Scientific Journal of Impact Factor (SJIF): 5.71
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406
International Journal of Advance Engineering and Research Development
Volume 5, Issue 03, March -2018

MALWARE DETECTION USING DATA ANALYTICS APPROACH OVER ANDROID ARCHITECTURE

Kanchana Binjhade[1], Dr. Varsha Sharma[2]

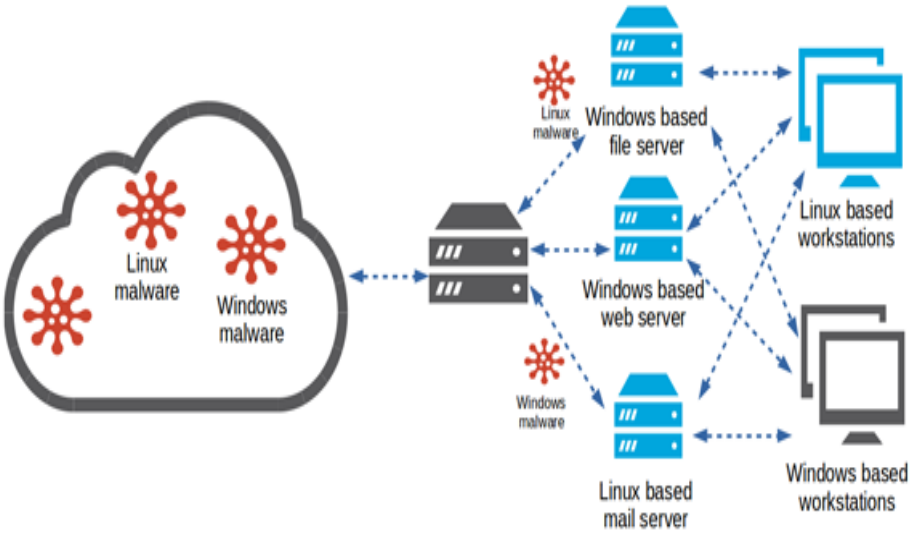
M.Tech. Scholar, School of Information Technology, UTD-RGPV Bhopal[1]
Professor, School of Information Technology, UTD-RGPV Bhopal[2]

Abstract — *Detection and prevention of malware on the mobile platform is a current time requirement. Various anti-malware frameworks were presented to reduce cyber-attack over mobile devices. Malware persist particular features or structure which make changes in software or users data. Therefore, an appropriate approach is needed that can improve the security of mobile devices. In this paper, we conduct a study of various malware detection techniques. In a recent Paper authors have given MADAM (Multi-Level Anomaly Detection for Android Malware) approach for malware detection in Android system and architecture, where they investigated incoming application installation, running application behavior learning. MADAM approach help in proper anomaly detection utilization, also previously given approaches which work either behavior based or pattern based in discussed. This paper overall discuss about the technique overview and scenario associate with them.*

Keywords- *Mobile Computing; Malware; malware detection; Mobile architecture; Android antivirus.*

I. INTRODUCTION

IDS and its security usage algorithms are defined by previous research. It deals with the network intrusion and other mobile anomalies. The machine learning techniques that help detection and prevention alerts are the component that can be used in this segment [18]. Where Android SDK follows the architecture to study the detection of anomalies [17]. Many surveys were conducted to help determine the anomalies of Android mobile devices or other programs. They study their behavior are usage and other Meta information parameters for normal or anomaly behavior [11, 12]. Android mobile malware detection got an important as for a large number of usage and clone application [10].
A classification is required in order to find intrusions detection by the algorithms which help to separate the outliers technique. Therefore, in this investigation, we are working on the classification of the IDS application using a different approach already discussed in the literature. In the previous search, the extraction process is done in large quantity and the variance of data that is extracted from the available static and real-time resources in a different way. Various resources produce positive and intrusion oriented data which may be harmful to the various aspect. Such extraction technique and model need to be investigated and enhance in future research.



"Figure 1.1: A demonstration of the malware and systems"

Mobile data computing simplifies the understanding and processing of data through micro devices such as the mobile unit and other integrated micro device software services and the use of Internet data. Intrusion into large calculated data must be investigated to avoid intrusion data. IDS over the mobile are important over the data capturing and process it accordingly.

