International Journal of Advanced and Innovative Research (2278-844)/
Volume 7 Issue 8

Energy Consumption Anomaly Based Intrusion Detection In Mobile Using Rule Based Data Mining Approach

[1]Aparna Sen, [2]Dr. Sanjeev Sharma
[1]Research Scholar, [2]Head of Department,
School of Information Technology, RGPV
Bhopal, India
Email: [2]sanjeev@rgtu.net, [1]aparnasen47@yahoo.com

Abstract- **Smartphones are important part of life today, where we use it for personal and professional purpose. Mobile applications make availability of different concepts to make it user friendly environment. Android is a popular platform which is open source and adopted by people. While dealing with a large structured platform to run a mobile application. There are area where the chances of finding anomaly which may harm the user device or its data. Thus a proper analysis of such incoming and outgoing entity is needed. Many technique to detect such is presented like behavior based, signature based detection etc. still a lacking in covering all anomaly properties. Battery is the internal entity which harms devices. In this paper a energy based rule mining EEHAD approach is presented for anomaly malware detection. The experiment performed on multiple android devices with set of application anomaly signature dataset. The output observed result shows the efficient of proposed work.**

Keywords: Smartphones, Intrusion, Anomaly Detection, Android, Rule Mining Technique.

I. INTRODUCTION

Nowadays mobile communications, Smartphone's overture new eligibilities to develop intricate applications, so that to make life is convenient for users [1]. Smartphone devices have been generally used and abundance sensitive information is saved in smartphones to keep their contact data, to browse the internet, to exchange messages, to keep notes, carry their personal files and documents, etc. Modern Smartphone's not only to conversation with each other but also to use a smartphone almost like a personal computer [2].

Mobile has basic resource that is battery life. Limited battery life has got an issue especially in the most recent generation of mobile devices. Once the battery is discharge, the device is abortive until it is recharged. The abundance of functionalities puts pressure on battery lifetime and consequence of Battery energy efficiency. To obtain energy eligibility of Smartphone's, it is crucial to understand where and how the energy or battery is lost [14].

Mobile devices popularity attracts malware authors too and enable users to access browse the Internet to various malware threats such as botnet, adware, viruses, Trojan horse, worms etc. [3]. The disparity of between ''attack'' and ''anomaly'' is that an attack can be defined as ''a sequence of operations that hold the security of a system at risk'' while an anomaly is ''an event that is mistrustful from the standpoint of security''. The main avail of anomaly-based detection techniques is their probable to detect beforehand unseen intrusion events [7]. Mobile transmission emails, documents, files, videos, audio connect to other devices for exchanging information and synchronizing activate various applications, which is attack to target devices. Android is composed having multi-layer security which gives adaptability to this stage. These are factors of android security:

- Design review
- Code Observe and Piercing testing
- Open source and community observe
- Incident response.

Rule based Technique plays most crucial roles in the region of verdict making sciences, knowledge discovery region, supporting business and scientific decision-making. Rule-based classifier makes use of a set of IF-THEN rules for classification. We can demonstration a rule in the following from: IF condition THEN conclusion.

- The THEN section of the rule is called rule consequent.

- The antecedent section the condition exists of one or more attribute tests and these tests are logically ANDed.
- The consequent section exists of class prediction.

We are formation of Energy Efficient Hybrid Anomaly Detection (EEHAD) Approach of mobiles on anomaly based IDS. The goal here is to detect anomalies though battery consumption, i.e. actions that deviate from the normal behavior of the legitimate user, that can be used for Rule Mining based Technique. The anomaly detection approach have to cognize the normal behavior of a user's device in order to be capable to discriminate between normal and abnormal, possibly malicious actions.

II. RELATED WORK

Radoglou et al. [1] presented lightweight IDS which are enhanced with a powerful MLP neural network for detecting anomaly behaviors of the Android mobile devices. The continuously monitors the network traffic of the mobile device and collects various features of the Net Flows. An artificial neural network (ANN) gathers the data flows and determines whether there is an invasion or not. The experimental results indicate that our IDS can detect an anomaly in the Android operating system effectively. Specifically, the accuracy and the detection rate of that system reaches 85% and 81% respectively.

