Detection of Cyber Attacks on Android and IOS

Shewale Harshali Kailas[1]

Research student, Department of Information Technology, B.K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan

---

Abstract - *Cyberattacks are the biggest problem in today's scenario. It interrupts the mobile apps and hacks networks. People are widely using online payment which is risky nowadays because of cyberattacks. Android is used popularly so attacks mostly happen on android cell phones. It is mandatory to detect cyberattacks for protecting personal information. Android provides openness and customization. Using android users can share data, communicate, and reuse functions. Users can mistakenly give access to malicious program then their personal information is corrupted. People are widely using IoT devices which are connected to networks accordingly usage of Android OS and IOS is increased. Mobile devices were used for business data, private areas, text messages, and contacts so cyberattacks are also increased.*

Keywords: -

Cyberattacks, android, detection, cybersecurity, network, intrusion

I. INTRODUCTION: -

Mobiles were widely used in day to day life to make things easier. Mostly, people referred Android and IOS based operating systems because they are easy to use and cheaper. According to reported on google that a number of smartphone users are reached 4.77 million from the year 2013 to 2017 and now in 2020 there were 3.5 billion people were using smartphones. Android mobiles not only capturing attentions of people but also increasing risk of security i.e. Cyberattacks.

Cyberattacks are done by some cyber criminals using one computer against more than one computer to hack the personal data of user of another device. Online transactions created more risk for cybercrimes. Also, there were 70,000 malicious applications found on google play. The first attack was found on communication devices in 1971 and each new day one method attacking has been developed. There were so many types of cyberattacks happening daily which are phishing, botnets, spyware, financial malware attacks, worm based attacks. Detection of this attacks is major difficulty. There are some techniques which detects cyberattacks or malicious content in devices. Deep learning and Machine learning algorithms are widely used to detect cyberattacks.

Deep learning is a sub-field of machine learning concerned with algorithms inspired by the structure and functions of neural networks and successfully implemented in many areas. In this paper, I used Deep learning and machine learning algorithm to detect malicious packets in an online fashion. Through experimental results,

II. Related Work: -

There has been a rich literature dealing with the detection of cyberattacks. In particular, the authors in [1] proposed an overview based on the literature on smart cities' major security problems and current solutions. In smart cities, there was a vast chance for cyberattacks. The authors in [3] were detected cyberattacks using Deep Learning and stated that compared to other Machine learning approaches deep learning was more Accurate, Flexible, and Stable. The authors in [10] proposed a method to authenticate the encryption and detection of clones within some seconds. To protect the device from clone attack and to secure data proposed method was used by the author and the method was a device made of Arduino coded in C language then that device sends that information to the server and then server which is implemented in Python language shows authentication information. If it is successful data is stored in MongoDB. The authors in [11] proposed a comparison between evasion techniques that were used by malware authors. Malicious content and violating the google play Store security policy founded in 700,000 applications. The virus, worms, Trojans, ransomware, rootkits, botnet, etc. were categorized in which malware was grouped. Different cybersecurity attacks are explained with the detection techniques. The authors in [13] proposed two attack detection processes which were counter detection and bandwidth monitoring detection. According to the author networks of mobile able to detect cyberattacks. Confidentiality, Integrity, and availability are based on the security of computing systems. The authors in [14] proposed a model using deep learning used to learn attack features. Compared designed deep learning models with the other 4 machine learning algorithms and results shown a model which was proposed by the author had 6% accuracy. The authors in [16] proposed a network security visualization tool called Eyesim which detects anomaly identifies wormhole attacks and alerts about the presence of wormhole attacks. Eyes detect multiple wormhole attacks accurately. The authors in [19] proposed mobile computing environments, analyses the security considerations about Smishing. S-Detector distinguishes the Smishing message and normal text message. The system used a morphological analyser and Naive Bayesian classifier of machine learning. The authors in [22] proposed a detection method for attacks of JFC (Juice filming charging) by analysing CPU usage. The author collected 187 participants data and the SVM classifier shows better performance. The author interviewed 103 participants in the laboratory of Denmark and China. The authors in [24] presented lightweight IDS for the detected malicious behaviour of Android devices enhanced with a powerful MLP neural network. Accuracy reaches 85.02% and 81.39%. The authors in [29] proposed the accuracy of the unsupervised technique which was 97.87%, supervised technique which was 97%, and semi-supervised which was 97.3%. Clustering was performed in the unsupervised technique. K-means, Droid Mat, KNN, Singular value decomposition was applied on a sample of 238 applications had an accuracy of 97.87%. The author in [31] proposed analysis in WEKA software, multi-layer perceptron (MLP) performs better in terms of recall, f-measure, and accuracy, precision.

