ISSN-2350-1413
Subscribers copy
Not for sale

Volume 5. No. 2
July - December 2018

i-manager's

Journal on Mobile Applications & Technologies

Driving the New Wave of Mobile Innovation

i-manager® Publications

ISSN - 2350-1413
Volume 5. No. 2
July - December 2018

i-manager's

Journal on Mobile Applications & Technologies

About the Journal

Mobile application development is the process by which application software is developed for low-power handheld devices which can be pre-installed on phones during manufacturing, downloaded by customers from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an "application-like" experience within a Web browser. i-manager's Journal on Mobile Applications and Technologies focus on how innovative applications and technologies will change our daily lives and how it will redefine businesses across industries.

i-manager's Journal on Mobile Applications & Technologies is presently in its 5th Year. The first issue was launched in 2014.

i-manager's Journal on Mobile Applications & Technologies is published by i-manager Publications, one of India's leading Academic Journal Publisher, publishing 28 Academic Journals in diverse fields of Engineering, Education, Management and Science.

Why Publish with us

i-manager Publications currently publishes academic Journals in Education, Engineering, Scientific and Management streams. All of i-manager's Journals are supported by highly qualified Editorial Board members who help in presenting high quality content issue after issue. We follow stringent Double Blind Peer Review process to maintain the high quality of our Journals. Our Journals target both Indian as well as International researchers and serve as a medium for knowledge transfer between the developed and developing countries. The Journals have a good mix of International and Indian academic contributions, with the peer-review committee set up with International Educators.

Submission Procedure

Researchers and practitioners are invited to submit an abstract of maximum (200 words)/Full paper on or before the stipulated deadline, along with a one page proposal, including Title of the paper, author name, job title, organization/institution and biographical note.

Authors of accepted proposals will be notified about the status of their proposals before the stipulated deadline. All submitted articles in full text are expected to be submitted before the stipulated deadline, along with an acknowledgment stating that it is an original contribution.

Review Procedure

All submissions will undergo an abstract review and a double blind review on the full papers. The abstracts would be reviewed initially and the acceptance and rejection of the abstracts would be notified to the corresponding authors. Once the authors submit the full papers in accordance to the suggestions in the abstract review report, the papers would be forwarded for final review. The final selection of the papers would be based on the report of the review panel members.

Format for Citing Papers

Author surname, initials (s.) (2018). Title of paper. i-manager's Journal on Mobile Applications & Technologies, 5(2), xx-xx.

Copyright

Contact e-mails

editor_jmt@imanagerpublications.com
submissions@imanagerpublications.com

ISSN - 2350-1413
Volume 5. No. 2
July - December 2018

i-manager's

Journal on Mobile Applications & Technologies

Abstracting / Indexing

ISSN - 2350-1413
Volume 5. No. 2
July - December 2018

i-manager's

Journal on Mobile Applications & Technologies

OUR OFFICES

Registered Office

3/343, Hill view,
Town Railway Nager,
Nagercoil, Kanyakumari District - 629001
Ph : 91-4652- 277675
E-mail : info@imanagerpublications.com

Editorial Office

13-B, Popular Building,
Mead Street, College Road,
Nagercoil, Kanyakumari District - 629001
Ph : (91-4652) 231675, 232675, 276675
E-mail : editor_jmt@imanagerpublications.com

Join with us

https://www.facebook.com/imanJMT/

https://www.facebook.com/imanagerPublishing/

https://twitter.com/imanagerpub

CONTENTS

RESEARCH PAPERS

EDITORIAL

Dr. M. V. Subramanyam
Principal,
Santhiram Engineering College,
Andhra Pradesh, India.

I take eminence pleasure and extremely delighted to furnish editorial message for July-December 2018 issue of i-manager's Journal on Mobile Applications and Technology (JMT), a peer reviewed Journal that focuses on how innovative applications and technologies will change our daily lives and how it will redefine businesses across industries. Mobile application development is the process by which application software is developed for low-power handheld devices which can be pre-installed on phones during manufacturing, downloaded by customers from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an "application-like" experience within a Web browser.

In the current issue, the first paper focuses on developing an android app for Premium Motor Spirit in gas stations as the consumers of petroleum products have been experiencing a huge challenge in accessing information about the availability of the product. Next as the need to look attractive and stunning to an event or any social activity is highly demanding in the present trend, the second paper presents a mobile based appointment and scheduling management system for makeup artist. The third paper is on design and implementation of an android Nigerian recipe generating system. Food is an essential requirement for the body for the vitality, development, counteractive action of disease and repair of body cells. Fourth paper focuses on a research that examines the psychological state of mobile phone users while creating passwords. Detecting malicious application on mobile devices is a paramount task as android applications became soft targets for malware hackers. As such, the fifth paper presents the use of whale optimization technique for feature selection of permission-based feature of android applications for better classification accuracy.