SeyedHasan et al. [11] presented an intrusion detection method for the smart phones using Data Mining techniques followed by its performance using real time user data. Author provides the new method Intrusion Detection Architecture for Mobile Networks (IDAMN). This method proved to be efficient in detecting intrusions. We analyzed the performance of two classifiers Naïve-Bayes and SVM. Both of the classifiers are very effective in detecting intrusions.

Ali Raza et al. [14]used three software tools (SystemSens, Battery Monitor & Power Tutor) perform energy measurements and came up with a model for some commonly used applications like Skype, YouTube, Viber, Tango and Facebook. We can obtain all log data and analyze the aspects of interest in a smartphone. It is possible to study "usage pattern" but allowing many users uploading data to the server, as part of research. We have examined the energy usage by these applications so that developers would focus on for further enhancement of power management.

TurkkaSalmi et al. [15] the main purpose was to find out various methods of using Smartphone's in an energy efficient way. In this, introduces the features of smartphone that can help manage battery consumption and analyses how smartphone user behavior affects the battery consumption. It was found out that even though the majority of the respondents knew how to use Smartphone's energy efficiently, several of the respondents were not necessarily doing so.

Thus the section discuss the work on which we have worked on various sections.

III. PREVIOUS APPROACH

In this section, previous approach and proposed approach result comparison is performed, as per the monitored results from implementation which is obtained is compared. The proposed algorithm EEHAD is presented and compared with existing solution. This chapter gives a comparison graph and statically analysis. As per observed, finally it shows the proposed approach is efficient in terms of total net flows, malicious net flows, accuracy, detection rate as well in the implementation analysis.

IV. PROPOSED METHOD

IDS system provides us the high security rates. An EEHAD approach which is working towards the energy optimization and battery monitoring is utilized in proposed technique. The battery consumption analysis their memory utilization, CPU observation are performed to help in Intrusion application detection monitoring in Android smart phone. The key components of these systems are:

• **Information Source:** Data utilized by the IDS.
• **Analysis Engine:** Process by which the intrusion Detection is made. The overall analysis of battery usage detection.
• **Response:** Action taken when an intrusion is detected.

The principal module is the analysis engine. The analysis engine applies three types of techniques for analyzing and detecting a security threat. These methods are the battery monitoring, energy depletion frequency, the signature based technique, the anomaly detection, and the protocol anomaly detection. In our approach, the second method is adopted, which usually depends on an Energy Efficient Hybrid Anomaly Detection (EEHAD) Approach. The Energy

Efficient Hybrid Anomaly Detection (EEHAD) Approach is used for detecting unknown threats. For this purpose, it is prior trained with the aim of normal and malicious traces. In the context of this paper a Rule Mining Technique (RMT) due to its light-weight operation and its efficiency.

