A MOBILE BOTNET DETECTION AND RESPONSE MODEL

Zubaile Bin Abdullah

Thesis submitted in fulfillment for the degree of
DOCTOR OF PHILOSOPHY
SCIENCE AND TECHNOLOGY

UNIVERSITI SAINS ISLAM MALAYSIA

July 2019

AUTHOR DECLARATION

بسم الله الرحمن الرحيم

I hereby declare that the work in this dissertation is my own except for quotations and summaries which have been duly acknowledged.

Date: 16th July 2019

Signature:
Name: Zubaile Bin Abdullah
Matric No: 4120107
Address: No 30, Jalan Kencana 1A/2,
Pura Kencana, Sri Gading,
83300 Batu Pahat
Johor.

BIODATA OF AUTHOR

Zubaile Bin Abdullah (Matric N.4120107) holds **Master** degree in ***Information Security*** from **R**oyal, **H**olloway, **U**niversity of **L**ondon (**RHUL**) and a **Bachelor** degree in ***Information Technology*** from **Uni**versity **T**eknologi **M**ARA (**UiTM)**.

He is currently a Ph.D. Candidate in Science and Technology at **Universiti Sains Islam Malaysia (USIM)**. **Zubaile** has almost **14 years' experience** in Information System and Cyber Security. Previously he worked as Academician in the Department of Information Security at Universiti Tun Hussein Onn Malaysian.

JOURNAL ARTICLE

Z. Abdullah, M. M. Saudi, and N. B. Anuar, "ABC: Android Botnet Classification Using Feature Selection and Classification Algorithms" Adv. Sci. Lett., vol. 23, no. 5, 2017. (Scopus Indexed Journal).

Z. Abdullah and M.M. Saudi, "RAPID - Risk Assessment of Android Permission and Application Programming Interface (API) Call for Android Botnet". International Journal of Engineering & Technology (IJET), vol. 7, no. 4.15, 2018. (Scopus Indexed Journal).

PROCEEDINGS

Z. Abdullah, M.M. Saudi, N.B. Anuar, "Mobile botnet detection: proof of concept", IEEE 5th Control and System Graduate Research Colloquium (ICSGRC), 2014, pp. 257–262, Aug (2014). (Scopus Indexed Proceeding)

Z. Abdullah and M.M. Saudi, "RAPID - Risk Assessment of Android Permission and Application Programming Interface (API) Call for Android Botnet", 1st International Conference on Recent Advancements in Science and Technology (ICoRAST2017).

ACKNOWLEDGEMENTS

I am deeply grateful to **ALLAH (S.W.T),** for giving me good health to successfully complete my PhD research, including completion of this thesis. Peace be upon **The Prophet Muhammad.**

I would also like to express my deep appreciation **to Ministry of Education** for funding my studies under **SLAB** programme and **Universiti Tun Hussein Onn** for approving and supporting my study leave.

I would also like to express my deep appreciation to **UNIVERSITI SAINS ISLAM MALAYSIA (USIM)** and especially to the **Fakulti Sains & Teknologi (FST)** for not only giving me the opportunity to pursue my PhD degree in this peaceful campus but also providing me with the facilities and resources I needed to successfully complete my PhD degree.

My very special appreciation and thanks should go to my principal supervisor **Associate Professor Dr. Madihah Mohd Saudi**, for her invaluable support, guidance, patience and care. **Associate Professor Dr. Madihah Mohd Saudi** has always been a source of hope, encouragement and willpower for me to do my very best. She tremendously assisted me throughout the dissertation journey.

I would also like to thank my co-supervisor, **Associate Professor Dr Nor Badrul Anuar Juma'at**, for the guidance, encouragement and advice he has provided especially in article and thesis writing throughout my time as his student. **Associate Professor Dr Nor Badrul Anuar Juma'at** is a prolific writer in information security field.

I am extremely grateful to my **parent** and **siblings**, who have given my unending support throughout my education journey and in my entire life. Their care, support, encouragement, and best Dua'a have made my study, including this thesis, a success. May **ALLAH (S.W.T)** grant my parents health and blessings always.

My deepest thanks go to my **lovely wife, Juliyana Binti Selamat**, together with my 5 jewels, **Sabrina Sasha Izzati**, **Irfan Izzat Khilfi**, **Elena Ezrin Izzati**, **Irfan Syahmi Iskandar** and **Irfan Zahrin Nazriel**, for providing me with unfailing support and continuous encouragement throughout my years of studies and through the process of researching and writing this thesis. My family have always been there for me and have always seized every opportunity to cheer me up all the time

Special thanks also go to **Allahyarham Selamat & Allahyarhamah Manisah**'s family for valuable support during my tenure of studies.

I would like to thank all the **research colleagues**, **FSKTM, UTHM Staff** and **friends** for their time and help they gave throughout my research. Their contribution to this research has been central and I will forever be sincerely grateful to them.

A MOBILE BOTNET DETECTION AND RESPONSE MODEL

ABSTRACT

Mobile botnet exploitation in smartphone could implicate to the leakage of sensitive and private information, loss of financial and degradation of smartphone's performance thus affecting organisations or users that rely on smartphones for business and personal activities. Detecting mobile botnet is a challenge for the existing antimalware software which depends on signature-based detection. Nonetheless, existing works on mobile botnet that are mostly focused on the development of detection model have issues on feature selection, detection accuracy rate and its detection model. In addition the existing works also lack on the mobile botnet threat response. Hence, based on the mobile botnet implication and existing gaps in the extant research, the objectives of this research are to construct a new mobile botnet classification using features based on mobile botnet architecture and feature's risk impact, to develop a mobile botnet detection and response model based on the mobile botnet classification, risk level and by applying apoptosis concept and to evaluate the proposed mobile botnet detection and response model based on accuracy rate. The new mobile botnet classification is used for mobile botnet detection whereas, for the response model, apoptosis is triggered to respond to mobile botnet detection and on risk level of mobile application. The experiment was conducted in a controlled lab environment, using static and dynamic analyses and by applying knowledge discovery procedure (KDD). 1500 mobile botnet samples from University of New Brunswick (UNB) dataset and 1000 benign samples from Google Play Store are used for training whereas 600 mobile botnet samples from Drebin dataset and another 400 benign samples from Google Play Store are used for testing. From the experiment, the proposed model has produced 98.8% detection accuracy rate and 2% false alarm rate. This result outperformed the existing work of ABIS by 6% and 5% improvement in true positive rate and detection accuracy rate respectively. Furthermore, the proposed model is also able to countermeasure the mobile botnet threat using apoptosis mechanism that triggered by application's risk level. Based on the evaluation, the result indicated significant improvement compared to other research findings, thus, fulfilling the abovementioned research gaps. As a conclusion, this research has produced a new model, which can detect and respond to mobile botnet threat effectively. For future work, this research can be used as a reference for the other researchers with the same interest.