III. Methodology: -

A]Dataset collection and evaluation methods: -

1)Dataset Collection: -
To verify the accuracy of machine learning cyber attack detection I used 2 public datasets.
KDDcup 1999 Dataset: - The KDDcup 1999 dataset [32] is widely used as a benchmark for the intrusion detection network model. Each record within the dataset contains 41 features and is labelled as either normal or a selected sort of attack. The training dataset contains 24 sorts of attacks, while testing dataset contains additional 14 types.

2) Evaluation Methods: -In this study, I use accuracy, precision, and recall which are parameters used in machine learning (deeplearning.net) as performance metrics to evaluate the deep-learning cyber-attack detection model.

B] Proposed system: -

The main purpose of this proposed system is to detect cyberattacks and identify what type of attacks.

Random Forest Classifier: -Algorithm is implemented using random forest classifier. It is used for classification and regression technique. As compared to other machine learning algorithm like Support vector machine, Logistic regression, Naive Bayes, K-nearest neighbour, Decision tree, linear discriminant analysis, and Random forest classifier is more flexible and give more accuracy with less number of dataset. Following is the architecture of proposed algorithm:

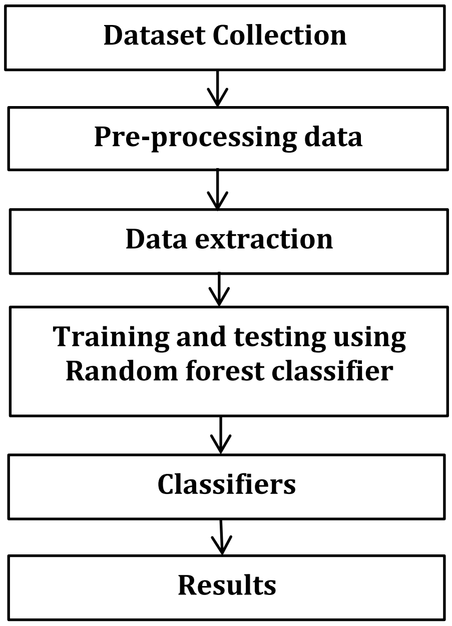

Fig. 1: Process for the proposed system

The proposed work uses a decision tree to identify the cyberattacks. The proposed work is based on the behaviour of the attack type. Fig. 1 describes the step by step process for the proposed system.

In the first step, KDDcup 1999 dataset is collected. In the second stage i.e. Pre-processing is the request to fit the models. It enhances the performance of our model.

In the third step, Data extraction is done means collecting different types of data from a variety of sources, many of which may be not organized properly which is transferred in an organized manner. In the fourth step, random forest classifier algorithm is applied on dataset algorithm is examined based on accuracy and execution time. In the fifth step, classifiers are used and in the last step types of attacks are demonstrated.

IV. EXPERIMENTAL RESULT

A] Visualizations of Datasets: - In fig.2 dataset is visualised using types of attacks. It illustrates mostly attacks are of dos type and some are of normal category.

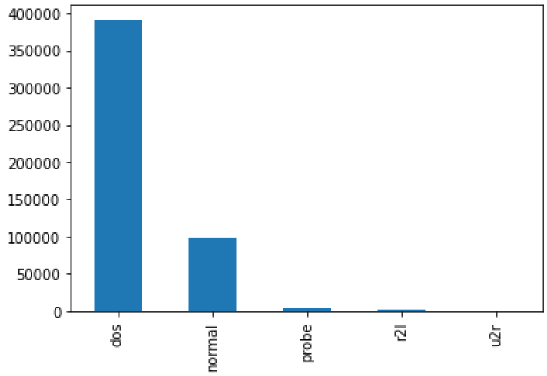

Fig-2: Types of attacks in KDD cup1999 dataset

Fig.3 explains training accuracy of KDD cup 1999 dataset.