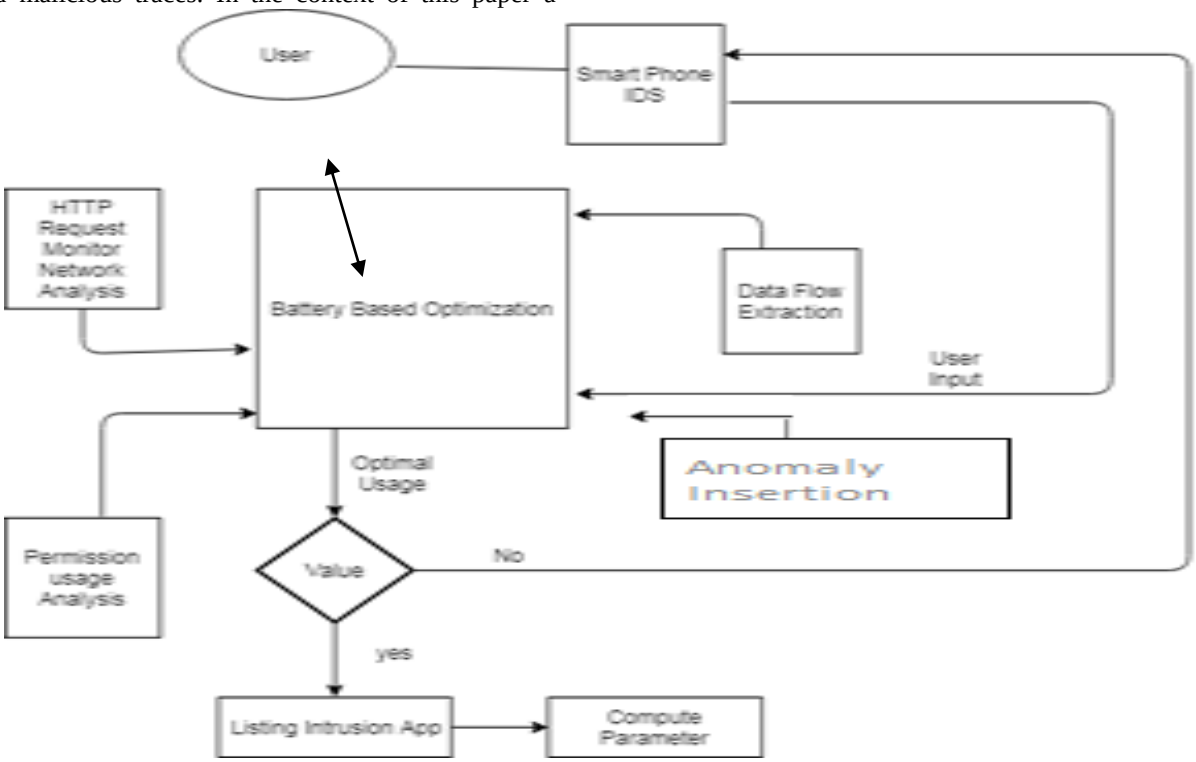

Fig. 1: The Proposed IDS Architecture.

Algorithm Architecture: A battery optimized RMT technique is presented which used the layered based approach along with battery usage monitoring of application. The given proposed below pseudo code algorithm help in understanding the proposed EEHAD Approach algorithm.

Input: Applications, Threshold value, IDS System framework installation

Output: Intrusion app listing, computation parameter, utilization monitoring.

Steps:

Begin [

Loading Configuration framework;

Loading App Info();

int n=numofapp();

foreach(1;n)//

{Finding app usage ();

Finding http request monitor ();

Data flow analysis ();

Permission usage analysis();

Battery usage per unit of time();

foreach app()

{

finding its statistic usage();

stack analysis();

}

computing optimal value()

{

finding app usage();

optimal data use();

battery analysis();

returnEv(Energy value);

}

if(Ev>th Value)

{

add Vector Listing();

}

return Intrusion app listing();

}

return computation parameters();

]

End;

In the given above solution proposed EEHAD is based on battery optimization which help in complete mobile app activity analysis. The EEHAD has given solution help in optimal analysis of application usage which help in intrusion application detection. The given pseudo code help in understanding of the work flow execution.

Experiment Evaluation& Result Analysis

This section presents the experimental results of the proposed IDS on an android platform with the features of Redmi 4 smartphone, CPU octa-core having 6.0.1 version, max 1.40 GHZ with 3 GB RAM. After testing my application it found anomaly apps which cover 7 applications under this. And the virus also detected in 6 applications.

V. RESULT ANALYSIS

The experimental results indicate that our IDS can detect anomalies of the Android system with relative accuracy and detection rate. The experiment results compared with traditional approach find its optional result. Comparison with proposed approach shows the efficiency of proposed work. The computation parameters are discussed here along with the observed result.