I express my sincere thanks to all authors for their outstanding contributions and members of the review committee for their competent evaluation of the submissions for bringing out this Journal in its present form. I strongly assure that this journal will be beneficial to academicians, researchers and industry experts to explore in the field of mobile application and technology.

Dr. M. V. Subramanyam
Editor-in-Chief
i-manager's Journal on Mobile Applications and Technology

ABOUT THE EDITOR-IN-CHIEF

Dr. M. V. Subramanyam is working as Professor in the Department of Electronics and Communication Engineering and Principal of Santhiram Engineering College since 2007. He received Doctoral degree from Jawaharlal Nehru Technological University, Hyderabad, in 2007 for his research contribution to Wireless Adhoc Networks. He has 27 years of teaching experience in Electronics and Communication Engineering. Dr. M. V. Subramanyam has authored six books, more than 161 peer-reviewed National & International Journals and Conference manuscripts. He is a senior member of IEEE and member of IETE, ISTE and IE(I). He completed seven research projects funded by various funding organizations like Institute of Engineers IE(I) and All India Council for Technical Education (AICTE). He received an Indian Patent for his contribution and novel research work entitled "A New Topology and its Management for Ad-hoc Wireless Networks" in the year 2015. He is an Editorial Board Member/ Reviewer of several National/ International reputed journals. He acted as a Chair/ Convener for several International/ National Level Conferences/ Symposiums. His research interests include Wireless Networks, Image Processing and Control Systems.

ANDROID MALWARE CLASSIFICATION USING WHALE OPTIMIZATION ALGORITHM

By

SALAMATU ALIYU SULAIMAN *

OLAWALE SURAJUDEEN ADEBAYO **

ISMAILA IDRIS ***

SULAIMON A. BASHIR ****

* PG Scholar, Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.
** Lecturer, Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.
*** Department of Computer Science, Federal University of Technology, Minna, Nigeria.
**** Lecturer, Department of Computer Science, Federal University of Technology, Minna, Nigeria.

Date Received: 11/01/2019 Date Revised: 11/02/2019 Date Accepted: 08/03/2019

ABSTRACT

The accuracy of any classification algorithm essentially depends on the cohesiveness and structure of the training dataset and its features. The detection of malicious applications running on android devices has become a task that cannot be overemphasized. This is due to the wide acceptability and usefulness of these devices. This usefulness however has also made the Android applications to become soft targets for malware hackers. In order to ameliorate this problem, different malware detection techniques have been proposed in the literature. However, the accuracy and false alarm rate still require improvements in order to have a versatile detector. This research therefore presents the use of Whale Optimization Technique for feature selection of permission-based feature of Android applications for better classification accuracy. The results show that the accuracy is improved using this algorithm compare to some known existing detector models with or without feature selector.

Keywords: Android Malware, Whale Optimization Algorithm, Android Permission Feature, Benign Android Application, Malicious Android Application, Candidate Detectors.

INTRODUCTION

Detecting malicious application on mobile devices is a paramount task that cannot be overemphasized. This is due to the usefulness and wide acceptability of Android applications based devices. This has however made these devices susceptible to system hackers to perpetrate their nefarious and fraudulent activities. These activities range from stealing of vital users' information to financial frauds and destruction of data. The aim of this research is to improve the accuracy of the classification algorithms using whale optimization feature selection. This will invariably improve the technique, so as to improve the coarseness of features and thereby increase the accuracy of detection model. In order to curb the effects of these aforementioned attackers activities, classification techniques have been used through classification algorithms with or without feature selection techniques to build model and enhance the finesse of features, and thereby improve the accuracy of the detector. The quest to improve classification accuracy however remains a daunted task as this determine the accuracy of detection models. This research adopts Whale Optimization Algorithm (WOA) in a way to refine the data and classified the features with three different classification algorithms namely Naïve Bayes, random forest and decision tree classification algorithms. The results of the classification show that random forest algorithm with whale optimization has better accuracy and false alarm rate than other algorithms.

WOA is a whale based technique, which uses their social behaviours to provide optimal solution to science, engineering, network and other categories of problems. This algorithm imitates the hunting instinct of the humpback whale, a category of the biggest earth animal to provide

solution to various optimization problems (Zaied, Ismail, & Mohamed, 2017). The helical curve network system of humpback whales was inherited by this optimization algorithm, which creates a bubbly helical curve network for circumscribe its prey using the best finding strategy or in a random manner to calculate prey's location (Zaied, Ismail, & Mohamed, 2017). Whale is not only the biggest animal but also special and intelligent creature. They has spindle cell in their brain, which is responsible for their social characteristics. The whale hump back gives it a special way of hunting animals and other aquatic preys. Whales also have sleepless attribute as they have to breathe from the surface of water. Therefore, the whale optimization algorithm was derived from the various characteristics of whale to solve barrier optimization problems.