Malware is the combination of two words called malware and software, so malware is software that imposes a harmful and damaging effect on software, the operating system or other components. A survey on various malware and malware detection techniques [13] is presented, which provides a description of the various types of attacks and types of malware, such as network-based malware attacks, ordinary malware attacks, etc. In network malware, malware is used as spyware to cause a harmful effect on users' machines, in normal malware such as autorun.inf system.inf, etc. They are used to put the detrimental effect on the user's machine. There are several techniques presented by users to detect malware in the system. As in [8], a hybrid signature call diagram is used to provide malware detection for several types of malware attacks, [11] a semantic malware detection technique that uses file semantics to detect malware is presented. In [9] we present the metamorphic malware detection technique to detect the different types of malware. [10] uses the contents of the file and the relationship of these files to provide malware detection with Mobile Computing, which provides a secure mechanism to transfer data to Mobile. In [12] a flow is presented for the malware detection technique and the security mechanism is presented for [7] that accept multiple agent architecture to provide security for the different types of data. The generation of dynamic code in the mobile and the solution of access to information is necessary to obtain [14, 15].
Further, this paper is organized as follows

Section II presents Literature Review, which describes various malware detection techniques. Section III Conclusion.

II. LITERATURE REVIEW

A review over the various techniques which are used for malware detection in Mobile computing is presented in this section.

Andrea Saracino, Daniele Sgandurra, GianlucaDini and Fabio Martinelli, [7] an algorithm and architecture for detection of anomaly and malware in android mobile have presented. This document presents MADAM, which is a host-based architecture and a malware detection platform. The author follows an approach based on multilevel and behavioral algorithms. Behavior-based pattern detection architecture was used by this technique. This architecture work on detection Rootkit, SMS Trojan, Spyware, Bot net, Ransom ware, installer, Trojan as intrusion entity. A different level of detection such as application installer and kernel level, further the activity running level and other given user activity level finding of malware is presented in this paper. They have done all type of global and activity monitoring in their execution. The presentation of the experiment was performed with android application build and execution. Where the total 2,800 application in different 125 categories is taken for testing. Finally, they have shown the detection of different virus and attack on mobile and show the efficiency and detection rate in their system while comparing to other existing mobile scenario. They have performed rooting and overhead is proper according to their given algorithm. A further working on the system with enhancement of limitation with increasing working with pattern detection and solving the problem of behavior-based detection is left by the author.

GianlucaDini, Fabio Martinelli, Andrea Saracino, and Daniele Sgandurra, [8] MADAM architecture by the authors of [7] is further performed with the pattern based extension and detection over the data. The authors conducted a first run and survey of the architecture and framework of Android. They have ability to manage 10 real-time malware. FPR, detection rate, monitoring activity log in the mobile phone usage is also performed by the author. The classifiers are trained to detect the anomaly of the malware and, therefore, the authors supervise their supervision. The additional extension of the author was given as a detection of behavioral actions and the creation of a behavior database for effective monitoring. The high-level supervision, which activates the alarm for the user on another mobile phone, remains in his future work.

Anshul Arora, Shree Garg, Sateesh K Peddoju, [9 a malware detection technique that uses its traffic analysis capabilities. According to them, a new job presents traffic efficiency and malware monitoring is carried out by them. They analyzed the traffic functionality, they found the difference between the features provided. In addition, the automatic compilation classifier performed the classification of anomalous malware. The category of their bots for malware is AnserverBot, Bgserv, DroidDream, etc., and they lead to the main work area of the anomalous malware as root. An analysis of packet traffic such as TCP and UDP is provided as monitoring, so the author performs a detection of packets and filters. Android emulator, remote server monitoring, command information.

MahmoodDeypir, [10 a technique that is working on matric basis. Permission and its usage model for any have proposed application, malware filtration and execution is performed by the author. A filtering process for suspicion entity and data is derived in this paper. A complete permission based filtration technique is opted by the computer. They have developed the code in MATLAB for their algorithm and proven the efficiency of their algorithm. But still the real-time implementation is not been performed and which is left for the future work. They have worked on the static dataset of permission and application dataset of 122 apps. 71331 number of permission is being used by the system to perform the algorithm.

