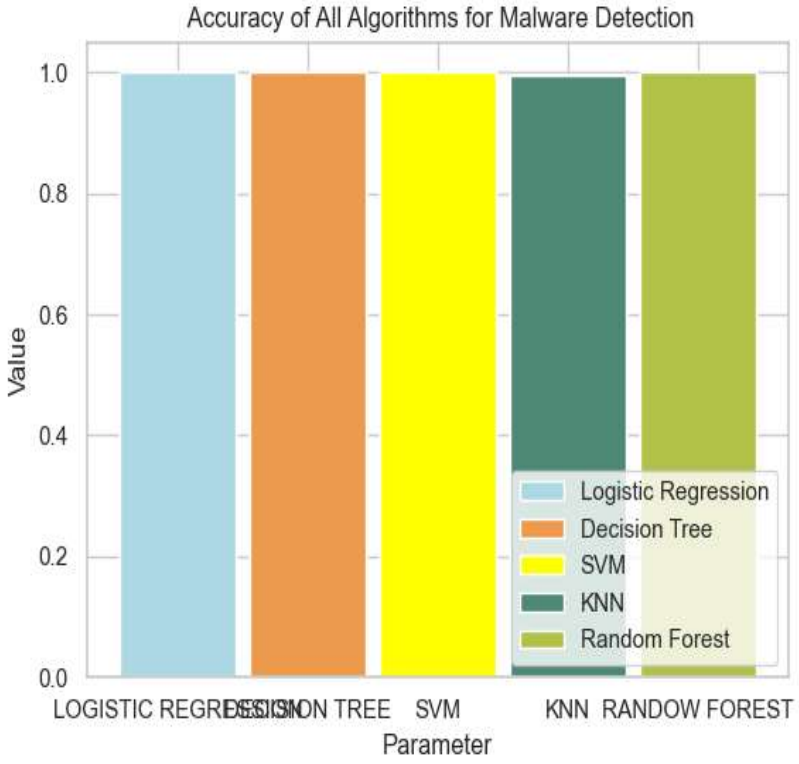

Figure 8: Average malware detection accuracy

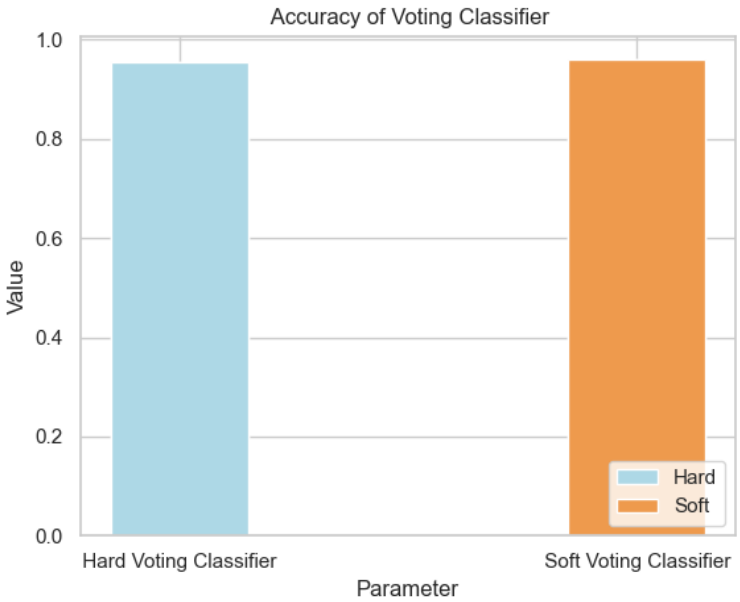

Figure 9: Reliability of voting classifier

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

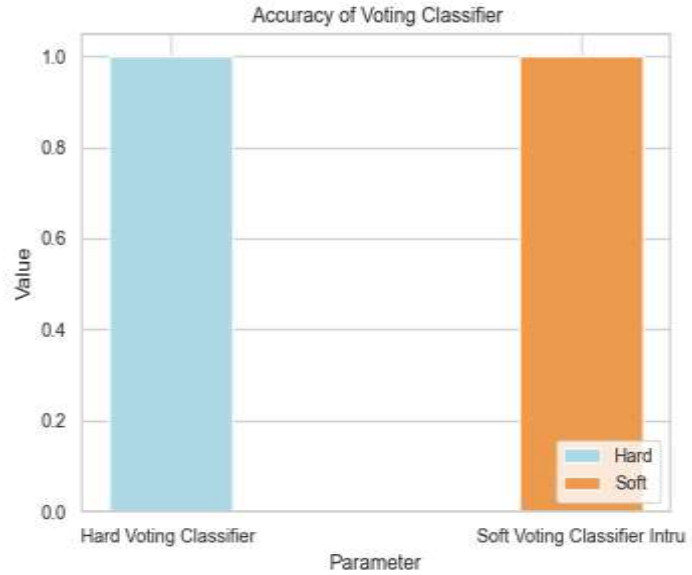

Figure 10: Accuracy of a voting classifier for detecting phishing

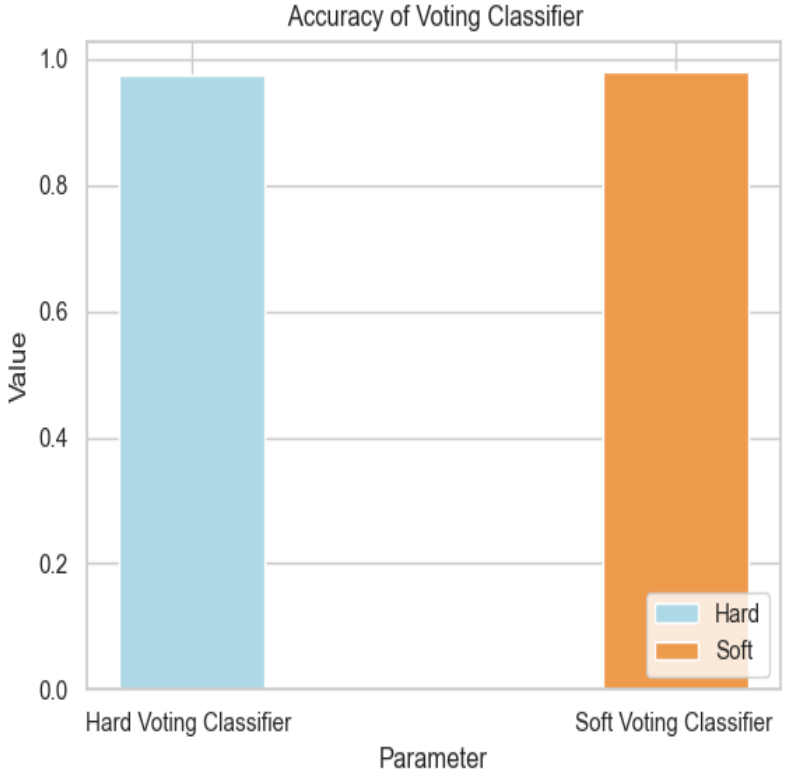

Figure 11: Reliability of intrusion detection.

A learning-based strategy was used successfully in this part to identify the poisoning attack in the MAC layer. Jamming in the physical layer is employed as a supplementary way to limit node throughput in the MAC layer. Utilizing the aforementioned strategy allows for the effective detection of attack actions on various layers, based on the previous information as well as the evidence that has been seen.

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

As part of the process of monitoring the assault, a model of the evidence that was captured and used to identify the covert attack operation is being developed. The optimization concept is used in order for the preventive element to successfully achieve the needed balance of protection and dependability in its operations. Because of this, the learning-based detection method may make use of several layers of observations to form an educated prediction as to whether or not a certain assault takes place. These multi-layer observations on the assaults are saved in the data bank of each node and utilized by the detection agent at the application and network layers to observe the activities of each node respectively. When malicious behavior was identified by signature matching, the reaction agent would bring the node back from the harm it had sustained.