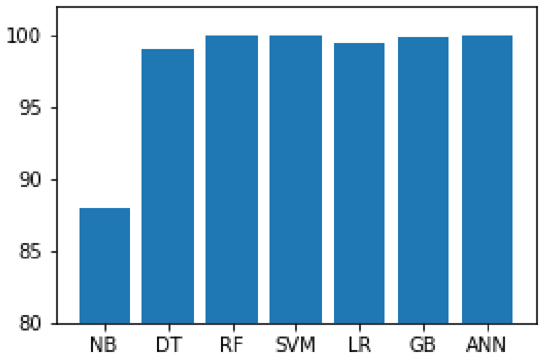

Fig-3: Trainig accuracy of KDD cup 1999 dataset

Fig.4 explains testing accuracy of KDD cup 1999 dataset.

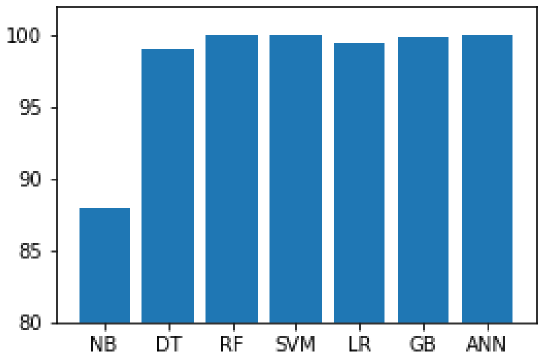

Fig-4: Testing accuracy of KDD cup 1999 dataset

Machine learning model	Training Accuracy	Testing Accuracy
Gaussian Naive Bayes(NB)	87.951%	87.903%
Decision Tree(DT)	99.05%	99.05%
Random Forest(RF)	99.99%	99.96%
Support Vector Machine(SVM)	99.87%	99.87%
Logistic Regression(LR)	99.35%	99.35%
Gradient Boosting Classifier(GB)	99.79%	99.77%
Artificial Neural Network(ANN)	99.77%	99.75%

Table-1: Comparison between training testing accuracy of different machine learning models

As shown the in Fig.3 and 4 an accuracy of 99% is achieved using Random forest classifier which is more as compared to other machine learning models.

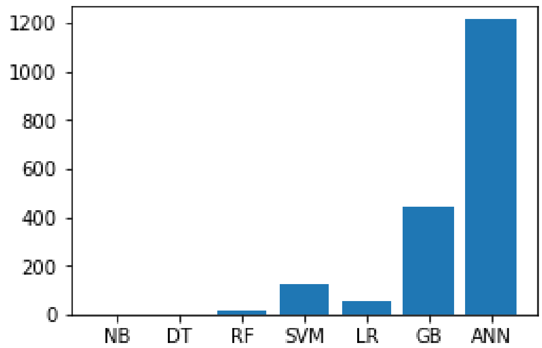

Fig-5: Trainig time of machine learning models for KDD cup 1999 dataset

Fig.5 explains ANN takes more training time as compared to other machine learning models.

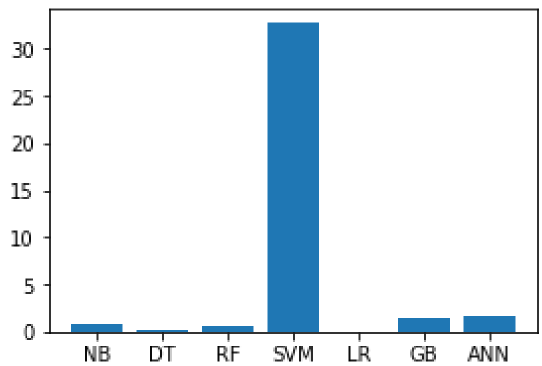

Fig-6: Testing time of machine learning models for KDD cup 1999 dataset

Fig.6 explains SVM takes more testing time as compared to other machine learning models.