1) Accuracy Analysis:

When an intrusion is indicated correctly, then, “True Positive" fact. If no attack has been find out by us a "True Negative". If IDS indicate an intrusion and this assertion is wrong a "False Positive" alarm is triggered. At the end non-intruder is find out and intruder is indeed in progress and "False Negative" (FN) incident. False Negative is the worst case the process of all detection situations causes wrong alarm. Given these terms, we evaluated our IDS using the accuracy value and the detection rate. Accuracy (ACC) is defined in the following equation total no. of outcomes divided by the no. of intruders.

$$ACC = \frac{TP + TN}{TP + FP + FN + TN}$$

2) Detection Rate:

On the other hand, the detection rate (DR) is the possibility that finds out the real intrusions from the given alarm.

$$DR = \frac{TP}{TP + FN}$$

3) Statistical Analysis:

According to the aforementioned definitions, the results of our experiments are summarized in Table 1 the experimental results indicate that our IDS can detect anomalies of the Android system with relative accuracy and detection rate to 77.27% and 89.21% respectively.

Precision = TP/ (TP+FP)

Recall = TP/ (TP+FN)

F-Measure= 2*((Precision*Recall)/(Precision+ Recall))

Parameters	Existing Algorithm	Proposed Algorithm
Computational Time	650ms	543ms
No. of Detection	5	7
Accuracy	68.23%	77.27%
Precision	0.63%	0.75%
Recall	0.47%	0.89%
F-Measure	0.54%	0.81%

Table 1 Result Analysis of Existing Algorithm with Proposed Algorithm

In the table given above shows the difference analysis between the existing technique and proposed EEHAD battery based approach. It helps in understanding the efficiency of proposed technique.

4) Graphical Comparison Analysis.

In this section an analysis of result is presented, the section gives an understanding of statistical graphical analysis.

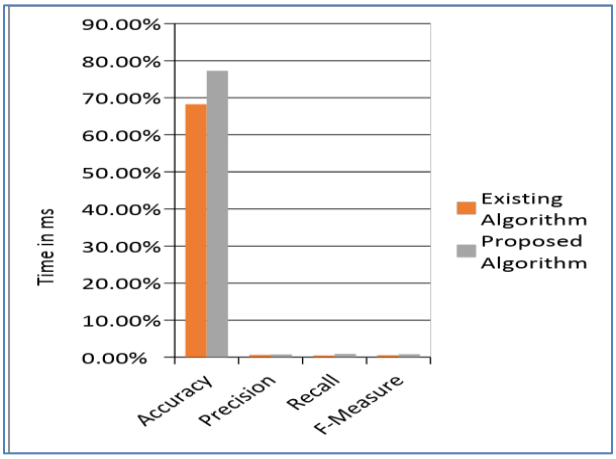

Fig.2Comparison between the existing intrusion application analysis and proposed solution which is battery based.

As presented in the figure 6.1, the energy consumption by various smart phones has been compared by time in milliseconds.

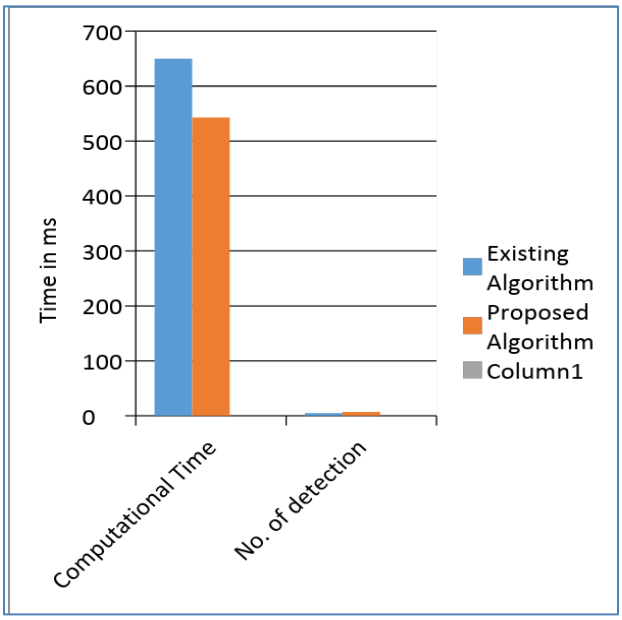

Fig.3 Comparison between the existing intrusion application analysis and proposed solution which is battery based.

