International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Performance Evaluation of Intrusion Detection System for Smart Devices using Neural Network Classifiers

Gopala B[1], Hanumanthappa M[2]

[1]Research Scholar, Department of Computer Science & Applications, Bangalore University, Bangalore, Karnataka, India

gopala.nishanth[at]gmail.com

[2]Professor, Department of Computer Science & Applications, Bangalore University, Bangalore, Karnataka, India

hanu6572[at]hotmail. com

Abstract: ***The multiple security threats arising in smart devices cause more computing power and reduce storage capabilities. Authentication and Encryption methods are not adequate to provide enough security for a smart device. An intrusion detection system improves protection and uses few resources on the smart device. An Intrusion Detection processwas proposed to detect intrusions in smart devices in a cloud environment using Data Mining techniques. A Network - based approach is used to eliminate the overhead dispensation from smartphones. A neural network classifieris implemented for all user call logs. A technique that runs on a smartphone of the user collects information from the user and transfers it to the remote server. These call logs are then moved to the already qualified classifier which analyzes. The ogs and sends back the feedback to the smartphones whenever abnormalities are found. The different neural classifiersare used to identify the classifier with better performance using the Weka data mining tool.***

Keywords: Intrusion detection system, neural network, cloud computing, Weka

1.Introduction

The quality infrastructure and affordability of mobile networks made smartphones popular and fast - growing communication devices. As the data transmissions are affordable and easily available smartphones are used for online transactions and mobile learning. For smartphones, there are a variety of third - party applications accessible for free on Google Play. The ease with which attackers can create dangerous applications for smartphones is due to the widespread availability of applications [1].

Smartphones have some limitations like using firewalls and antivirus scanners on smart mobile devices makes difficult its operations because battery endurance and computing power are both insufficient.

To get beyond these constraints, cloud computing offers a variety of services. It significantly reduces bandwidth and power consumption in mobile phones. Because of cloud computing, the dynamics of safeguarding smartphones through the network are changing, which detects network misbehavior and sends a reaction signal to the smartphone device.

In the existing system, antivirus softwareis used to protect smartphones which consume more battery power even in standby mode. The detection range of antivirus software is limited to the data set accessible to the software. The amount of data that must be updated regularly, have an impact on bandwidth efficiency [2].

2.Types of Mobile Phone Attacks

2.1 Malware

Malware is software that is meant to obtain unauthorized access to a computer system without the knowledge of the owner. Malware on a mobile device can obstruct normal operations by consuming more power, memory, and input and output resources, or simply cause the device to stop responding to user input, exposing personal information to unauthorized parties. It is capable of deleting or altering data on the device, as well as initiating undesired interactions. The device's owner often purchases information transmission. For example, spyware could cause the device to dial an expensive service [4].

2.2 Trojan

Trojan programs are the most common type of malicious assault. An electronic device Trojan that sends spam emails to Internet users is fairly widespread these days. This will degrade network performance and cause a slew of other problems for users, but there will be no straight cost to them. A Trojan on a cell phone, on the other hand, could cost the customer a lot of money. Consumers will not get mobile bills for another 30 days after discovering that their phone has been infected with a computer virus [6].

2.3 Worm

The development of a self - replicating mobile application is the second point of attack. A Trojan horse is frequently used to create this form of computer malware.

3.Methods of Intrusion Detection

Despite the sort of recognition method utilized, the intrusion detection system is dependent on the variety ofdata provided as key to the detection techniques. Intrusion detection solutions are usually classed as either host - based or networkbased on the kind of monitoring facts used. Network data, such as network traffic and data packets, is used to detect intrusions. In contrast, data from the mobile device, such as system events, CPU activity, utilization of RAM, file input or output activity, network input or output activity, and operating system information, is used in host - based intrusion detection [8].

3.1 Network - Based IDS

Advantages:

- The mobile phone's surplus processing is minimized.
- Intrusions from the outside are detected.

Disadvantages:

- On the smartphone, there is no access to monitoring data used for recognition.
- The communication atmosphere is highly scrappy because of connectivity to various sources on multiple interfaces.
- On the device itself intrusions, such as malware, are not detectable.
- It's not easy to collect all essential network - based monitoring data for every part of networks and communication interfaces.