5. Conclusion

Cybercrime techniques such as phishing, malware, and intrusions use online services to steal people's personal information. To give the algorithm the best accuracy, the system uses phishing websites, malware detection, and the KDD dataset while applying several categorization techniques. Unsupervised machine learning algorithms identify cyber-attacks more effectively than supervised machine learning algorithms, so in the future, we hope to use them to design and host websites.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] SomaiyaVidyaviharet.all, Phishing Website Detection using Machine Learning,IJCA, Volume 181-No.23,October 2018.
[2] Sadeh N, Tomasic A, Fette I. Learning to detect phishing emails. Proceedings of the16th international conference on World Wide Web. 2007: p. 649-656
[3] AndrBergholz, Gerhard Paa, Frank Reichartz, Siehyun Strobili, and SchloBirlinghoven. Improved phishing detection usingmodel-based features. In FifthConference on Email and Anti-Spam, CEAS, 2008
[4] UCI Machine Learning Repository." http://archive.ics.uci.edu/ml/, 2012.
[5] H. A. Chip man, E. I. George, and R. E. McCulloch.BART: Bayesian AdditiveRegression Trees. Journal of the Royal Statistical Society, 2006. Ser.B,Revised.
[6] S. Nawafleh, W. Hadi (2012). Multi-class associative classification to predictingphishing websites. International Journal of Academic Research Part A; 2012;4(6),302-306J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2.Oxford: Clarendon, 1892, pp.68–73.
[7] P. Tiwari, R. Singh International Journal of Engineering Research &Technology (IJERT) ISSN: 2278-0181Vol. 4 Issue 12, December-2015.
[8] J. P. Marques de Sa. Pattern Recognition: Concepts,Methods and Applications. Springer, 2001.
[9] D. Michie, D. J. Spiegelhalter, and C. C. Taylor. Machine Learning, Neural and Statistical Classication. Ellis Horwood, 1994.
[10] L. Breiman. Random forests. Machine Learning,45(1):5{32, October2001
[11] Mrs. Sayantani Ghosh, Mr. Sudipta Roy, Prof. Samir K.Bandyopadhyay, "A tutorial review on Text Mining Algorithms".
[12] Mauro Ribeiro, Katarina Grolinger, and Miriam AM Capretz. 2015. Mlaas: Machine
    a. learning as a service. In Proceedings of the 2015 IEEE 14th International Conference on
    b. Machine Learning and Applications (ICMLA). IEEE, Miami, FL, USA, 896–902.

[13] Ahmed Salem, Yang Zhang, Mathias Humbert, Pascal Berrang, Mario Fritz, and Michael Backes. 2019. ML-Leaks: Model and Data Independent Membership Inference Attacks and Defenses on Machine Learning Models. In Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS). IEEE, San Diego, California, USA, 1–15.

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022

[14] Ferdinando S Samaria and Andy C Harter. 1994. Parameterisation of a stochastic model for human face identification. In Proceedings of the Second IEEE Workshop on Applications of Computer Vision. IEEE, Sarasota, FL, USA, 138–142.
[15] AMAZON ML SERVICES. 2019. Amazon aws Machine Learning. https://aws.amazon.com/machine-learning/
[16] Snehkumar Shahani, Jibi Abraham, and R Venkateswaran. 2017. Distributed Data Aggregation with Privacy Preservation at Endpoint. In Proceedings of the IEEE International Conference on Management of Data. IEEE, Chennai, India, 1–9.
[17] Richard Shay, SarangaKomanduri, Adam L Durity, Phillip Seyoung Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2014. Can long passwords be secure and usable?. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, Toronto, ON, Canada, 2927–2936.
[18] Reza Shokri and Vitaly Shmatikov. 2015. Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, Denver, Colorado, USA, 1310–1321.
[19] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. 2017. Membership inference attacks against machine learning models. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP). IEEE, San Jose, CA, USA, 3–18.
[20] Amit Kumar Sikder, Hidayet Aksu, and A SelcukUluagac. 2017. 6thsense: A context-aware sensor-based attack detector for smart devices. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17). USENIX Association, Vancouver, BC, Canada, 397–414.
[21] Tom W Smith, Peter Marsden, Michael Hout, and Jibum Kim. 2012. The General social surveys. Technical Report. National Opinion Research Center at the University of Chicago
[22] Raphael Spreitzer, Felix Kirchengast, Daniel Gruss, and Stefan Mangard. 2018. ProcHarvester: Fully automated analysis of procfs side-channel leaks on Android. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security (AsiaCCS). ACM, Incheon, Republic of Korea, 749–763.

[23] NedimSrndic and Pavel Laskov. 2014. Practical evasion of a learning-based classifier: A case study. In Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP). IEEE, San Jose, CA, USA, 197-211
[24] Johannes Stallkamp, Marc Schlipsing, Jan Salmen, and Christian Igel. 2012. Man vs. computer: Benchmarking machine learning algorithms for traffic sign recognition. Neural networks 32 (2012), 323–332.
[25] Jingchao Sun, XiaocongJin, Yimin Chen, Jinxue Zhang, Yanchao Zhang, and Rui Zhang. 2016. VISIBLE: Video-assisted keystroke inference from tablet backside motion. In Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS). IEEE, San Diego, CA, USA

DOI: https://doi.org/10.54216/IJWAC.060202

Received: September 08, 2022 Accepted: November 03, 2022