1. Related Work

A research work (Mirjalili, & Lewis, 2016) presents a new meta-heuristic based optimization algorithm inspired by nature. This algorithm is termed Whale Optimization Algorithm (WOA). It imitates the social function of humpback whales. The authors evaluated this algorithm using 29 mathematical optimization problems and 6 structural design problems. The results of this evaluation shows that the WOA algorithm perform excellently compared to other meta-heuristic algorithms as well as traditional techniques. Another research (Rajeshkumar, & Kousalya, 2017) integrated WOA with back propagation neural network in order to the diagnose diabetes mellitus. In the proposed methodology, WOA technique develops new solutions in solution space and back propagation algorithm finds the globally optimal solution. The results show that proposed algorithm outperforms other methodologies.

In (Hu, & Bai, 2017), a concept of inertia weights was introduced into WOA in order to obtain the Improved Whale Optimization Algorithms (IWOAs). The results of IWOAs depict that whale technique with inertia weights perform better than WOA, FOA, ABC, and PSO and are very competitive for predictive tasks compared with others. Another research (Zaied, Ismail, & Mohamed, 2017) applied WOA with artificial neural network to on route finding problem in ad-hoc network. In this case, the ad hoc network require to find the location of moving device which keep changing its position and also needed to find the best path from one device to another for data delivery. Whale optimization in this case was used to find the best path using the best find strategy or in a random manner (Pillai, Nandakumar, Priyadarshini, & Devabalaji, 2017) used WOA to solve the economic dispatch problem. The achieved results using the Whale Algorithm was compared with obtained results using other intelligent methods such as Particle Swarm Optimization (PSO) and found to be better.

Another research (El Aziz, Ewees, & Hassanien, 2017) presented a novel idea for determining the multilevel thresholding values for the segmentation of image. The proposed method optimize the threshold using whale algorithm. The thresholding value was then used to split the image into segments. The experimental results showed that the new technique has better performance in solving multilevel thresholding problem for image segmentation with owner processing time.

The work in (Yogapriya, Saravanabhavan, & Vennila, 2018) proposes an approach for effective image retrieval system for the extraction of feature, feature selection, and classification and similarity measurements. A classification algorithm was used as an evaluation criteria, for identifying the best subset of features. An experiment conducted on medical image dataset and the proposed CBMIR system was evaluated using statistical parameters.

Computer codes that come with malicious intents are referred to as malware (MNCS, MSAN, & Mishra, 2012). Effort to detect, analyze and remove malware is in great demand across computing and device platform. Various methods and algorithms have been worked out by many researchers such as by (Mirjalili, & Lewis, 2016); Siddiqui, 2008; Eder, Rodler, Vymazal, & Zeilinger, 2013; Christodorescu, Jha, Seshia, Song, & Bryant, 2005; Shabtai, Kanonov, Elovici, Glezer, & Weiss, 2011), among others. Some closely related work that apply almost similar approach as in this present research are (Agrawal, & Srikant, 1994; Siddiqui, 2008; Shabtai, Fledel, & Elovici, 2010). Code obfuscation is a common technique uses by malware writers (Bose, Hu, Shin, & Park, 2008). This invariably prevents its detection by different detectors. This

obfuscation technique could be polymorphic or metamorphic in nature. A virus that hides itself completely in a host to evade detection is called metamorphic virus while the one that obfuscates its decryption loops using code insertion and transposition is called polymorphic virus (Christodorescu, Jha, Seshia, Song, & Bryant, 2005). In addition, there are various other techniques adopted by metamorphic malware, which include register renaming, dead code insertion, block reordering and command substitute, modification and inclusion of new behavior so as to increase its strength and viability.

The previous techniques used for analyzing and detecting malicious applications were classified into static analysis, dynamic analysis, and a hybrid technique. Static analysis analyses a program code without actually executing the code (Drake, Lanier, Mulliner, Fora, Ridley, & Wicherski, 2014). This static analysis scans the software for malicious patterns without installing it on the system. On the other hand, dynamic analysis executes the application in a fully isolated domain, i.e. sandbox (Aafer, Du, & Yin, 2013), which intervenes and logs low-level interactions with the program for further analysis using Android emulator which is normally used for ordinary Android applications' testing and debugging.

In the detection of malicious application on a mobile platform, the maiden literatures include (Eder, Rodler, Vymazal, & Zeilinger, 2013; Shabtai, Kanonov, Elovici, Glezer, & Weiss, 2011). Other Android malware detection researches include (Dini, Martinelli, Saracino, & Sgandurra, 2012; Walenstein, Deshotels, & Lakhotia, 2012; Holla, & Katti, 2012; Burguera, Zurutuza, & Nadjm-Tehrani, 2011; Blasing, Batyuk, Schmidt, Camtepe, & Albayrak, 2010; Christodorescu, Jha, Seshia, Song, & Bryant, 2005).