3.2. Host - Based IDS

Advantage

As the information obtained from the mobiles closely matches the behavior of devices, the intrusion detection process using host - based data gathering produces more precise and dependable outcomes than other approaches.

Disadvantage

Smartphones are resource - constrained devices. Host - based intrusion detection is not so feasible for smartphones.

4.Intrusion DetectionTechniques

- **Anomaly Detection:** - The Anomaly detection is a significant tool for detecting deceit network intrusions and additionaldifficult - to - find events. Anomaly detection does not necessitatepreviousfacts of an intrusion to detect freshintrusions. The core problem is unable to describe the nature of the attack, resulting in high false positivesrates [9].

- **Misuse Detection:** - By using the patterns of known attacks' low - security locations in the system, misuse detection systems compare and identify known invasions. To detect misuse, the IDS analyses the data and compares it tovast databases of threat signatures. The Intrusion detection model searches for a detailedassault that was previously reported. Signatures for the "guessing password assault, " for example, are frequently "at least for unsuccessful login attempts within 2 minutes. " The benefit of misuse detection is it able toperfectly and rapidly detect instances of recognized assaults. The drawbackis it unable todetect truly novel assaults[9].

5.Proposed Intrusion Detection Method

Misuse detection systems compare and contrast information. The creation of a novel data mining technique for identifying mobile phone system intrusion. Some worms can access calls from a cell without the operator's knowledge. These types of malware can too send money transfer requests via text messages or phone calls without the user's knowledge. Because such attacks are difficult to detect, the user may not be aware of them until the end of the month when she receives her bill. As a result of the telecom provider's actions, the consumer will also incur a loss. Instead of waiting until the end of the month to detect these types of attacks, the new approach will detect them immediately and notify the user of known incursions by matchingthem with patterns of known attacks or low secured regions in the system. The IDS examines the processed data it gathered and compares it to wide databases of information.

The call records of users who desire to utilize this service are collected, and a classifier is created for that user. The user's call logs are used to train the classifier. On the user's computer, the software will be installed. This software on the user'scell phone will upload the decision logs to the isolated servers every day at a certain time. The uploaded call records are then analyzed and fed into a classifier that has already been trained. The already trained classifier will be aware of the user's typical behavior. The classifier checks these call logs and, if any anomalies are identified, the classifier notifies the user, who can then choose to receive an e - mail or text message as shown in figure 1.

Only observed irregularities that are greater than a certain threshold value are sent to reduce false alarms.

A network - based strategy is employed for the phone logs collected by a program that existson theportable device and transfers phone logs data to the isolated server. This frees up the mobile's processing power, allowing the limited battery capacity and hence computer resources to be put to better use.

To classify the call logs, the Nave - Bayes neural network classifier and J48 classifiers are tested to evaluate which classifier delivers the best results. The Weka Data Mining tool is used to run simulations. The various user call logs are gathered to see how the amount of the collection affects performance. The performance of the classifier was evaluated using a ten - fold cross - validation method.

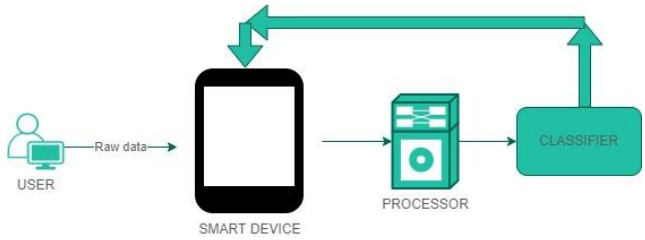

Figure 1: System Architecture

6.Simulation

The results of the simulations detectionof intrusions efficiently and effectively by neural network classifiers. The Weka Data Mining tool employs the neural network classifiers Naive - Bayes and J48. The information is gathered from many sources.