Keywords: Mobile Botnet, Classification, Detection, Response, Apoptosis, Risk Level

ABSTRAK

Exploitasi botnet mudah alih dalam telefon pintar menyebabkan kebocoran maklumat sensitif dan peribadi, kehilangan kewangan dan kemerosotan sistem telefon pintar dan memberi kesan kepada organisasi atau pengguna yang bergantung pada telefon pintar untuk urusan perniagaan dan peribadi. Pengesanan botnet mudah alih merupakan satu cabaran untuk perisian antimalware sedia ada yang bergantung kepada pengesanan berasaskan 'signature'. Tambahan pula penyelidikan sedia ada terhadap botnet mudah alih yang kebanyakannya tertumpu kepada pembangunan model pengesanan dan mempunyai isu-isu terhadap pemilihan ciri, kadar ketepatan pengesanan dan model pengesanannya. Di samping itu, penyelidikan sedia ada juga tidak mempunyai tindakbalas terhadap ancaman botnet mudah alih. Oleh itu, berdasarkan implikasi botnet mudah alih dan jurang dalam penyelidikan yang sedia ada, objektif kajian ini adalah: (i) untuk membina klasifikasi botnet mudah alih baru menggunakan ciri-ciri berdasarkan senibina botnet mudah alih dan kesan risiko ciri, (ii) untuk membangunkan pengesan botnet mudah alih dan model tindak balas berdasarkan klasifikasi botnet mudah alih, tahap risiko dan dengan menggunakan konsep apoptosis dan (iii) untuk menilai model pengesanan dan tindak balas botnet mudah alih yang dicadangkan berdasarkan kadar ketepatan. Klasifikasi botnet mudah alih yang baharu digunakan untuk pengesanan botnet mudah alih manakala untuk model respons, apoptosis dipicu untuk bertindak balas terhadap pengesanan botnet mudah alih dan pada tahap risiko aplikasi mudah alih. Eksperimen ini dijalankan di persekitaran makmal terkawal, menggunakan analisis statik dan dinamik dan dengan menggunakan prosedur penemuan pengetahuan (KDD). 1500 sampel botnet mudah alih dari dataset University of New Brunswick (UNB) dan 1000 sampel aplikasi dari Google Play Store digunakan untuk latihan manakala 600 sampel botnet mudah alih dari dataset Drebin dan 400 sampel aplikasi dari Google Play Store digunakan untuk pengujian. Berdasarkan ekperimen yang dijalankan, model yang dicadangkan telah menghasilkan 98.8% kadar ketepatan pengesanan dan 2% kadar penggera palsu. Keputusan ini mengatasi prestasi kerja ABIS sebanyak 6% dan peningkatan 5% dalam kadar positif sebenar dan kadar ketepatan pengesanan. Selain itu, model yang dicadangkan juga dapat memberi respons terhadap ancaman botnet mudah alih, yang dicetuskan oleh tahap risiko dan bertindak balas melalui mekanisme apoptosis. Berdasarkan penilaian, kajian yang dilakukan ini menunjukkan peningkatan yang ketara berbanding dengan penemuan penyelidikan lain, dan memenuhi jurang penyelidikan yang dinyatakan di atas. Sebagai kesimpulan, kajian ini telah menghasilkan model baharu, yang dapat mengesan dan bertindak balas terhadap ancaman botnet mudah alih dengan berkesan. Untuk kerja masa depan, penyelidikan ini boleh digunakan sebagai rujukan kepada penyelidik lain dalam minat yang sama.

Kata Kunci: Botnet, Klasifikasi, Pengesanan, Tindakbalas, Apoptosis, Tahap Risiko

الملخص

ان تسخير شبكة الروبوت (بوتنت) المتنقلة في الهواتف الذكية له تأثير على تسرب المعلومات الحساسة والخاصة, وفقدان وإنحطاط أداء الهواتف الذكية وبالتالي يؤثر على أداء المؤسسات أوالمستخدمين للأجهزة الذكية في الأنشطة التجارية والأنشطة الشخصية. أكتشاف شبكة البوتنت المتنقلة يعتبر تحدي بالنسبة لبرامج الحماية التي تستخدم طريقة قاعدة التوقيع للكشف عنها. ومع ذالك, فإن الأبحاث الحالية على البوتنت المتنقل والتي في الغالب تركز على تطوير نموذج إكتشاف تعتمد على مبادء الإكتشاف المستقبلي وإكتشاف معدل الدقة. بالإضافة إلى ذلك, الأبحاث الحالية أيضا ينقصها دراسة ردة الفعل عند حدوث خطر من شبكة البوتنت المتنقلة. بالتالي, بناءا على تأثيرات شبكة البوتنت المتنقلة والفجوة في البحوث الحالية, هذا البحث سيدرس الأهداف التالية. إنشاء تصنيف جديد لشبكات البوتنت المتنقلة بإستخدام قاعدة المستقبل على بناء شبكة البوتنت المتنقلة وخاصية تأثير المخاطر. تطوير نموذج يشمل إكتشاف وردة الفعل لشبكة البوتنت المتنقلة بناءا على تصنيف شبكة البوتنت, مستوى الخطر, وايضا استخدام مفهوم أبوبتوسيس. وأخيرا تقييم النموذج المقترح بمقارنته بنموذج معدل الدقة. التصنيف المقترح لشبكة البوتنت المتنقلة تم إستخدامه لإكتشاف البوتنت المتنقلة, في حين لنموذج ردة الفعل تم استخدام أبوبتوسيس لشن ردة الفعل على شبكة البوتنت المتنقلة المكتشفه وعلى مستوى الخطر للتطبيق. التجربة العملية أجريت في بيئة مختبر بإستخدام نماذج تحليل ثابتة ومتغيرة و ايضا بتطبيق إجراء كشف المعرفة. لإجراء التجربة تم استخدام 1500 عينة من شبكة البوتنت المتنقلة من جامعة نيو برونسك و 1000 عينة من جوجل بلاي ستور استخدمت للتدريب وايضا 600 عينة من دربين و 400 عينة من جوجل بلاي ستور استخدمت للفحص.من التجربة، أنتج النموذج المقترح 98.8٪ معدل دقة الكشف و 2٪ معدل إنذار كاذب. تفوقت هذه النتيجة على عمل الحالي بنسبة 6 ٪ و 5 ٪ أفضلية على طريقة المعدل إالإيجابي وكذلك طريقة دقة المعدل. علاوة على ذلك, النموذج المقترح قادر على قياس خطر شبكة البوتنت المتنقلة باستخدام آلية أبوبتوسيس التي تشن بإستخدام برنامج مستوى المخاطر. بناءً على التقييم ، أشارت النتيجة إلى تحسن كبير مقارنةً بنتائج البحوث الأخرى ، وبالتالي ، سد ثغرات البحث المذكورة أعلاه.كإستنتاج ، أنتج هذا البحث نموذجًا جديدًا ، يمكنه اكتشاف تهديد شبكة البوتنت المتنقلة بشكل فعال. بالنسبة للعمل في المستقبل ، يمكن استخدام هذا البحث كمرجع للباحثين الآخرين بنفس الاهتمام.