V.Conclusion

This proposed model is used to detect cyberattacks. This model was compared with other machine learning models for accuracy. Using a Random forest classifier, the dataset is trained. The model gave an accuracy of 99%. This proposed model performs better than other machine learning models like Gaussian Naïve Bayes, Decision Tree, SVM, Logistic Regression, GB, ANN. Also, training and testing time are compared with different macine learning models. So in the future Random forest classifier will help for the rapid and effective identification of cyberattacks.

ACKNOWLEDGEMENT

I would like to thank Prof. Swapna Augustine Nikale, Department of Information Technology, B.K. Birla College (Autonomous) Kalyan for guiding throughout the research work.

REFERENCES

1. AlDairi, A., & Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. Procedia Computer Science, 109, 1086–1091
2. Varol, N., Aydogan, A. F., & Varol, A. (2017). Cyber attacks targeting Android cell phones. 2017 5th International Symposium on Digital Forensic and Security (ISDFS), 1–5.
3. Nguyen, K. K., Hoang, D. T., Niyato, D., Wang, P., Nguyen, D., & Dutkiewicz, E. (2018b). Cyber attack detection in mobile cloud computing: A deep learning approach. 2018 IEEE Wireless Communications and Networking Conference (WCNC), 1–7.
4. Cavallari, M., Tornieri, F., & de Marco, M. (2018). Innovative Security Techniques to Prevent Attacks on Wireless Payment on Mobile Android OS. Advances in Intelligent Systems and Computing, 421–437.
5. Karthick, S., & Binu, S. (2017). Android security issues and solutions. 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 1–5.
6. Bhatnagar, S., Malik, Y., & Butakov, S. (2018b). Analysing Data Security Requirements of Android Mobile Banking Application. Lecture Notes in Computer Science, 30–37. https://doi.org/10.1007/978-3-030-03712-3_3
7. Froberg, B., & Merkle, L. D. (2018). Ensuring Android Execution Containers with Formal Methods. 2018 Annual Reliability and Maintainability Symposium (RAMS), 1–4. https://doi.org/10.1109/ram.2018.8463090
8. Tawalbeh, L. A., Tawalbeh, H., Song, H., & Jararweh, Y. (2017). Intrusion and attacks over mobile networks and cloud health systems. 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 1–6. https://doi.org/10.1109/infcomw.2017.8116345
9. Park, M., Seo, J., Han, J., Oh, H., & Lee, K. H. (2018). Situational awareness framework for threat intelligence measurement of android malware. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 9(3), 25-38. https://doi.org/10.22667/JOWUA.2018.09.30.025
10. Naik, S., & Maral, V. (2017). Cyber security — IoT. 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 1–4. https://doi.org/10.1109/rteict.2017.8256700
11. Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. Future Generation Computer Systems, 97, 887–909. https://doi.org/10.1016/j.future.2019.03.007
12. Zheng, X., Pan, L., & Yilmaz, E. (2017). Security analysis of modern mission critical android mobile applications. Proceedings of the Australasian Computer Science Week Multiconference on - ACSW '17, 1–10. https://doi.org/10.1145/3014812.3014814
13. Nguyen, K. K., Hoang, D. T., Niyato, D., Wang, P., Nguyen, D., & Dutkiewicz, E. (2018a). Cyberattack detection in mobile cloud computing: A deep learning approach. 2018 IEEE Wireless Communications and Networking Conference (WCNC), 1. https://doi.org/10.1109/wcnc.2018.8376973
14. Chen, Y., Zhang, Y., Maharjan, S., Alam, M., & Wu, T. (2019). Deep Learning for Secure Mobile Edge Computing in Cyber-Physical Transportation Systems. IEEE Network, 33(4), 36–41. https://doi.org/10.1109/mnet.2019.1800458
15. Rivers, O. (2020, July 30). A Study on Cyber Attacks and Vulnerabilities in Mobile Payment Applications | Journal of the Colloquium for Information Systems Security Education. https://Cisse.Info/Journal/Index.Php/Cisse/Article/View/112
16. Tsitsiroudi, N., Sarigiannidis, P., Karapistoli, E., & Economides, A. A. (2016). EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs. 2016 9th IFIP Wireless and Mobile Networking Conference (WMNC), 1–7. https://doi.org/10.1109/wmnc.2016.7543976