ProcessedData Files (. arfffiles):

WekarecognizesARFF format. The results of the simulations indicate the efficient and effective process of intrusion detection by neural network classifiers. The Weka Data Mining tool employs the neural network classifiers Naive - Bayes and J48. The informationwas gathered from many sources are in. ARFFformat. Below mentioned some examples of the model. ARFF data file

[at]relationlogssimplified

[at]attribute day{Mon, Tue, Wed, Thu, Fri, Sat, Sun}

[at]attributeminutes numeric

[at]attribute type of call {LO, LD, IL}

[at]attribute time {AM, PM, EV, NI, MN}

[at]attributeclass {no, yes}

[at]attribute whatsapp {voice, video}

[at]Data

Table 1: Call List

Day	Duration	Time	Type	Class	WhatsApp
Mon	1	AM	LD	NO	voice
Mon	16	EV	LO	NO	video
Thu	4	AM	LO	YES	Video
Thu	2	PM	LD	NO	Voice
Thu	2	PM	LO	NO	Voice
Fri	3	EV	LD	YES	Voice
Fri	4	EV	LD	YES	Video
Sat	1	EV	LD	NO	Video
Fri	2	EV	LD	NO	Voice
Fri	1	PM	LO	NO	Video

For classification, the Naive Bayes classifier and J48 classifiers are employed to see which classifier performs better.

10 - fold cross - validation is a machine learning technique that is used to check the prediction of data by a learning systemthat hasn't been trained. The dataset for training is arbitrarily divided into ten groups, with the first nine groups being used for classifier training and the last group being used to test the classifier. The process is replicated until all of the sets have been covered, and the entire performance is calculated by adding all 10 folds together.

7.Results

The results of experiments are classified as either positive (YES) or negative (NO). The result is referred to as true positive if both the actual value and forecast are YES and the result is referred to as false positive if the true value is NO. A true negative (TN) occurs when the forecast value and the actual value do not match, whereas a false negative (FN) occurs when the forecasted result is none and the actual value is YES.

The true positive rate (TPR) and the false positive rate (FPR) are required to construct a ROC curve (FPR). The TPR builds a classifier by correctly categorizing positive samples from available positive samples during the test. The false - positive rate is the percentage of false positives that appearedamid all negative samples accessible throughout the test. The formulas to find FPR and TPR.

TPR = TP / (TP + FN)
FPR = (FP + TN) / FP

The good prediction approach would result in some extent within the upper left angle of the ROC space or coordinate (0, 1), suggesting 100 percent sensitivity and 100 percent specificity. The ROC curve for each user is plotted to investigate the classifier's performance. Figure 2 represents the ROC curve using the Naïve - Bayes classifier and figure 3 represents the ROC curve using the J48 classifier.

Naïve - Bayes Classifier

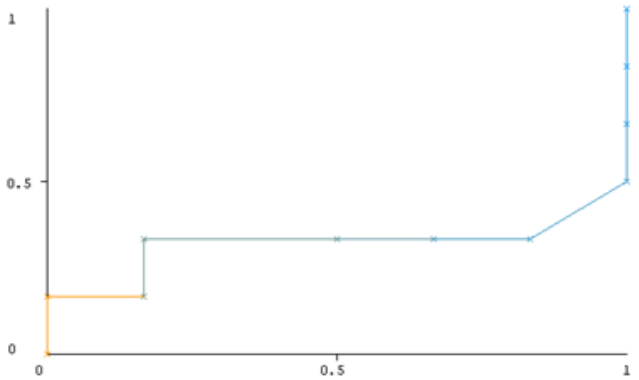

Figure 2: Performance using Naïve Bayesclassifier

The J48 classifier

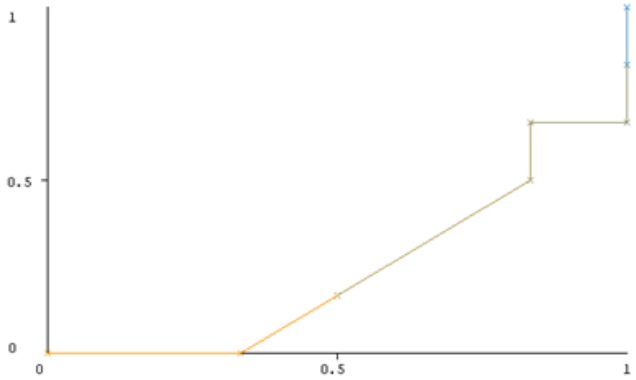

Figure 3: Performance using J4 classifier

Comparision between Naive - Bayes and J48 classifiers

Users	Correctly Classified Instances % (Naive - Byes)	Correctly Classified Instances % (J48)
User 1 (whatsapp)	58.33	33.33
User 2 (whatsapp)	65	45
User 3 (time)	45	40
User 4 (time)	64.28	53.57
User 5 (Type of call)	75	75