Gates, C.S., Chen, J., Li, N., and Proctor, R.W. [11] a malware detection technique was presented to detect malware and rootkits. A discussion on risk communication of the Android application, its follow-up on the particular model is

discussed. This also requires the monitoring of system calls and the cancellation of system calls, and an external host monitoring system based on a carrier vector machine is also used. In the call monitoring system, all system calls activated by users are monitored in the parameter before execution. In the system call hash, the entire monitored system called copies is verified before installation. Then a vector-based machine-based system is used that classifies all malware and rootkit attacks in the mobile system view. But that technique suffers from precision, then a new technique to provide accurate results for intrusion detection.

Kelley, P.G., Cranor, L.F., and Sadeh, N. [12] we present a technique based on the carrier vector machine to detect intrusion into the mobile computing architecture. An application of decision making based on the intrusion and detection of its applicability in the mobile ID is presented. They discussed the terminology related to the privacy question and the prevention of user data with the application. In this sense, a monitoring system based on vector support machines at the hypervisor level is used to detect malware in the mobile computing system. In mobile virtualization, you can find several types of threats that require advanced functions to address such mobile malware. Therefore, an improved mechanism is needed to provide an accurate result for this problem. Ruofan Jin, Bing Wang, [13] presents a description of the various malware detection techniques used for intrusion detection. An application based on SDN that works with network software and works for the detection of intrusions in the mobile application. Various machine learning techniques can be used to provide a detection mechanism for mobile computing. In that way, it requires an enhanced technique to pride accurate intrusion detection for such techniques.

Geneiatakis, D., Fovino, I. N., Kounelis, I., & Stirparo, P. [14] a malware detection technique for visualizes Mobile environment is presented. There is various system resilience related risks are occurred in these virtualization techniques. The new technique is required which can deal with the issues related to the risk in the programming. A Verification level approach for user and data package is presented. This paper discussed about the application permission and rule based intrusion approach. A network monitoring entity is presented in the system. In this technique, a network analysis and analysis system (NAE) engine is used to handle such problems. But these techniques are not effective in dealing with such problems; A new technique is needed to provide better malware detection performance.

PallaviKaushik, Amit Jain, [15] A new malware detection software technique is presented, which offers advanced malware detection and advanced forensic functionality and improved implementation capabilities for various programs. But this technique still requires an improvement in malware detection to provide advanced functionality for better intrusion detection. J. Chen, M. H. Alalfi, T. R. Dean and Y. Zou, [16] present a review of various malware detection techniques, which offers a brief description of the techniques of malware detection and malware detection. A detection based on cloning of a specific application of the algorithm is discussed. This document helps you understand how other applications work depending on the current application. The approach based on the intrusion of cloning applications is analyzed in the document. There are several techniques, such as the host-based technique, the detection of malware in the mobile scenario that is displayed; Malware detection for the host user is generally used to provide a malware detection system.

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., &Wetherall, D [17] author worked on a model which is software-defined networking based model performed in Open modelers with Apache Java functionality is performed. An Approach which is working with permission of installation and their validity to work with current scenario is discussed. A test bed setup with i7 system and 8 GB RAM is considered for the implementation. A topology of the different component, their communication setup. Floodlight controller based system for controlling the architecture structure is presented in their proposed work. Suspicious network malware detection with real-time traffic data analysis is performed by them.

Himgouri P. Barge, et. al, [18] A malware detection technique based on ontology for mobile data is presented.
An ontology of mobile application data, an algorithm based on web-based analysis is analyzed in more detail. Malware is the combination of malware and software that indicates malicious software. The definition of the various malware is presented. This uses a K-media cluster technique to classify several malware attacks into different classes. Based on these classes, a malware detection is performed to detect malicious software. On the mobile, the user uses the Internet to access several applications, which can cause any malicious software on the user's computer. Therefore, a malware detection is performed that uses these definitions to detect threats in that application.