2. Proposed Model Framework

The accuracy of a model directly depend on the finesse and coarseness of the data and features being trained (Adebayo, & AbdulAziz, 2014). The normalization and refinement of data has, therefore, over time, brought improvement to the accuracy of detection model. This proposed model improved the accuracy and false alarm rate of detecting Android malicious application using WOA for feature selection and three different classification algorithms for classification task. The whale optimization is used for feature selection from the set of features in order to remove redundancy. WOA is an algorithm that copies the hunting behavior of the humpback whale which is one of the largest animals on earth. The algorithm imitates the spiral net technique of humpback whales, in which the whale creates a bubbly spiracle net for encircling the pray and then find the prey either by applying the best find strategy or randomly. Classification algorithms used including Naïve Bayes, random forest, and decision tree are among the best algorithms in the classification task for detection modelling.

The model select the best features for the classification modelling task and modeled the features using the aforementioned algorithms. The existing detection algorithms used Particle Swarm Optimization with apriori algorithm (Adebayo, & Aziz, 2015), apriori association analysis for signature extraction (Siddiqui, 2008). These previous techniques, however, where characterized with shortcomings. This research used WOA for the selection of dataset features in order to improve the structure of features by eliminating the redundant features. The whale algorithm in this case select the best features from dataset using the whale humpback search technique. The classification algorithms then apply to the best set of features for classification. This yield best classification model for the detection system. The model can be used to classify Android application into either malicious or benign application depending on the class to which they belong. Figures 2 and 3 show the proposed model framework and data flow model respectively.

2.1 The Original Whale Optimization Algorithm

The most important task in whale optimization algorithm is the best agents' estimation. The structure of whale optimization algorithm includes exploration and exploitation phases. Figure 1 shows the complete algorithm of original whale optimization.

2.1.1 The Prey Encircling

This is an exploration phase, where whale calculate the distance of its prey before encircling it. The humpback whale encircling its prey according to the following equations (1) and (2):

$$\vec{D} = \left| \vec{C}.\vec{X}^{*}(t) - \vec{X}(t) \right| \quad (1)$$

$$X(t+1) = \vec{X}^{*}(t) - \vec{A}.\vec{D} \quad (2)$$

Where t indicates the current iteration of the optimization. A $\vec{A}$ and $\vec{C}$ C are coefficient vectors of the equation.

X* represents the position vector, which should be updated in each iteration to attain better solution attainment. Vectors A and C were calculate using equations (3), and (4).

$$\vec{A} = 2\vec{a}.\vec{r} - \vec{a} \quad (3)$$

$$\vec{C} = 2\vec{r} \quad (4)$$

Where a is a linear vector decrease from 2 to 0 over iterations and vector r in [0, 1]. The (X, Y) position of a search agent was updated in line with the current best record