As presented in the figure 6.2 the energy consumption by various smart phones has been compared by time in milliseconds.

In this section, previous approach and proposed approach result comparison is performed, as per the monitored results from implementation which is obtained is compared. The proposed EEHAD approach algorithm is presented and compared with existing solution. This section gives a comparison graph and statically analysis. As per observed, finally it shows the proposed approach is efficient in terms of total net flows ,malicious net flows, accuracy, detection rate as well in the implementation analysis.

VI. CONCLUSION

In this era of science we all are using smartphones or say it is a daily essential for everyone whether it is a chatting, mailing, surfing internet, using social networking sites, email services etc. These all features are now available on our smartphones that saves time and money but on one side we have an advantages and facilities provided by smartphones similarly, on the other side it increased the chances for the intruders to write mobile malwares for their sake. The popularity and the advanced functionalities of the modern mobile devices attract the attention of hackers

and cyber criminals. In this paper, we presented Anomaly detecting of malicious behaviors of the Android mobile devices through the battery consumption time based on IDS by EEHAD Approach using Rule Mining Technique. The experimental results indicate that our IDS can detect an anomaly in the Android operating system effectively and enhance EEHAD Approach algorithm which deals with the battery analysis and behavior structure analysis of mobile application in android devices. The experimental results indicate that our IDS can detect an anomaly in the Android operating system effectively. Specifically, the accuracy and the detection rate of the proposed system reaches 77.27% and 89.21% respectively.

REFERENCES

[1] Panagiotis I. Radoglou- Grammatikis, Panagiotis G. Sarigiannidis, "Flow Anomaly Based Intrusion Detection System for Android Mobile Devices", IEEE 2017 6th International Conference on Modern Circuits and Systems Technologies (MOCAST).

[2] Aubrey-Derrick Schmidt, Frank Peters, Florian Lamour, Christian Scheel, Seyit Ahmet amtepe, S¸ahin Albayrak, "Monitoring Smartphones for Anomaly Detection" http://www.springerlink.com DOI:10.1007/s11036-008-0113-x.

[3] BelalAmro, MALWARE DETECTION TECHNIQUES FOR MOBILE DEVICES, International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol.7, No.4/5/6, December 2017.

[4] V. Jyothsna, A Review of Anomaly based Intrusion Detection Systems, International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, September 2011.

[5] V. V. Rama Prasad, A Review of Anomaly based Intrusion Detection Systems, International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, September 2011.

[6] Syed FarhanAlamZaidi, A Survey on Security for Smartphone Device, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.

[7] BelalAmro, MALWARE DETECTION TECHNIQUES FOR MOBILE DEVICES, International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol.7, No.4/5/6, December 2017.

[8] Areej Mustafa Abuzaid, An Efficient Trojan Horse Classification (ETC), IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013

[9] MadihahMohd Saud, An Efficient Trojan Horse Classification (ETC), IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013

[10] P. Ravali, A Comparative Evaluation of OSI and TCP/IP Models, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14.

[11] Seyed Hasan Mortazavi Zarch, Farhad Jalilzadeh, Madihesadat Yazdanivaghef "Data Mining For Intrusion Detection in Mobile Systems" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727Volume 6, Issue 5 (Nov. - Dec. 2012), PP 42-47 www.iosrjournals.org.

[12] Rajinder Singh, An Overview of Android Operating System and Its Security Features, Rajinder Singh Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 2(Version 1), February 2014, pp.519-521.

[14] Ali Raza, "A battery and Network Usage Model for Smartphones", (1st June 2012) Faculty of Engineering and Science University of Agder.

[15] Turkka Salmi, "Energy efficient use of the Smartphone's", (2017) Oulu University of Applied Sciences Degree programme in Business Information Technology.