الكلمات المفتاحية: شبكة البوتنت المتنقل، التصنيف، الكشف، ردة الفعل، أبوبتوسيس، مستوى الخطر.

CONTENT PAGE

Contents **Page**

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF APPENDICES

Page

ABBREVIATION

ABDA	Android Botnet Detection and Response Application
API	Application Programming Interface
C&C	Command and Control
DDoS	Distributed Denial of Service
DVM	Dalvik Virtual Machine
FAR	False Alarm Rate
FNR	False Negative Rate
FPR	False Positive Rate
GPS	Global Positioning System
HIS	Human Immune System
IDS	Intrusion Detection System
KDD	Knowledge Discovery in Databases
NIST	National Institute of Standards and Technology
PAMPs	Pathogen Associated Molecular Patterns
PRRs	Pattern Recognition Receptors
SMS	Short Message System
TNR	True Negative Rate
TPR	True Positive Rate
UID	Unique User Identification
UNB	University of New Brunswick

CHAPTER 1: INTRODUCTION

This chapter highlights the background of the research, current research problems, motivation, research questions, research objectives, scope, contributions, thesis structure and summary of this chapter.

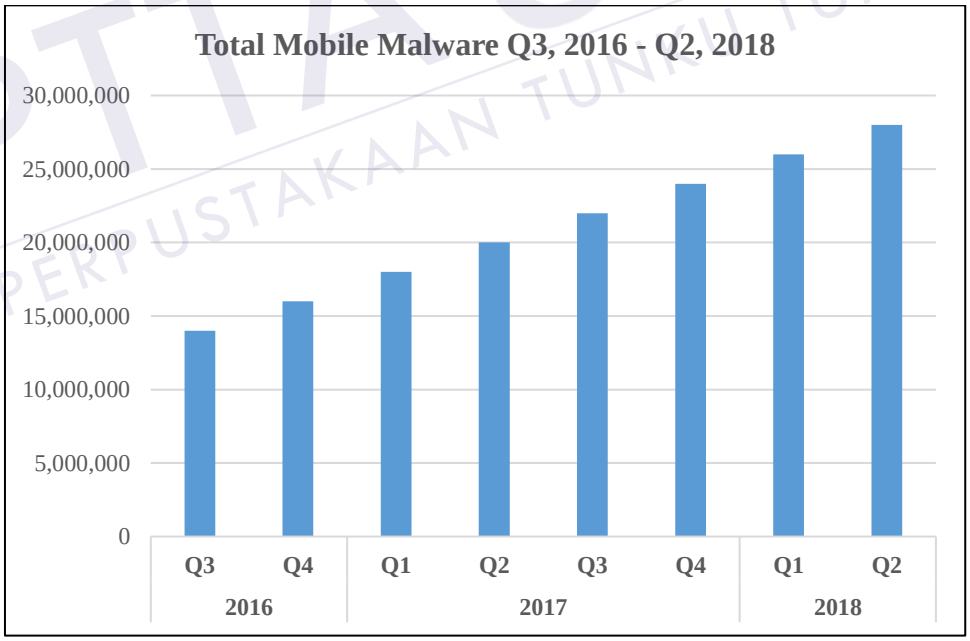
1.1 Background

The number of smartphone users has risen significantly across the globe, due to its multi-functionality capabilities (Li & Clark, 2013; Tong & Yan, 2017; Shezan et al., 2017). Apart from the usual functions of a mobile phone such as making calls or sending text messages, the smartphones also are being used for web browsing, social networking, gaming, business operation and online banking transaction. Smartphone users are also keep confidential information such as bank account number, username and password for online banking, credit card number and private memorabilia in their smartphone. Due to these circumstances, smartphones are recently targeted by the attackers with different way of exploitation such as masquerading as legitimate mobile application (app) and but had embed malwares in it.

Recent report by McAfee Labs, (2018), indicated that mobile malware attacks on smartphone have exponentially growth as presented in Figure 1.1. The attacks came

from different type of malwares such as trojan, ransomware, spyware, virus and mobile botnet (Eslahi et al., 2012; Mylonas et al., 2013; Anwar et al., 2016). Among of these malware, mobile botnet is the most dangerous as it poses serious threat to the smartphone users and the smartphone's system (Zhou & Jiang, 2012; Feizollah et al., 2015; Anwar et al., 2016; Tansettanakorn et al., 2016). A main difference between mobile botnet and other mobile malware is the utilization of Command and Control (C&C) infrastructure. The C&C allows mobile botnet to receive commands from botmaster; an attacker who operates and controls the mobile botnet remotely. Once a smartphone is installed and infected with mobile botnet application, the attacker will have superior access and control over the compromised smartphone.

Figure 1.1: Total Mobile Malware from Q3, 2016 to Q2, 2018 (McAfee Labs, 2018)



For this research, mobile botnet is defined as a malicious application that infected smartphone without user consent or knowledge. Once infected by mobile botnet, the smartphone can be controlled by an attacker called a botmaster via exploitation of

application features that are permission, API call and system call. The botmaster will then be able to manipulate the compromised smartphones to commit cyber-crimes or -attacks, which includes spam messages, premium text messaging services subscription, identity theft scams, degrade smartphone and phishing scams which implying to invasion of privacy (Wang et al., 2016; Chen et al., 2017), financial loss (Etaher et al., 2015; Shezan et al., 2017) and degradation of smartphone system performance (Hsieh et al., 2015; Rodriguez-Mota et al., 2016). These implications could lead to a breach of confidentiality, integrity and availability which are critical principles in information security. Table 1.1 presents the implication, malicious activity, threat and security breach of the mobile botnet on a smartphone.

Table 1.1: Implication, Malicious Activity, Threat and Security Breach of Mobile Botnet Attack on Smartphone.

Implication	Malicious Activity	Threat	Security Breach
Privacy	Expose user location Read phone detail & specification Read contact list Read message	Privacy exposed Leakage of sensitive information	Confidentiality
Financial	Subscribing to premium number Pay-per-phone service Sending unauthorized message via Short Message System (SMS)	Loss of financial Overbilling	Integrity
System	Battery Drainage Wi-Fi Scanning GPS Excessive Scanning Abusive Advertising	Smartphone system malfunction Smartphone system slowdown	Availability

These critical security implications possess by mobile botnet have promoted a strong research interest among security researchers in developing mobile botnet detection models that are able to detect mobile botnet in smartphone. However, most of the models have certain shortcomings, which includes model complexity to be implemented into smartphones and low detection accuracy rate. This research, on the other hand, looked into developing detection model with better detection accuracy rate to rectify the abovementioned shortcomings. Furthermore, the existing mobile botnet detection models also lack the response mechanism to mobile botnet threat once it has been detected. Therefore, an apoptosis concept was also applied in this research as a solution to the response mechanism.