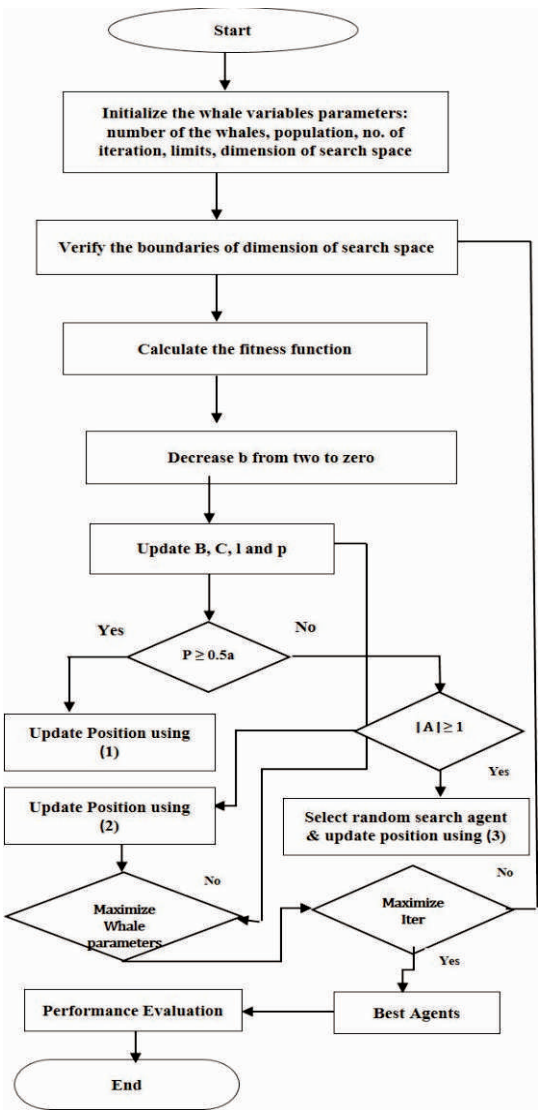

Figure 1. Whale Optimization Flowchart

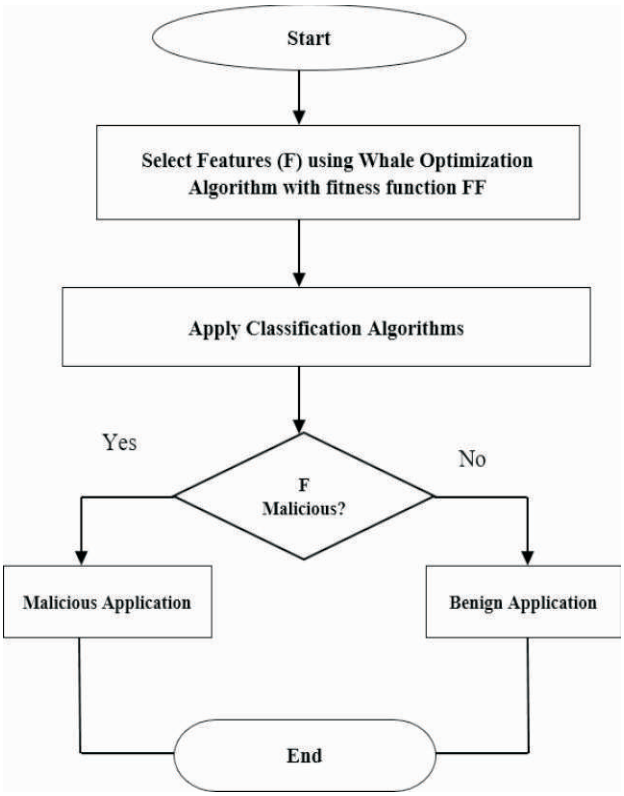

Figure 2. Proposed Model Framework

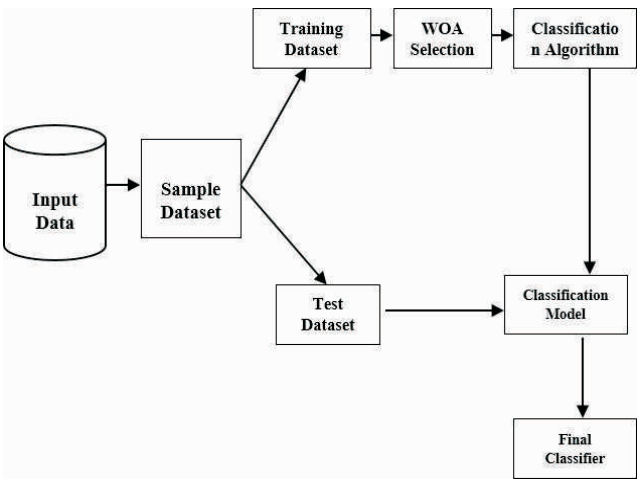

Figure 3. Proposed Android Malware Data Flow Model

(X*, Y*) position. Adjusting the value of $\vec{A}$ and $\vec{C}$ bring about different locations around the best agent. The basic two approaches to whale attacking model are in exploration phase, which are bubble net attacking method (shrinking encircling mechanism and spiral updating position).

The method used in this research is the use of WOA to select the best set of features of Android permission based features for the classification of Android applications into

either malicious or benign. The method is trained.

The best set of features are trained with three different classification algorithms, namely Naïve Bayes, J48 decision tree, and Random forest algorithm. The results show a better performance of models with WOA compared to others.

2.2 Optimization of Classification Algorithm with Whale Optimization Algorithm (CA-WOA)

In order to optimize WOA with classification algorithm, the Android permission based features were selected using WOA and were thereafter trained with classification algorithms for better performance. The WOA used fitness function to determine which feature meet up with the required index fold. Figures 2 and 3 show the proposed model framework and data model respectively.

3. Empirical Study

In order to examine the validity of this research's hypotheses in the previous section, the malicious and benign android applications used were derived from (Contagio, N.D. GooglePlay, 2013) respectively. Supervised learning experiment were carried out to compare the best results. In order to ensure better representation of dataset for supervised learning algorithms using stratified sampling technique, the dataset was divided into training and testing. Whale Optimization Algorithm was used for the selection of best feature set for classification algorithms. Holdout evaluation technique was used for classification training and testing while dataset was divided into 70% training and 30% testing data. The data contains in both training and test set are piece of android permission based features extracted from Android .apk files. In order to train the data, the training data was employed while the test set was used to evaluate the performance of the classification model. Three different classification algorithms were used for supervised learning with the extracted features of Android applications.

3.1 Dataset Analysis

The entire empirical process steps in the research include data gathering, Android application analysis, disassembling, extraction of features, selection of feature, test on the dataset, and classification model building. One thousand five hundred Android applications (.apk) both good and malware files were gathered. The Android executable malicious programs were gathered from (Contagio, N.D) dump while benign applications were from official Android market (Google Play, 2013) represents 66.7% and 33.3% respectively. In order to analyze the dataset statistically, static analysis in (Adebayo, & Aziz, 2014a; Varghese, & Walker, 2011) was used with other tools combination. The needed source code of the program and features were obtained from this initial experiment.