17. Choudhary, N., & Jain, A. K. (2017). Comparative Analysis of Mobile Phishing Detection and Prevention Approaches. Information and Communication Technology for Intelligent Systems (ICTIS 2017) - Volume 1, 349–356. https://doi.org/10.1007/978-3-319-63673-3_43
18. Grisham, J., Samtani, S., Patton, M., & Chen, H. (2017). Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 1–7. https://doi.org/10.1109/isi.2017.8004867
19. Joo, J. W., Moon, S. Y., Singh, S., & Park, J. H. (2017). S-Detector: an enhanced security model for detecting Smishing attack for mobile computing. Telecommunication Systems, 66(1), 29–38. https://doi.org/10.1007/s11235-016-0269-9
20. Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber Threat Intelligence: Challenges and Opportunities. Advances in Information Security, 1–6. https://doi.org/10.1007/978-3-319-73951-9_1
21. Aneja, L., & Babbar, S. (2018). Research Trends in Malware Detection on Android Devices. Data Science and Analytics, 629–642. https://doi.org/10.1007/978-981-10-8527-7_53
22. Meng, W., Jiang, L., Choo, K.-K. R., Wang, Y., & Jiang, C. (2019). Towards detection of juice filming charging attacks via supervised CPU usage analysis on smartphones. Computers & Electrical Engineering, 78, 230–241. https://doi.org/10.1016/j.compeleceng.2019.07.008
23. Meng, W., Jiang, L., Wang, Y., Li, J., Zhang, J., & Xiang, Y. (2018). JFCGuard: Detecting juice filming charging attack via processor usage analysis on smartphones. Computers & Security, 76, 252–264. https://doi.org/10.1016/j.cose.2017.11.012
24. Radoglou-Grammatikis, P. I., & Sarigiannidis, P. G. (2017). Flow anomaly-based intrusion detection system for Android mobile devices. 2017 6th International Conference on Modern Circuits and Systems Technologies (MOCAST), 1. https://doi.org/10.1109/mocast.2017.7937625
25. Amro, B. (2017). Malware Detection Techniques for Mobile Devices. SSRN Electronic Journal, 1–10. https://doi.org/10.2139/ssrn.3430317
26. Khilosiya, B., & Makadiya, K. (2020) MALWARE ANALYSIS AND DETECTION USING MEMORY FORENSIC, JULY 2020, Multidisciplinary International Research Journal of Gujarat Technological University ISSN: 2581-8880,1-12
27. Pieterse, H., Olivier, M., & van Heerden, R. (2019). Detecting Manipulated Smartphone Data on Android and iOS Devices. Communications in Computer and Information Science, 89–103. https://doi.org/10.1007/978-3-030-11407-7_7
28. Kulkarni, K., & Javaid, A. Y. (2018). Open source android vulnerability detection tools: A survey. arXiv preprint arXiv:1807.11840.
29. Jamil, Q., & Shah, M. A. (2016). Analysis of machine learning solutions to detect malware in android. 2016 Sixth International Conference on Innovative Computing Technology (INTECH), 1–7. https://doi.org/10.1109/intech.2016.7845073
30. Shivangi, Sharma, G., Johri, A., Akshita, Goel, A., & Gupta, A. (2018). Enhancing RansomwareElite App for Detection of Ransomware in Android Applications. 2018 Eleventh International Conference on Contemporary Computing (IC3), 1–4. https://doi.org/10.1109/ic3.2018.8530614
31. Olorunshola, O. E., & Oluyomi, A. O. (2019). ANDROID APPLICATIONS MALWARE DETECTION: A Comparative Analysis of some Classification Algorithms. 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), 1–6. https://doi.org/10.1109/icecco48375.2019.9043284
32. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
33. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 1–6, https://doi.org/10.1109/cisda.2009.5356528