Apoptosis is one of the specialisms in Human Immune System (HIS) and is known as cell- programmed death (Sridevi & Jagajothi, 2014). For this research, the concept of apoptosis which is the ability of human body to eliminate intruder's threat such as virus in human body is being adapted and applied for mobile botnet detection and response model. . However, there are two challenges which need to be addressed. Firstly, how to differentiate between benign and mobile botnet for detection and response? Secondly, how to trigger detection and response mechanism against mobile botnet? This research had successfully solved this challenges by constructing new mobile botnet classification for mobile botnet detection and assessment of risk level based on security metrics to trigger the apoptosis response mechanism. Indeed, mobile botnet detection and apoptosis response algorithms have been developed to solve the challenges.

The discussed issues above and challenges have been the main motivation of this research with the aim to improve mobile botnet detection accuracy rate and response by proposing a new mobile botnet detection in smartphone with applicable response model.

1.2 Problem Statement

Numerous methods have been proposed to counteract a mobile botnet threat due to their devastating consequences on smartphone users and smartphone system. One of the methods is signature-based detection in which implemented by most antimalware vendors (Feizollah et al., 2015; Sharma & Sahay, 2016; Sun, 2016). Signature-based detection is a method where a unique identifier for a known mobile botnet is established so that the botnet can be identified in the future. The signature can be a unique pattern of code that attached to smartphone application or can be the hash algorithms of a known bad application. If that specific pattern or signature is discovered in mobile application, the application can be flagged as being malicious. However, the drawback of this method is, the signature needs to be updated regularly. Falling to update the signature will expose smartphone users from new or unknown mobile botnet attacks. Unfortunately, it has been proven that the speed at which mobile botnets are created is substantially greater than the rate at which signature updates can be carried out (Chang & Wang, 2016). Furthermore, the mobile botnet signature is unique for a single mobile botnet, thus, simple modification in a mobile botnet code leads to a new variant and could bypass the signature-based detection.

On the hand, other existing works, have integrated machine learning with mobile botnet detection method. This method is capable of detecting anomalies with few challenges for implementation. The first challenge is related to smartphone resource constraint, while the second challenge is on feature selection. According to Mostafa et al., (2015); Sun et al., (2017) and Ali et al., (2017), the use of machine learning algorithm in mobile botnet detection models is ineffective as smartphone has limited computational power, storage and battery life. In addition, Khune & Thangakumar, (2012) and J. Milosevic et al., (2017) have indicated that the machine learning algorithms integrated detection models are highly complex and resource consuming when executed on smartphone. As a result, they could not be deployed on smartphone. Hence, these existing models are only executable in smartphone-simulation environment or computer server for the mobile botnet detection. Therefore, a solution for mobile botnet detection is required for implementation in a smartphone.

Basically, feature is an attribute extracted from mobile application and used in machine learning to classify and detect an application whether it is a mobile botnet or benign application. The features consist of numerous elements such as requested permissions, application programming interface (API) calls, strings, operation codes, system calls and network traffics (Feizollah et al., 2015; Baskaran & Ralescu, 2016; da Costa et al., 2017; Chen et al., 2018). However, not all the features are relevant for mobile botnet classification and detection. The used of irrelevant features might present problems such as increasing machine learning model complexity and reduce detection accuracy rate (Vajdi et al., 2016; Fereidooni et al., 2016; Arora & Peddoju, 2017). Karim et al., (2015) and da Costa et al., (2017) have stressed out that selecting significant features which characterized mobile botnet is very important in mobile botnet detection model. This

helps to reduce the selection of irrelevant features. Therefore, in this research, a new feature selection for mobile botnet classification is proposed. The selection of features is based on mobile botnet architecture and feature's risk impact to reduce selection of irrelevant features and for optimal mobile botnet detection's accuracy.

Finally, most existing mobile botnet detection models that have being proposed are not accompanied with applicable have response mechanism towards mobile botnet threat. This is because the existing research mainly focused on feature selection for mobile botnet classification and detection. Undoubtedly, joining in a response mechanism with mobile botnet detection is essential in order to quickly terminate the mobile botnet threat and restore a smartphone back to its safe operational mode.

Therefore, based on the implications of mobile botnet threat and gaps in existing research, it is utmost importance to develop a new mobile botnet detection and response model. Mobile botnet detection and response are crucial in protecting a smartphone user and functionality of the smartphone against privacy, financial and system invasions by mobile botnet. These include the reducing of irrelevant features for mobile botnet classification and the development of high accuracy mobile botnet detection and applicable response model for smartphone.

1.3 Research Questions

This research attempts to answer the following research questions in order to challenge the previously mentioned problems:

1) What are the features that should be selected to construct new mobile botnet classification?
2) How a new mobile botnet classification can differentiate benign application and mobile botnet application?
3) How to trigger detection and response mechanism against mobile botnet threat?

1.4 Research Objectives

The main objectives for this research are as follow:

1) To construct a new mobile botnet classification using features based on mobile botnet architecture and feature's risk impact.
2) To develop mobile botnet detection and response model based on the mobile botnet classification, risk level and by applying apoptosis concept.
3) To evaluate the proposed mobile botnet detection and response model based on accuracy rate.

The objectives of this research have been mapped with research outcome as presented in Figure 1.2.

REFERENCES

Abdul Kadir, A. F., Stakhanova, N. & Ghorbani, A. A. 2015. Android Botnets: What URLs are Telling Us. In *Network and System Security*. Elsevier, pp. 78–91. Available at: http://www.sciencedirect.com/science/article/pii/B9780124166899000022.

Abdullah, Z., Saudi, M. M. & Anuar, N. B. 2014. Mobile botnet detection: Proof of concept. In *Proceedings - 2014 5th IEEE Control and System Graduate Research Colloquium, ICSGRC 2014*.

Ahmadi, M., Ulyanov, D., Semenov, S., Trofimov, M. & Giacinto, G. 2015. Novel Feature Extraction, Selection and Fusion for Effective Malware Family Classification. , (March). Available at: http://arxiv.org/abs/1511.04317.

Akella, R., Debroy, S., Calyam, P., Berryman, A., Zhu, K. & Sridharan, M. 2016. Security Middleground for Resource Protection in Measurement Infrastructure-as-a-Service. *IEEE Transactions on Services Computing*, 1374(c), pp.1–1. Available at: http://ieeexplore.ieee.org/document/7593347/.

Aksu, M. U., Dilek, M. H., Tatli, E. I., Bicakci, K., Dirik, H. I., Demirezen, M. U. & Aykir, T. 2017. A quantitative CVSS-based cyber security risk assessment methodology for IT systems. In *2017 International Carnahan Conference on Security Technology (ICCST)*. IEEE, pp. 1–8. Available at: http://ieeexplore.ieee.org/document/8167819/.

Ali, M. A. M. & Maarof, M. A. 2013. Dynamic innate immune system model for malware detection. *2013 International Conference on IT Convergence and Security, ICITCS 2013*, pp.3–6.