8.Conclusion

An intrusion detection system that uses data mining techniques and real - time user data to detect intrusions in smartphones. The Naive - Bayes and J48 classifiers are effective at detecting intrusions. The classifiers outperformed the humans by more than 90%. The Naive - Bayes classifier, on the other hand, outperforms the J48. Smart phones' processing overhead is reduced because of the network - based approach.

References

[1] Al - Maksousy, H. H., Weigle, M. C., & Wang, C. (2018). NIDS: Neural Network - based Intrusion Detection System.2018 IEEE International Symposium on Technologies for Homeland Security (HST). https: //doi. org/10.1109/ths.2018.8574174

[2] Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019). AD - IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning.2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). https: //doi. org/10.1109/ccwc.2019.8666450

[3] Chamou, D., Toupas, P., Ketzaki, E., Papadopoulos, S., Giannoutakis, K. M., Drosou, A., &Tzovaras, D. (2019a). Intrusion Detection System Based on Network Traffic Using Deep Neural Networks.2019 IEEE 24th International Workshop on Computer - Aided Modeling and Design of Communication Links and Networks (CAMAD). https: //doi. org/10.1109/camad.2019.8858475

[4] Elsayed, N., Zaghloul, Z. S., Azumah, S. W., & Li, C. (2021). Intrusion Detection System in Smart Home Network Using Bidirectional LSTM and Convolutional Neural Networks Hybrid Model.2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS). https: //doi. org/10.1109/mwscas47672.2021.9531683

[5] Midzic, A., Avdagic, Z., &Omanovic, S. (2016). Intrusion detection system modeling based on neural networks and fuzzy logic.2016 IEEE 20th Jubilee International Conference on Intelligent Engineering Systems (INES). https: //doi. org/10.1109/ines.2016.7555118

[6] Moloja, D., &Mpekoa, N. (2017). Securing M - voting using cloud intrusion detection and prevention system: A new dawn.2017 IST - Africa Week Conference (IST - Africa). https: //doi. org/10.23919/istafrica.2017.8102318

[7] Roopak, M., Yun Tian, G., & Chambers, J. (2019). Deep Learning Models for Cyber Security in IoT Networks.2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). https: //doi. org/10.1109/ccwc.2019.8666588

[8] Tama, B. A., & Rhee, K. H. (2017). Performance evaluation of intrusion detection system using classifier ensembles. International Journal of Internet Protocol Technology, 10 (1), 22. https: //doi. org/10.1504/ijipt.2017.10003843

[9] Verma, A. K., Kaushik, P., &Shrivastava, G. (2019). A Network Intrusion Detection Approach Using Variant of Convolution Neural Network.2019 International Conference on Communication and Electronics Systems (ICCES). https: //doi. org/10.1109/icces45898.2019.9002221

[10] Yadav, N., Pande, S., Khamparia, A., & Gupta, D. (2022). Intrusion Detection System on IoT with 5G Network Using Deep Learning. Wireless Communications and Mobile Computing, 2022, 1–13. https: //doi. org/10.1155/2022/9304689
[11] Yeh, H. T., Chen, B. C., & Wu, Y. C. (2012). Mobile user authentication system in cloud environment. Security and Communication Networks, 6 (9), 1161–1168. https: //doi. org/10.1002/sec.688
[12] Zhang, Y., Chen, X., Jin, L., Wang, X., &Guo, D. (2019). Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data. IEEE Access, 7, 37004–37016. https: //doi. org/10.1109/access.2019.2905041