As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, *9*(SI01): 95-98, 2023

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST09SI0118
Available online at: http://www.ijmtst.com/vol9si01.html

Effective Scanners for Identifying Malware on Android Devices

J.Kannamma, D. Vijaya Kumari, J.Himabala, T.Karuna Latha

Department of Computer Science and Engineering, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada.

To Cite this Article
J.Kannamma, D. Vijaya Kumari, J.Himabala, T.Karuna Latha. Effective Scanners for Identifying Malware on Android Devices. International Journal for Modern Trends in Science and Technology 2023, 9(SI01), pp. 95-98. https://doi.org/10.46501/IJMTST09SI0118

Article Info
Received: 26 January 2023; Accepted: 22 February 2023; Published: 26 February 2023

ABSTRACT

The rapid spread of computer networks has changed people's perceptions of network security. Because computer networks are widely accessible, they are susceptible to a variety of hacking assaults. Network threats are innumerable and can be lamentable. Researchers have developed intrusion detection systems (IDS) that can detect attacks in a variety of situations. Various abuse and abnormal detection strategies have been used.Many of the existing technologies are complementary, as certain approaches perform better in specific settings than others. This survey came up with a new intrusion detection system (IDS). The classification method comprises of two parts: the detection theory of the intrusion detection system "IDS" and the operational components. This is part of our project.

KEYWORDS: RF, ANN.

1.INTRODUCTION

- **Machine Learning:**

In the context of statistics, machine learning is called an application of artificial intelligence where accessible data is processed or algorithmically assisted in the processing of statistical data.

Machine learning relies on automation, but it still requires human monitoring.

Machine learning requires a high degree of generalization to create a system that works well with data samples that have not yet been encountered.

Machine learning is a new discipline of computer science that incorporates a wide range of data processing techniques. Some of these techniques include (for instance logistic regression and principal component analysis) are based on well-established statistical methods, whereas others are not.

Objective of Project:

- To avoid data loss.
- More throughputs.
- To reduce time consumption.
- Continuous energy check up of all data to avoid communication failure.
- To find the intruder at the early stage

Computer Network Security will show you how to detect malware. The basic idea is to reuse system information that has already been created in different phases of the network stack. For the first time, I've encountered such a malware attack. Computer Network Security Detection, a various number of sensors form a wireless sensor network.

[13] The network of nodes is scattered. A wireless sensor network is set up because safety while traveling is a top priority. As a result, advanced malware detection systems have been developed. Malware Detection System Heterogeneous Hybrid Malware Detection System (H-HMDS).

[14] Detection Predictive detection is used at many levels to ensure the highest level of security against malware The major purpose of this project is to assess the power level in order to permit continuous communication of each connection and identifying the network to find malware. The following are the project's key objectives:

1. Detecting early attacks.

2. To abate on packet losses.

3. To enhance throughput

4. To subside on time spent.

5. To avoid node failure, all nodes should be checked for energy on a regular basis.

.2. RELATED WORK

- **Random Forest (RF):**
- Random Forest, also known as Random Decision Forest, is an ensemble learning method for classification, regression, and other tasks in which multiple decision trees are generated during training and the output is either in-class mode regression of individual trees.
- Random forests outperform decision trees in most cases, but they are less accurate than gradient-enhanced trees.
- However, data features can have an impact on how well they work.
- For different machine learning problems, decision trees are a popular strategy.

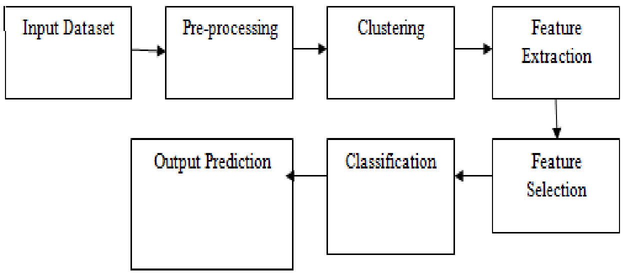
3. PROPOSED WORK

Artificial Neural Network:

- An Artificial Neural Network (ANN) is a type of neural network in which the connections between nodes build a graph over time.
- This means that you can move dynamically over time. ANNs, which are derived from feedforward neural networks, can process sequences of variable length inputs using internal state (memory).
- As a result, activities such as unsegmented, connected handwriting recognition, and speech recognition are possible.
- The term "artificial neural network" applies broadly to two types of networks that are similar in the overall structure. One has a finite momentum and the other has an infinite momentum. Both types of networks have dynamic temporal behavior.
- A directed acyclic graph that cannot be expanded and replaced by a feedforward-only neural network is an iterative infinite moment network.