Ali, M. Al, Svetinovic, D., Aung, Z. & Lukman, S. 2017. Malware detection in android mobile platform using machine learning algorithms. In *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*. IEEE, pp. 763–768. Available at: http://ieeexplore.ieee.org/document/8286109/.

Almasizadeh, J. & Azgomi, M. A. 2013. A stochastic model of attack process for the evaluation of security metrics. *Computer Networks*, 57(10), pp.2159–2180. Available at: http://dx.doi.org/10.1016/j.comnet.2013.03.011.

Alsaleh, M., Alomar, N. & Alarifi, A. 2017. Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods K.-K. R. Choo, ed. *PLOS ONE*, 12(3), p.e0173284. Available at: https://dx.plos.org/10.1371/journal.pone.0173284.

Alshahrani, H., Mansourt, H., Thorn, S., Alshehri, A., Alzahrani, A. & Fu, H. 2018. DDefender: Android application threat detection using static and dynamic analysis. In *2018 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, pp. 1–6. Available at: http://ieeexplore.ieee.org/document/8326293/.

Amini, A. & Jamil, N. 2018. A Comprehensive Review of Existing Risk Assessment Models in Cloud Computing. *Journal of Physics: Conference Series*, 1018, p.012004. Available at: http://stacks.iop.org/1742-6596/1018/i=1/a=012004?key=crossref.a3888bf9f8bd093064ff84cf89975942.

Amos, B., Turner, H. & White, J. 2013. Applying machine learning classifiers to dynamic Android malware detection at scale. In *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, pp. 1666–1671. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6583806&tag=1.

Anwar, S., Zain, J. M., Inayat, Z., Haq, R. U., Karim, A. & Jabir, A. N. 2016. A static approach towards mobile botnet detection. In *2016 3rd International Conference on Electronic Design (ICED)*. IEEE, pp. 563–567. Available at: http://ieeexplore.ieee.org/document/7804708/.

Arabo, A. & Pranggono, B. 2013. Mobile Malware and Smart Device Security: Trends, Challenges and Solutions. In *2013 19th International Conference on Control Systems and Computer Science*. IEEE, pp. 526–531. Available at: http://ieeexplore.ieee.org/document/6569314/.

Arora, A. & Peddoju, S. K. 2017. Minimizing Network Traffic Features for Android Mobile Malware Detection. In *Proceedings of the 18th International Conference on Distributed Computing and Networking - ICDCN '17*. New York, New York, USA: ACM Press, pp. 1–10. Available at: http://dl.acm.org/citation.cfm?doid=3007748.3007763.

Arora, A. & Peddoju, S. K. 2018. NTPDroid: A Hybrid Android Malware Detector Using Network Traffic and System Permissions. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, pp. 808–813. Available at: https://ieeexplore.ieee.org/document/8455983/.

Arp, D., Spreitzenbarth, M., Malte, H., Gascon, H. & Rieck, K. 2014. Drebin: Effective and Explainable Detection of Android Malware in Your Pocket. *Symposium on Network and Distributed System Security (NDSS)*, pp.23–26.

Arshad, S., Ali, M., Khan, A. & Ahmed, M. 2016. Android Malware Detection & Protection: A Survey. *International Journal of Advanced Computer Science and Applications*, 7(2), pp.463–475. Available at: http://thesai.org/Publications/ViewPaper?Volume=7&Issue=2&Code=ijacsa&SerialNo=62.

Asokan, N., Davi, L., Dmitrienko, A., Heuser, S., Kostiainen, K., Reshetova, E. & Sadeghi, A.-R. 2013. Mobile Platform Security. *Synthesis Lectures on Information Security, Privacy, and Trust*, 4(3), pp.1–108. Available at: https://doi.org/10.2200/S00555ED1V01Y201312SPT009.

Azuwa, M. P., Ahmad, R., Sahib, S. & Shamsuddin, S. 2012. A propose technical security metrics model for SCADA systems. In *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*. IEEE, pp. 70–75. Available at: http://ieeexplore.ieee.org/document/6246089/.

Baskaran, B. & Ralescu, A. 2016. A Study of Android Malware Detection Techniques and Machine Learning. *Cluster Computing*, 19(4), pp.2295–2304. Available at: http://ecommons.udayton.edu/cgi/viewcontent.cgi?article=1015&context=maics%0Ahttp://link.springer.com/10.1007/s10586-016-0630-5.

Bayar, N., Darmoul, S., Hajri-Gabouj, S. & Pierreval, H. 2015. Fault detection, diagnosis and recovery using Artificial Immune Systems: A review. *Engineering Applications of Artificial Intelligence*, 46, pp.43–57.

Bernaschi, M., Gabrielli, E. & Mancini, L. V 2000. Operating system enhancements to prevent the misuse of system calls. In *Proceedings of the 7th ACM conference on Computer and communications security - CCS '00*. New York, New York, USA: ACM Press, pp. 174–183. Available at: http://portal.acm.org/citation.cfm?doid=352600.352624.

Burguera, I., Zurutuza, U. & Nadjm-Tehrani, S. 2011. Crowdroid: Behavior-Based Malware Detection System for Android. *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices - SPSM '11*, p.15. Available at: http://dl.acm.org/citation.cfm?id=2046619%5Cnhttp://dl.acm.org/citation.cfm?doid=2046614.2046619.

Canfora, G., Medvet, E., Mercaldo, F. & Visaggio, C. A. 2015. Detecting Android malware using sequences of system calls. In *Proceedings of the 3rd International Workshop on Software Development Lifecycle for Mobile - DeMobile 2015*. New York, New York, USA: ACM Press, pp. 13–20. Available at: http://doi.acm.org/10.1145/2804345.2804349.

Chang, Y.-C. & Wang, S.-D. 2016. The Concept of Attack Scenarios and Its Applications in Android Malware Detection. In *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, pp. 1485–1492. Available at: http://ieeexplore.ieee.org/document/7828552/.

Chen, C.-M., Lai, G.-H. & Lin, J.-M. 2017. Identifying Threat Patterns of Android Applications. In *2017 12th Asia Joint Conference on Information Security (AsiaJCIS)*. IEEE, pp. 69–74. Available at: http://ieeexplore.ieee.org/document/8026043/.

Chen, Z., Yan, Q., Han, H., Wang, S., Peng, L., Wang, L. & Yang, B. 2018. Machine learning based mobile malware detection using highly imbalanced network traffic. *Information Sciences*, 433–434, pp.346–364. Available at: https://linkinghub.elsevier.com/retrieve/pii/S0020025517307077.

Cheng, Y., Deng, J., Li, J., DeLoach, S. A., Singhal, A. & Ou, X. 2014. Metrics of Security. In *Advances in Information Security*. pp. 263–295. Available at: http://link.springer.com/10.1007/978-3-319-11391-3_13.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. & Stoddart, K. 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56, pp.1–27. Available at: http://dx.doi.org/10.1016/j.cose.2015.09.009.

da Costa, V. G. T., Barbon, S., Miani, R. S., Rodrigues, J. J. P. C. & Zarpelao, B. B. 2017. Detecting mobile botnets through machine learning and system calls analysis. In *2017 IEEE International Conference on Communications (ICC)*. IEEE, pp. 1–6. Available at: http://ieeexplore.ieee.org/document/7997390/.