Frequent feature structures are search globally in the entire data collection using the WOA so as to extract the best features from the disassembled parsed files. In order to examine whether there exist relationship or not on the selected features and their final class values was carried out on the entire features by statistical test using p-value. The features found without any significant relationship with the target variable were removed from the dataset. The results of classification using supervised techniques with different classification algorithms and WOA is presented in Table 1.

3.2 Performance Evaluation Criteria

The proposed technique in this research was measured using the estimation parameters depending on the research questions and research hypotheses as defined in this subsection.

3.2.1 Research Questions

The proposed model was evaluated based on the following research questions:

- Can the use of WOA as a selection technique improve the detection rate of malicious applications?
- Does the classification algorithm affect the results of classification models?

3.2.2 Research Hypotheses

- There is no significant different between the results of classification model using WOA selection technique and the one without selection techniques.
- The classification results are not affected by kind of classification algorithms.

3.2.3 Experimental Test using Statistical Parameters

This tests evaluate the performance of classification models in detecting malicious Android application. The

tests include Accuracy (ACC), True positive (measures sensitivity), True negative, False positive (measures specificity), and Root Mean Square Error (RMSE). Equations (5), (6), (7), (8), and (9) show the equations in the respective statistical tests used in the experiments.

3.2.3.1 The Accuracy Measure

The accuracy of a model was defined and measured using the following defined parameters:

- ***TP:*** A malicious Android app that was truly classified as malicious
- ***TN:*** Benign Android app classified as good application
- ***FP:*** malware-free Android app classified as malware.
- ***FN:*** Malicious Android app classified as good apps (malicious-free android application).

Therefore:

$$TPR = \frac{TP}{TP + FN} \quad (5)$$

$$TNR = \frac{TN}{TN + FP} \quad (6)$$

$$FPR = \frac{FP}{FP+TN} \quad (7)$$

$$FNR = \frac{TN}{TN+FN} \quad (8)$$

The accuracy of the model measures the proportion of correctly classified instances (features)

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad (9)$$

3.3 Experimental Settings and Implementation

The foundation of this research experiment was based on the defined research questions and hypotheses in section 3.2. The objective of the experiment is to examine the effectiveness of using WOA as a feature selection technique over other contemporary models. To this end, Android permission features were extracted from executable. These features were selected using WOA and other selection techniques and used to train classification algorithms for learning experiment.

Statistical parameters Accuracy (ACC), False Positive Rate (FPR), True Positive Rate (TPR), and error rate were measured and used to determine the effectiveness of the models. Table 1 and Table 2 show the results of supervised learning experiment for different classification models. The permission structure of numeric data is shown in Figure 4.

4. Experimental Results and Discussion

In order to compare the effectiveness of new classification models using WOA with other existing models, the statistical results of experimented models in terms of accuracy, and detection rate were tabulated. Table 1 shows the average accuracy, detection, and error rates of supervised learning experiment with or without WOA selection techniques while Table 2 presented the average statistics of best model in this research with other existing classification models (AA-PSO, GA, PSO).

The results of experiment shows that random forest has the best results in term of accuracy of 98.21% with the detection rate of 98.50%. The results also show that other algorithms with WOA as selection technique performed better in terms of accuracy and detection rate compare to the ones without WOA. Naïve Bayes classifier also has better accuracy of 94.89% but with high false alarm and error rates.

In comparing models in this research with existing models, random forest with WOA model has the best overall average accuracy of 98.21%, average detection rate of 98.50%, false alarm rate of 0.0158, and 0.0363 Root Mean Square Error. Figure 4 shows the permission structure of binary vector feature used to train classification algorithms. In Figure 4, the binary data 1 represents the presence of a feature in an android application while 0 represents the absent of a particular feature in an application.

Conclusion and Recommendation

This research proposed a classification model for the

Classification Models	TPR	FPR	Accuracy	F-Measure	RMSE
Naïve Bayes	0.9270	0.2771	0.8280	0.8500	0.3748
Naïve Bayes with WOA	0.9489	0.2705	0.8411	0.8598	0.3668
J48	0.8815	0.1053	0.8802	0.9075	0.3233
J48 with WOA	0.8883	0.1332	0.8791	0.9030	0.3210
Random Forest	0.9200	0.1409	0.8960	0.9164	0.2662
Random Forest with WOA	0.9850	0.0158	0.9821	0.9852	0.0363

Table 1. Average Accuracy, Detection, and Error Rates of Classification Models

Models	Avg. Detection Rate (TPR) (%)	Avg. False Alarm Rate (FPR) (%)	Average Accuracy	F-Measure (%)	RMSE
GA	96.34	0.0108	97.71	97.53	0.0764
PSO	96.08	0.0490	95.80	97.03	0.2050
AA-PSO	98.25	0.0192	98.17	98.25	0.0355
Naïve Bayes with WOA	0.9489	0.2705	0.8411	0.8598	0.3668
J48 with WOA	0.8883	0.1332	0.8791	0.9030	0.3210
Random Forest with WOA	98.50	0.0158	98.21	98.52	0.0363