"Table 1: Analysis of the available recent algorithms"

Authors	**Algorithm/Technique**	**Tools & Techniques**	**Advantage**	**Disadvantages**	**Remark/ Further extension**
Andrea Saracino, Daniele Sgandurra, GianlucaDini and Fabio Martinelli [7]	MADAM technique for malware detection in Android mobile.	Android SDK, Eclipse.	Work best with multiple level and different type of available entities.	Behavior based is not accurate version of detection. A high level of new anomaly can't be detected.	More accurate system with auto learning new pattern can be invented which means to recognize new anomaly pattern.
Gianluca Dini , Fabio Martinelli , Andrea Saracino , and Daniele Sgandurra [8]	MADAM technique with training phase and database for behavior and other detection module with real-time data access and coverage. Efficiency of classifier is used to detect Malware.	Android SDK, Eclipse Android development tool.	Working with behavior based but real time data access and monitoring log is an advantage work of this system.	Database driven and fixed detection approach.	More complex dataset can be prepared. Data classification cab be more efficient.
Anshul Arora, Shree Garg, Sateesh K Peddoju [9]	Network analysis based approach, monitoring network Logs, UDP and TCP monitoring over the data.	Android Emulator, Android SDK.	Working with network phase detection and monitoring. Working with TCP and UDP network data traffic packet is worked by author.	Data packet monitoring may leads to intrusion. May lead to insecurity over the data packet filtration.	Security over the transmission and protocols can be implemented using encryption system.
MahmoodDeypir [10]	Application installing and frequency based approach is used in this paper. A metric based approach for working with malware usage and permission is used by author. Permission based algorithm with static dataset is given by system.	MATLAB 2013a for the algorithm implementation and simulation is done by the author.	Working with matric based approach makes it efficient and fast. Working with network and facility is detected by the system.	Security is not concerned in network level filtration and detection.	A security over the network can be extending.
Gates, C. S., Chen, J., Li, N., & Proctor, R. W.[11]	Malware detection for the software defined networking is performed by the author in this system. They worked on detection with suspicion network identity and activity.	Open Flow controller	Software defined networking and architecture. Software given dataset and working on given scenario is performed.	No proper real-time scenario is generated by them.	A real-time scenario with extended usage in mobile can be extension of their concept. Learning from the auto setup characteristics if left by the author for further work.
[12]Kelley, P. G., Cranor	An ontology-based malware detection	Ontology based/ Android	Signature and network	Limited detection based on the	Applicable for particular

[13] Ruofan Jin	technique SDN based application	device framework Software networking and working towards intrusion detection	architecture based detection. A description of the various malware detection techniques	available dictionary. It requires an enhanced technique to pride accurate intrusion detection	range of malware detection and prevention. Can be used to provide a detection mechanism for Mobile computing.
[14] Geneiatakis	NAE (Network Analysis engine)	Verification level approach for user and data package is presented.	A malware detection technique for visualizes Mobile environment is presented.	These techniques are not efficient to deal	The application permission and rule based intrusion approach.
[15] PallaviKaushik	Deploy ability for the various software.	A new malware detection software technique is presented	Malware detection to provide an enhanced functionality	This technique still requires an improvement in malware detection	Malware detection to provide an enhanced functionality for the better intrusion detection.
[16] J. Chen, M. H. Alalfi	Host-based technique	A Clone based detection of anomaly relevant algorithm application is discussed	The various malware detection techniques is presented	Still there is a requirement for the modify malware detection techniques	Malware detection for the guest user is generally used to provide a malware detection system.
[17] Kelley, P. G., Consolvo	Apache Java functionality is performed	Open modelers with Apache Java functionality is performed	Floodlight controller based system	Suspicious network malware detection	A topology of the different component, their communication setup.
[18] Himgouri P. Barge	An ontology-based malware detection technique	The malware detection technique is used	The definition of the various malware is presented.	Malware is the combination of malicious and software which means a harmful software.	Still some modifications are required.

III. PROPOSED WORK

As per the previous works and their limitations. A conclusion is drawn that the further extension can be done in the following area.