Deylami, H. M., Muniyandi, R. C., Ardekani, I. T. & Sarrafzadeh, A. 2016. Taxonomy of malware detection techniques: A systematic literature review. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, pp. 629–636. Available at: http://ieeexplore.ieee.org/document/7906998/.

Deypir, M. 2016. A new approach for effective malware detection in Android-based devices. In *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*. IEEE, pp. 112–116. Available at: http://ieeexplore.ieee.org/document/7736461/.

Dini, G., Martinelli, F., Matteucci, I., Petrocchi, M., Saracino, A. & Sgandurra, D. 2016. Risk analysis of Android applications: A user-centric solution. *Future Generation Computer Systems*. Available at: http://dx.doi.org/10.1016/j.future.2016.05.035.

Dini, G., Martinelli, F., Saracino, A. & Sgandurra, D. 2012. MADAM: A multi-level anomaly detector for android malware. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7531 LNCS, pp.240–253.

Enck, W., Octeau, D., McDaniel, P. & Chaudhuri, S. 2011. A Study of Android Application Security. *USENIX Security*, 39(August), pp.21–21. Available at: http://www.usenix.org/event/sec11/tech/slides/enck.pdf%5Cnhttp://dl.acm.org/citation.cfm?id=2028067.2028088.

Eslahi, M., Salleh, R. & Anuar, N. B. 2012. MoBots: A new generation of botnets on mobile devices and networks. In *2012 International Symposium on Computer Applications and Industrial Electronics (ISCAIE)*. IEEE, pp. 262–266. Available at: http://ieeexplore.ieee.org/document/6482109/.

Eslahi, M., Yousefi, M., Naseri, M. V., Yussof, Y. M., Tahir, N. M. & Hashim, H. 2016. Mobile Botnet Detection Model based on Retrospective Pattern Recognition. *International Journal of Security and Its Applications*, 10(9), pp.39–44. Available at: http://www.sersc.org/journals/IJSIA/vol10_no9_2016/5.pdf.

Etaher, N., Weir, G. R. S. & Alazab, M. 2015. From ZeuS to Zitmo: Trends in Banking Malware. In *2015 IEEE Trustcom/BigDataSE/ISPA*. IEEE, pp. 1386–1391. Available at: http://ieeexplore.ieee.org/document/7345443/.

Everett, H. & McFadden, G. 1999. Apoptosis: An innate immune response to virus infection. *Trends in Microbiology*, 7(4), pp.160–165.

Fayyad, U., Piatetsky-Shapiro, G. & Smyth, P. 1996. The KDD process for extracting useful knowledge from volumes of data. *Communications of the ACM*, 39(11), pp.27–34. Available at: http://portal.acm.org/citation.cfm?doid=240455.240464.

Feizollah, A., Anuar, N. B., Salleh, R., Amalina, F., Ma'arof, R. R. & Shamshirband, S. 2013. A study of machine learning classifiers for anomaly-based mobile botnet detection. *Malaysian Journal of Computer Science*, 26(4), pp.251–265.

Feizollah, A., Anuar, N. B., Salleh, R. & Wahab, A. W. A. 2015. A review on feature selection in mobile malware detection. *Digital Investigation*, 13, pp.22–37. Available at: http://dx.doi.org/10.1016/j.diin.2015.02.001.

Felt, A., Greenwood, K. & Wagner, D. 2011. The effectiveness of application permissions. *WebApps '11: 2nd USENIX Conference on Web Application Development*, pp.75–86. Available at: https://www.usenix.org/legacy/events/webapps11/tech/final_files/webapps11_proceedings.pdf#page=83.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E. & Wagner, D. 2012. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*. New York, New York, USA: ACM Press, p. 1. Available at: http://dl.acm.org/citation.cfm?doid=2335356.2335360.

Feng, P., Ma, J. & Sun, C. 2017. Selecting Critical Data Flows in Android Applications for Abnormal Behavior Detection. *Mobile Information System*, 2017, pp.1–16.

Fereidooni, H., Conti, M., Yao, D. & Sperduti, A. 2016. ANASTASIA: ANdroid mAlware detection using STatic analySIs of Applications. In *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, pp. 1–5. Available at: http://ieeexplore.ieee.org/document/7792435/.

Ferrante, A., Medvet, E., Mercaldo, F., Milosevic, J. & Visaggio, C. A. 2016. Spotting the Malicious Moment: Characterizing Malware Behavior Using Dynamic Features. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE, pp. 372–381. Available at: http://ieeexplore.ieee.org/document/7784595/.

Forrest, S., Perelson, A. S., Allen, L. & Cherukuri, R. 1994. Self-nonself discrimination in a computer. In *Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy*. IEEE Comput. Soc. Press, pp. 202–212. Available at: http://ieeexplore.ieee.org/document/296580/.

Fox, S., Leitch, A. E., Duffin, R., Haslett, C. & Rossi, A. G. 2010. Neutrophil apoptosis: Relevance to the innate immune response and inflammatory disease. *Journal of Innate Immunity*, 2(3), pp.216–227.

Girei, D. A., Ali Shah, M. & Shahid, M. B. 2016. An enhanced botnet detection technique for mobile devices using log analysis. In *2016 22nd International Conference on Automation and Computing (ICAC)*. IEEE, pp. 450–455. Available at: http://ieeexplore.ieee.org/document/7604961/.

Google 2019. Android Developers. Available at: https://developer.android.com/images/system-architecture.jpg [Accessed March 9, 2019].

Google 2018. Distribution dashboard | Android developers. Available at: https://developer.android.com/about/dashboards/ [Accessed August 21, 2018].

Gopinath Bharathi, A. K. B., Singh, A., Tucker, C. S. & Nembhard, H. B. 2016. Knowledge discovery of game design features by mining user-generated feedback. *Computers in Human Behavior*, 60(July), pp.361–371. Available at: http://dx.doi.org/10.1016/j.chb.2016.02.076.

Grace, M., Zhou, Y., Zhang, Q., Zou, S. & Jiang, X. 2012. RiskRanker: Scalable and Accurate Zero-day Android Malware Detection. In *Proceedings of the 10th international conference on Mobile systems, applications, and services - MobiSys '12*. New York, New York, USA: ACM Press, p. 281. Available at: http://dl.acm.org/citation.cfm?doid=2307636.2307663.

Hijawi, W., Alqatawna, J. & Faris, H. 2017. Toward a Detection Framework for Android Botnet. In *2017 International Conference on New Trends in Computing Sciences (ICTCS)*. IEEE, pp. 197–202. Available at: http://ieeexplore.ieee.org/document/8250288/.