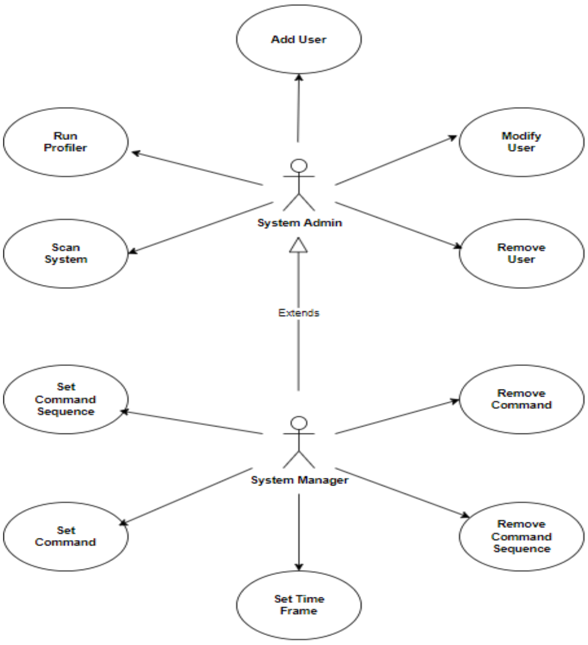
Additional conservative states are possible in both finite and infinite pulse-repeating networks, and conservatives can be controlled directly by neural networks. It can also be used instead of memory if the network or graph contains time delays or if there is a feedback loop. Storage area networks (LSTMs) and gated regression units include such regulated conditions. This is called gate state or gate memory. Another term is feedback neural networks (FNN).

4.SYSTEM ARCHITECTURE

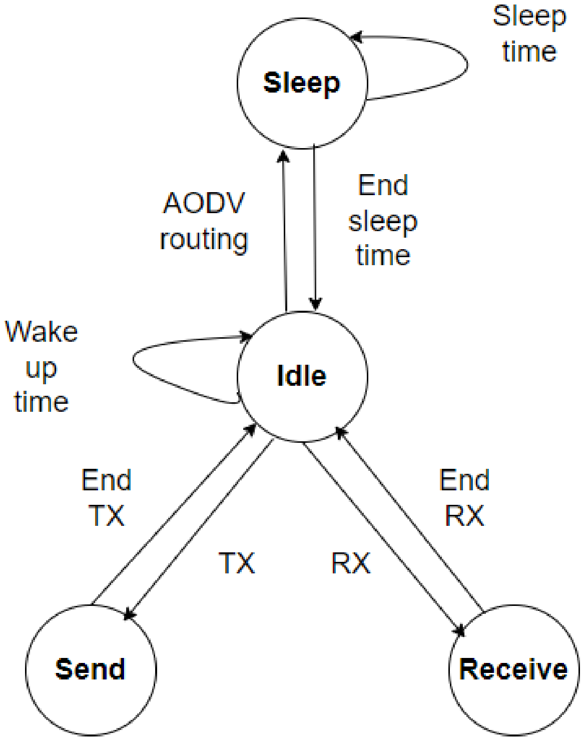


5. UML Diagram:

Use Case:

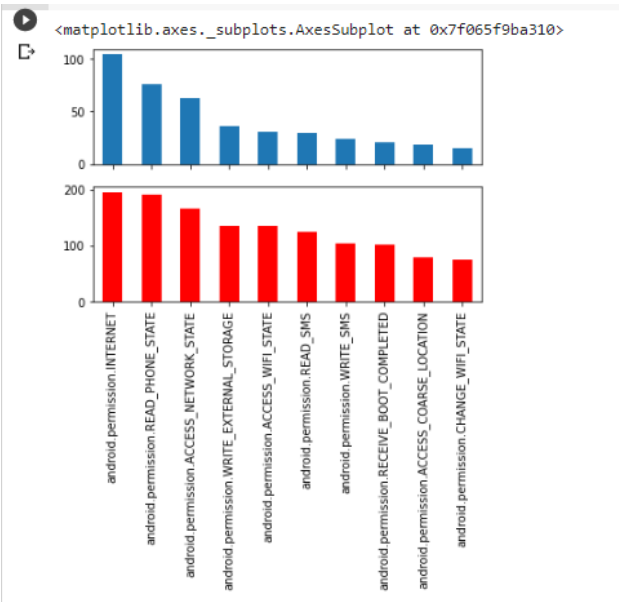


Deployment Diagram:



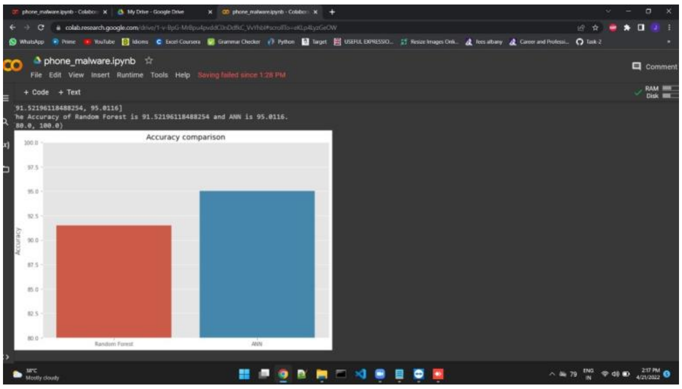
6. RESULT:

Classification of malware data and normal data.



```
<matplotlib.axes._subplots.AxesSubplot at 0x7f065f9ba310>
```

The Accuracy of Random Forest is 91.52196118488254 and ANN is 95.0116.



```
91.52196118488254, 95.0116]
he Accuracy of Random Forest is 91.52196118488254 and ANN is 95.0116.
80.0, 100.0)
```

6. CONCLUSION

Currently, both academia and businesses are interested in detecting malware. He gave an overview of the current state of MDS based on the taxonomy and provided instance of past and present efforts. This taxonomy also emphasizes modern work, while adequately covering past and present discoveries. Each technique has its own set of benefits and drawbacks. We do not believe that there is a single standard that can provide complete protection against computer network malware.There is no single version that can defend against all attackers. Building and maintaining a vulnerable computer system and network is technically demanding and economically difficult given the environment in which the system operates, cost and computational constraints, and the desired level of security

. It takes money.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] I. F. Akyildiz et al., "Wireless Sensor Networks: A Survey, "Elsevier Comp. Networks, vol. 3, no. 2, 2019, pp. 393–422

[2] G.Li, J.He, Y. Fu. "Group-based Malware detection system in wireless sensor networks" Computer Communications, Volume 31, Issue 18 (December 2019)

[3] Michael Brownfield, "Wireless Sensor Network Denial of Sleep Attack", Proceedings of the 2019 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY.

[4] FarooqAnjum, DhanantSubhadrabandhu, SaswatiSarkar *, Rahul Shetty, "On Optimal Placement of Malware Detection Modules in Sensor Networks", Proceedings of the First International Conference on Broadband Networks (BROADNETS19).

[5] Parveen Sadotra et al, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.9, September- 2019, pg. 23-28

[6] K. Akkayaand M. Younis, ―A Survey of Routing Protocols in Wireless Sensor Networks, ‖ in the Elsevier Ad Hoc Network Journal, Vol. 3/3 pp. 325-349, 2019.

[7] A. Abduvaliyev, S. Lee, Y.K Lee, "Energy Efficient Hybrid Malware Detection System for Wireless Sensor Networks", IEEE International Conference on Electronics and Information Engineering, Vol.2, pp. 25-29, August 2019.

[8] Parveen Sadotra and Chandrakant Sharma. A Survey: Intelligent Malware Detection System in Computer Security. International Journal of Computer Applications 151(3):18-22, October 2019.

[9] A. Araujo, J. Blesa, E. Romero, D. Villanueva, "Security in cognitive wireless sensor networks. Challenges and open problems", EURASIP Journal on Wireless Communications and Networking, February 2019.

[10] A. Becher, Z. Benenson, and M. Dorsey, \Tampering with motes: Real-world physical attacks on wireless sensor networks." in SPC (J. A. Clark, R. F. Paige, F. Polack, and P. J.Brooke, eds.), vol. 3934 of Lecture Notes in Computer Science, pp. 104{118, Springer, 2019.

[11] I. Krontiris and T. Dimitriou, \A practical authentication scheme for in-network programming in wireless sensor networks," in ACM Workshop on Real- World Wireless Sensor Networks, 2019.

[12] M. Ali Aydın *, A. HalimZaim, K. GokhanCeylan "A hybrid Malware detection system design for computer network security" Computers and Electrical Engineering 35 (2019) 517–526.

[13] Parvathi, D. S. L., Leelavathi, N., Ravikumar, J. M. S. V., & Sujatha, B. (2020, July). Emotion Analysis Using Deep Learning. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 593-598). IEEE.

[14] Kumar, J. R., Sujatha, B., &Leelavathi, N. (2021, February). Automatic Vehicle Number Plate Recognition System Using Machine Learning. In IOP Conference Series: Materials Science and Engineering (Vol. 1074, No. 1, p. 012012). IOP Publishing."