1. Auto-Learning process of the data and malware features need to be performed which can be done by efficient ANN technique such as KNN technique.
2. A security option can be opted while performing the network based analysis and real-time analysis detection over the algorithm.
3. An auto-learning, enhanced security model can be derived with network usage analysis in the proposed system.

IV. CONCLUSION

In the current scenario, there are several techniques to detect intrusions in mobile computing. Several on-demand services are provided to the user. These techniques require advanced functionality to address these problems. This article presents a brief description of the techniques used to detect malware in Mobile Computing.

REFERENCES

[1]. Fang Z., Han W, and Li Y (2014) "Android security based on permissions: problems and countermeasures, IT and security", 43, 205-218.
[2]. Mylonas A, et. al, "Assess privacy risks in Android: a user-centered approach", 2013.
[3]. S. Poeplau, Fratantonio Y., A. Bianchi, C and G. Vigna Kruegel, "Execute this! The analysis of code dynamics load insecure and malicious applications on the Android" in NDSS'14 of 2014.
[4]. A. S. Sayyad, T. Menzies and H. Ammar, "On the value of user preferences in research-based software engineering: a case study in software product lines", in ICSE, 2013, pp. 492-501.
[5]. Android Developer, "Package Manager [document WWW] .Google.URL, https: //developer.android.com/reference/android/content/pm/PackageManager.html", 2016 [Access 01:06:16].
[6] Omar N., M. Albared, T. Al-Moslmi and A. Al-Shabi, "A comparative study of the algorithms of feature selection and machine learning for the classification of the Arab feeling", in: 10th Asian Information Conference of Recovery Societies, AIRS 2014, Kuching, Malaysia, December 3-5, 2014, pp. 429-443.
[7] Andrea Saracino, Daniele Sgandurra, GianlucaDini and Fabio Martinelli, "MADAM: Detection and prevention of Android malware based on effective and efficient behavior", IEEE 2015.
[8] GianlucaDini, Fabio Martinelli, Andrea Saracino and Daniele Sgandurra, "MADAM: a multi-level anomaly detector for Android malware", Springer 2015.
[9] Anshul Arora, Shree Garg, Sateesh K Peddoju, "Detection of malware by analyzing network traffic on Android-based mobile devices", 4 Eighth International Conference on the next generation of mobile applications, services and technologies IEEE 2014.
[10] MahmoodDeypir, "A new approach for effective malware detection in Android-based devices", XIII ISC International Conference on Information Security and Cryptology (ISCISC2016) from September 7 to 8, 2016; Shahid Beheshti University - Tehran, Iran.
[11]. Gates, C. S., Chen, J., Li, N., and Proctor, R. W. (2014). "Effective risk communication for Android applications: reliable and secure computing", IEEE transactions su, 11 (3), 252-275.
[12] Kelley, P. G., Cranor, L. F., and Sadeh, N, "Privacy as part of the decision-making process of the application, in Proceedings of the SIGCHI conference on human factors in calculation systems" (pp. 3393-3402). ACM, (2013, April).
[13] Ruofan Jin, Bing Wang, "Detection of malware for mobile devices through a software-defined network", 2013 Second research and training workshop on the GENI experiment.
[14] Geneiatakis, D., Fovino, I. N., Kounelis, I., and Stirparo, P. (2015). A permission verification approach for Android mobile applications. Computer and security, 49, 192-205
[15] PallaviKaushik, Amit Jain, "Android Malware Detection Techniques", International Journal of Computer Applications (0975 - 8887) Volume 122 - No.17, July 2015.
[16] J. Chen, M. H. Alalfi, T. R. Dean and Y. Zou, "Android malware detection using cloning detection", J. Compute. Sci. Technol., Vol. 30, no. 5, pp. 942-956, 2015.
[17] Kelley, PG, Consolvo S, Cranor, L. F, Jung J, Sadeh N and Wetherall D, "An enigma of permissions: installation of applications on an Android smartphone in financial cryptography and data security", (pp. 68-79). Springer Berlin Heidelberg, (2012).
[18] Himgouri P. Barge, et. al, "Detection of mobile malware through the analysis of the behavior of the web application network", International Journal of Computer Science and Mobile Computing Vol.3, December 2014.