Hsieh, W.-C., Wu, C.-C. & Kao, Y.-W. 2015. A study of android malware detection technology evolution. In *2015 International Carnahan Conference on Security Technology (ICCST)*. IEEE, pp. 135–140. Available at: http://ieeexplore.ieee.org/document/7389671/.

Hur, J. B. & Shamsi, J. A. 2017. A survey on security issues, vulnerabilities and attacks in Android based smartphone. In *2017 International Conference on Information and Communication Technologies (ICICT)*. IEEE, pp. 40–46. Available at: http://ieeexplore.ieee.org/document/8320163/.

Irwan, Asnar, Y. & Hendradjaya, B. 2015. Confidentiality and privacy information security risk assessment for Android-based mobile devices. In *2015 International Conference on Data and Software Engineering (ICoDSE)*. IEEE, pp. 1–6. Available at: http://ieeexplore.ieee.org/document/7436972/.

Jeon, W., Kim, J., Lee, Y. & Won, D. 2011. A Practical Analysis of Smartphone Security. In M. J. Smith & G. Salvendy, eds. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 311–320. Available at: http://link.springer.com/10.1007/978-3-642-21793-7.

Jo, S. & Chung, K. 2012. Proceedings of the International Conference on IT Convergence and Security 2011. *Control*, 120(January 2016), pp.81–90. Available at: http://www.springerlink.com/index/10.1007/978-94-007-2911-7.

Jorgensen, Z., Chen, J., Gates, C. S., Li, N., Proctor, R. W. & Yu, T. 2015. Dimensions of Risk in Mobile Applications. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy - CODASPY '15*. New York, New York, USA: ACM Press, pp. 49–60. Available at: http://dl.acm.org/citation.cfm?doid=2699026.2699108.

Kalige, E., Burkey, D. & Director, I. P. S. 2012. A Case Study of Eurograbber: How 36 Million Euros Was Stolen via Malware. *Versafe White Paper*, (December).

Karim, A., Salleh, R. & Khan, M. K. 2016. SMARTbot: A behavioral analysis framework augmented with machine learning to identify mobile botnet applications. *PLoS ONE*, 11(3), pp.1–35.

Karim, A., Salleh, R., Khan, M. K., Siddiqa, A. & Choo, K.-K. R. 2016. On the Analysis and Detection of Mobile Botnet. *Journal of Universal Computer Science*, 22(4), pp.567–588.

Karim, A., Salleh, R. & Shah, S. A. A. 2015. DeDroid: A Mobile Botnet Detection Approach Based on Static Analysis. In *2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*. IEEE, pp. 1327–1332. Available at: http://ieeexplore.ieee.org/document/7518419/.

Kaur, P., Singh, M. & Josan, G. S. 2015. Classification and Prediction Based Data Mining Algorithms to Predict Slow Learners in Education Sector. *Procedia Computer Science*, 57, pp.500–508. Available at: http://dx.doi.org/10.1016/j.procs.2015.07.372.

Khune, R. S. & Thangakumar, J. 2012. A cloud-based intrusion detection system for Android smartphones. In *2012 International Conference on Radar, Communication and Computing (ICRCC)*. IEEE, pp. 180–184. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6450572.

Kim, H., Agrawal, N. & Ungureanu, C. 2012. Revisiting storage for smartphones. *ACM Transactions on Storage*, 8(4), pp.1–25. Available at: http://dl.acm.org/citation.cfm?doid=2385603.2385607.

Kim, T., Kang, B., Rho, M., Sezer, S. & Im, E. G. 2019. A Multimodal Deep Learning Method for Android Malware Detection Using Various Features. *IEEE Transactions on Information Forensics and Security*, 14(3), pp.773–788. Available at: https://ieeexplore.ieee.org/document/8443370/.

Koli, J. D. 2018. RanDroid: Android malware detection using random machine learning classifiers. In *2018 Technologies for Smart-City Energy Security and Power (ICSESP)*. IEEE, pp. 1–6. Available at: https://ieeexplore.ieee.org/document/8376705/.

Kostiainen, K., Reshetova, E., Ekberg, J.-E. & Asokan, N. 2011. Old, new, borrowed, blue --. In *Proceedings of the first ACM conference on Data and application security and privacy - CODASPY '11*. New York, New York, USA: ACM Press, p. 13. Available at: http://dl.acm.org/citation.cfm?id=1943517%5Cnhttp://dblp.uni-trier.de/db/conf/codaspy/codaspy2011.html#KostiainenREA11.

Kotenko, I. & Doynikova, E. 2013. Security metrics for risk assessment of distributed information systems. In *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*. IEEE, pp. 646–650. Available at: /Users/jamie/SkyDrive/Forensics/CTEC5306/Research/security metrics for risk assessment of distributed information systems.pdf.

Kumar, A., Kuppusamy, K. S. & Aghila, G. 2018. FAMOUS: Forensic Analysis of MObile Devices Using Scoring of application permissions. *Future Generation Computer Systems*, 83, pp.158–172. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167739X17323257.

Li, Q. & Clark, G. 2013. Mobile Security: A Look Ahead. *IEEE Security & Privacy*, 11(1), pp.78–81. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84873374971&partnerID=tZOtx3y1.

Liang, S. & Du, X. 2014. Permission-combination-based scheme for Android mobile malware detection. *2014 IEEE International Conference on Communications, ICC 2014*, (JUNE 2014), pp.2301–2306.

Liang, X., Tian, J., Ding, X. & Wang, G. 2015. A Risk and Similarity Aware Application Recommender System. *Journal of Computing and Information Technology*, 23(4), p.303. Available at: http://cit.srce.unizg.hr/index.php/CIT/article/view/2537.

Lindorfer, M., Neugschwandtner, M. & Platzer, C. 2015. MARVIN: Efficient and Comprehensive Mobile App Classification through Static and Dynamic Analysis. In *2015 IEEE 39th Annual Computer Software and Applications Conference*. IEEE, pp. 422–433. Available at: http://ieeexplore.ieee.org/document/7273650/.

Lindorfer, M., Neugschwandtner, M., Weichselbaum, L., Fratantonio, Y., Veen, V. Van Der & Platzer, C. 2016. ANDRUBIS - 1,000,000 Apps Later: A View on Current Android Malware Behaviors. *Proceedings - 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS 2014*, pp.3–17.

Mahindru, A. & Singh, P. 2017. Dynamic Permissions based Android Malware Detection using Machine Learning Techniques. *Proceedings of the 10th Innovations in Software Engineering Conference on - ISEC '17*, (March 2018), pp.202–210. Available at: http://dl.acm.org/citation.cfm?doid=3021460.3021485.

Martín, A., Lara-Cabrera, R. & Camacho, D. 2019. Android malware detection through hybrid features fusion and ensemble classifiers: The AndroPyTool framework and the OmniDroid dataset. *Information Fusion*, 52(December 2018), pp.128–142. Available at: https://linkinghub.elsevier.com/retrieve/pii/S1566253518306778.

Mas'ud, M. Z., Sahib, S., Abdollah, M. F., Selamat, S. R. & Huoy, C. Y. 2017. A Comparative Study on Feature Selection Method for N-gram Mobile Malware Detection. , 19(5), pp.1–7.