Table 2. Model Performance with other Models in Terms of Error and Accuracy

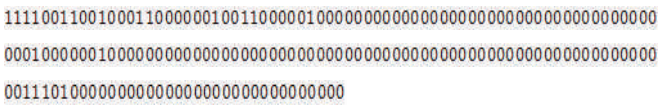

Figure 4. Permission Structure of Binary Feature Vector

detection of Android malicious application using Whale Optimization Algorithm as feature selection technique and features of Mobile Android Application. The research conducted supervised learning experiment using classification algorithms with Android application features. The supervised learners were trained using 70% training data and 30% test data. The classification results measure the accuracy and detection rates of the models. The final results show that new model using WOA has better performance in terms of accuracy, true detection, and error rates than other existing known models.

References

[1]. Aafer, Y., Du, W., & Yin, H. (2013, September). Droidapiminer: Mining API-level features for robust malware detection in android. In *International Conference on Security and Privacy in Communication Systems* (pp. 86-103). Springer, Cham.

[2]. Adebayo, O. S., & Aziz, N. A. (2014a, November). Techniques for analysing Android malware. In *2014 The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M),* (pp. 1-6). IEEE.

[3]. Adebayo, O. S., & Aziz, N. A. (2014 b, December). Android malware classification using static code analysis and Apriori algorithm improved with particle swarm optimization. In *2014 Fourth World Congress on Information and Communication Technologies (WICT),* (pp. 123-128). IEEE.

[4]. Adebayo, O. S., & Aziz, N. A. (2015). Static Code Analysis of permission-based features for android malware classification using apriori algorithm with Particle Swarm Optimization. *Journal of Information Assurance & Security*, 10(4).

[5]. Agrawal, R., & Srikant, R. (1994, September). Fast algorithms for mining association rules. In *Proc. 20th int. Conf. Very Large Data Bases, VLDB* (Vol. 1215, pp. 487-499).

[6]. Blasing, T., Batyuk, L., Schmidt, A. D., Camtepe, S. A., & Albayrak, S. (2010). An android application sandbox system for suspicious software detection. In *2010 5th International Conference on Malicious and Unwanted Software (MALWARE 2010)* (pp. 55-62). IEEE.

[7]. Bose, A., Hu, X., Shin, K. G., & Park, T. (2008, June). Behavioral detection of malware on mobile handsets. In *Proceedings of the 6th international Conference on Mobile Systems, Applications, and Services* (pp. 225-238). ACM.

[8]. Burguera, I., Zurutuza, U., & Nadjm-Tehrani, S. (2011, October). Crowdroid: behavior-based malware detection system for android. In *Proceedings of the 1st ACM Workshop on Security and Privacy In Smartphones and Mobile Devices* (pp. 15-26). ACM.

[9]. Christodorescu, M., Jha, S., Seshia, S. A., Song, D., & Bryant, R. E. (2005, May). Semantics-aware malware detection. In *IEEE Symposium on Security and Privacy,* (pp. 32-46). IEEE.

[11]. Contagio (ND). *Contagio Mobile* [Data Set] Retrieved from http://www.contagiominidump.com

[12]. Dini, G., Martinelli, F., Saracino, A., & Sgandurra, D. (2012). MADAM: a multi-level anomaly detector for android malware. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security* (pp. 240-253).

[13]. Drake, J. J., Lanier, Z., Mulliner, C., Fora, P. O., Ridley, S. A., & Wicherski, G. (2014). *Android hacker's handbook*. USA: John Wiley & Sons.

[14]. Eder, T., Rodler, M., Vymazal, D., & Zeilinger, M. (2013). A framework for analyzing android applications. In *1st international Workshop on Emerging Cyberthreats and*

Countermeasures (ECTCM) (pp. 711-719).

[15]. El Aziz, M. A., Ewees, A. A., & Hassanien, A. E. (2017). Whale Optimization Algorithm and Moth-Flame Optimization for multilevel thresholding image segmentation. *Expert Systems with Applications,* 83, 242-256.

[16]. GooglePlay. (2013). *Google Play Store* [Mobile Apps] Retrieved from https://play.google.com/store

[17]. Holla, S., & Katti, M. M. (2012). Android based mobile application development and its security. *International Journal of Computer Trends and Technology*, 3(3), 486-490.

[18]. Hu, H., & Bai, Y. (2017). Ting Xu Improved whale optimization algorithms based on inertia weights and theirs applications. *International Journal of Circuits, Systems and Signal Processing*, 11, 12-26.

[19]. Mirjalili, S., & Lewis, A. (2016). The whale optimization algorithm. *Advances in Engineering Software*, 95(c), 51-67.

[20]. MNCS, M., MSAN, M., & Mishra, A. (2012). Malware Detection, Supportive Software Agents and Its Classification Schemes. *International Journal of Network Security & Its Applications*, 4(6), 33-49.

[21]. Pillai, A., Nandakumar, S. K., Priyadarshini, & Devabalaji, K. R. (2017). Economic Dispatch Problem using Whale Optimization Algorithm. *International Journal of Pure and Applied Mathematics*, 117(22), 253-257.

[22]. Rajeshkumar, J., & Kousalya, K. (2017). Diabetes Data Classification Using Whale Optimization Algorithm and Back propagation Neural Network. *International Research Journal of Pharmacy*, 8(11), 219-222. Retrieved from www.irjponline.com

[23]. Shabtai, A., Fledel, Y., & Elovici, Y. (2010, December). Automated static code analysis for classifying android applications using machine learning. In *2010 International Conference on Computational Intelligence and Security* (pp. 329-333). IEEE.

[24]. Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., & Weiss, Y. (2011). Andromaly: A Behavioral Malware Detection Framework for Android Devices. *Journal of Intelligent Information Systems,* 38(1) 161-190.

[25]. Siddiqui, M. (2008). *Data mining methods for malware detection* (Doctoral Dissertation, University of Central Florida).

[26]. Varghese, V. J., & Walker, S. (2011). *Dissecting Andro Malware.* Retrieved from https://www.sans.org/reading-room/whitepapers/malicious/dissecting-andro-malware-33754

[27]. Walenstein, A., Deshotels, L., & Lakhotia, A. (2012, June). Program structure-based feature selection for android malware analysis. In *International Conference on Security and Privacy in Mobile Information and Communication Systems* (pp. 51-52). Springer, Berlin, Heidelberg.

[28]. Yogapriya, J., Saravanabhavan, C., & Vennila, I. (2018). Medical Image Retrieval System using Local Binary Patterns, Whale Optimization & Relevance Vector Machine Algorithms. *Taga Journal*, 14, 3164-3191.

[29]. Zaied, A. N., Ismail, M. M., & Mohamed, S. S. (2017). An Optimization Algorithm for Optimal Problem of Permutation Flow Shop Scheduling. *International Journal of Computer Applications,* 173(2), 26-34.

ABOUT THE AUTHORS

Salamatu Aliyu Sulaiman is a student of Mater of Technology of Cyber Security Science, Federal University of Technology, Minna, Nigeria and a staff of Independent National Electoral Commission Nigeria.

Dr. Olawale Surajudeen Adebayo is a Lecturer in the Department of Cyber Security Science, Federal University of Technology Minna, Niger State, Nigeria. He earned his PhD in Computer Science from International Islamic University Malaysia in 2017. He also earned Bachelor of Technology in Mathematics and Computer science from Federal University of Technology, Minna, Nigeria in 2004 and was conferred with his MSc in Computer Science by the University of Ilorin, Kwara State, Nigeria in 2009. His current research themes include malware detection, information security, cryptology, and data mining security. He has published many academic papers in these research themes. He is a member of Computer Professional Registration Council of Nigeria (CPN), Nigeria Computer Society (NCS), IEEE, Global Development Network, and International Association of Engineers (IAENG) among others. He is a reviewer of many local and International Journals.

Dr. Ismaila Idris received a B.Tech. (Hons) in Mathematics Computer Science from the Federal University of Technology, Minna and M.Sc in Information Security from University of Ilorin in 2002 and 2009 respectively. He received a PhD degree from Universiti Teknologi Malaysia in 2014. He has two patent works with Innovation and Commercialization Centre (ICC), Malaysia. He is a member of editorial board Journal of Computer Engineering and Information Technology and International Journal of Artificial Intelligence and Applications (IJAIA). Member board of trustee and National Vice President Cyber Security Experts Association of Nigeria (CSEAN), member Computer Professional Council of Nigeria (CPN), member of International Association of Engineers (IAENG) and also member of Association for Computing Machinery (ACM).

Dr. S. A. Bashir received B.Tech, M.Sc and Ph.D Degrees in Computer Science from Ladoke Akintola University of Technology Ogbomoso, Nigeria, in 2003, University of Ibadan, Nigeria, in 2008 and Robert Gordon University Aberdeen UK in 2017 respectively. He is a lecturer in the Department of Computer Science at the Federal University of Technology, Minna, Nigeria. He is a recipient of the National Information Technology Development Fund PhD Scholarship (2012) and has various publications to his credit. He is a member of the ACM and Nigeria Computer Society. His reearch interests include Application of Machine Learning to Activity Recognition, Deep Learning and Intelligent Systems.

i-manager® Publications

3/343, Hill view, Town Railway Nager, Nagercoil
Kanyakumari Dist. Pin-629 001.
Tel: +91-4652-276675, 277675

e-mail: info@imanagerpublications.com
contact@imanagerpublications.com
www.imanagerpublications.com

i-manager Printing Press