Mas'ud, M. Z., Sahib, S., Abdollah, M. F., Selamat, S. R., Yusof, R. & Ahmad, R. 2013. Profiling mobile malware behaviour through hybrid malware analysis approach. In *2013 9th International Conference on Information Assurance and Security (IAS)*. IEEE, pp. 78–84. Available at: http://ieeexplore.ieee.org/document/6947737/.

McAfee Labs 2018. *McAfee Labs Threats Report*, Available at: https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2018.pdf [Accessed April 15, 2018].

Medzhitov, R. & Janeway, C. A. 2002. Decoding the patterns of self and nonself by the innate immune system. *Science (New York, N.Y.)*, 296(5566), pp.298–300. Available at: http://www.ncbi.nlm.nih.gov/pubmed/11951031.

Milosevic, J., Regazzoni, F. & Malek, M. 2017. *Hardware Security and Trust* N. Sklavos, R. Chaves, G. Di Natale, & F. Regazzoni, eds., Cham: Springer International Publishing. Available at: http://link.springer.com/10.1007/978-3-319-44318-8.

Mohd Saudi, M., Woodward, M., Cullen, A. J. & Mohd Noor, H. 2008. An overview of apoptosis for computer security. In *2008 International Symposium on Information Technology*. IEEE, pp. 1–6. Available at: http://ieeexplore.ieee.org/document/4631907/.

Moonsamy, V., Rong, J. & Liu, S. 2014. Mining permission patterns for contrasting clean and malicious android applications. *Future Generation Computer Systems*, 36, pp.122–132. Available at: http://dx.doi.org/10.1016/j.future.2013.09.014.

Morales-Ortega, S., Escamilla-Ambrosio, P. J., Rodriguez-Mota, A. & Coronado-De-Alba, L. D. 2016. Native malware detection in smartphones with android OS using static analysis, feature selection and ensemble classifiers. In *2016 11th International Conference on Malicious and Unwanted Software (MALWARE)*. IEEE, pp. 1–8. Available at: http://ieeexplore.ieee.org/document/7888731/.

Mostafa, A. H., Elfattah, M. M. A. & Youssif, A. A. A. 2015. Reduced Permissions Schema for Malware Detection in Android Smartphones. In *Recent Advances in Computer Science, 19th Int. Conf. on Circuits, Systems, Communications and Computers (CSCC 2015)*,. pp. 406–413.

Mylonas, A., Kastania, A. & Gritzalis, D. 2013. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers and Security*, 34, pp.47–66.

Mylonas, A., Theoharidou, M. & Gritzalis, D. 2014. Assessing Privacy Risks in Android : A User-Centric Approach. , pp.21–37.

Narudin, F. A., Feizollah, A., Anuar, N. B. & Gani, A. 2016. Evaluation of machine learning classifiers for mobile malware detection. *Soft Computing*, 20(1), pp.343–357.

Naway, A. & LI, Y. 2018. A Review on The Use of Deep Learning in Android Malware Detection. *International Journal of Computer Science and Mobile Computing*, 7(12), pp.42–58. Available at: https://arxiv.org/pdf/1812.10360.pdf.

Olsen, M. M., Siegelmann-Danieli, N. & Siegelmann, H. T. 2008. Robust artificial life via artificial programmed death. *Artificial Intelligence*, 172(6–7), pp.884–898. Available at: https://linkinghub.elsevier.com/retrieve/pii/S0004370207001506.

Oppliger, R. 2015. Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale. *IEEE Security & Privacy*, 13(6), pp.18–21. Available at: http://ieeexplore.ieee.org/document/7349099/.

Oulehla, M. & Malanik, D. 2016. Detection of Mobile Botnets using Neural Networks. *Future Technologies Conference (FTC)*, (December), pp.1324–1326. Available at: http://ieeexplore.ieee.org/abstract/document/7821774/.

Parham, P. 2015. *The Immune System*, Garland Science.

Peng, H., Gates, C., Sarma, B., Li, N., Qi, Y., Potharaju, R., Nita-Rotaru, C. & Molloy, I. 2012. Using Probabilistic Generative Models for Ranking Risks of Android Apps. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, pp.241–252. Available at: http://doi.acm.org/10.1145/2382196.2382224.

Peng, S., Yu, S. & Yang, A. 2014. Smartphone Malware and Its Propagation Modeling: A Survey. *IEEE Communications Surveys & Tutorials*, 16(2), pp.925–941. Available at: http://ieeexplore.ieee.org/document/6563277/.

Pieterse, H. & Olivier, M. S. 2012. Android Botnets on the Rise: Trends and Characteristics. *2012 Information Security for South Africa - Proceedings of the ISSA 2012 Conference*.

Qiao, M., Sung, A. H. & Liu, Q. 2016. Merging permission and api features for android malware detection. *Proceedings - 2016 5th IIAI International Congress on Advanced Applied Informatics, IIAI-AAI 2016*, pp.566–571.

Qu, W. & Zhang, D.-Z. 2007. Security Metrics Models and Application with SVM in Information Security Management. In *2007 International Conference on Machine Learning and Cybernetics*. IEEE, pp. 3234–3238. Available at: http://ieeexplore.ieee.org/document/4370705/.

Quan, D., Zhai, L., Yang, F. & Wang, P. 2014. Detection of Android Malicious Apps Based on the Sensitive Behaviors. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, pp. 877–883. Available at: http://ieeexplore.ieee.org/document/7011341/.

Riordan, J. & Alessandri, D. 2000. Target Naming and Service Apoptosis. In *Security*. pp. 217–225.

Rodriguez-Mota, A., Escamilla-Ambrosio, P. J., Morales-Ortega, S., Salinas-Rosales, M. & Aguirre-Anaya, E. 2016. Towards a 2-hybrid Android malware detection test framework. In *2016 International Conference on Electronics, Communications and Computers (CONIELECOMP)*. IEEE, pp. 54–61. Available at: http://dx.doi.org/10.1109/CONIELECOMP.2016.7438552.

Rubenking, N. J. 2018. The Best Antivirus Protection of 2018 - PCMag Asia. *Ziff Davis, LLC*. Available at: https://sea.pcmag.com/antivirus/22/guide/the-best-antivirus-protection-of-2018 [Accessed August 26, 2018].

Sahal, A. A., Alam, S. & Sogukpinar, I. 2018. Mining and Detection of Android Malware Based on Permissions. In *2018 3rd International Conference on Computer Science and Engineering (UBMK)*. IEEE, pp. 264–268. Available at: https://ieeexplore.ieee.org/document/8566510/.

Sanz, B., Santos, I., Nieves, J., Laorden, C., Alonso-Gonzalez, I. & Bringas, P. G. 2013. MADS: Malicious Android Applications Detection through String Analysis. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. pp. 178–191. Available at: http://link.springer.com/10.1007/978-3-642-38631-2_14.

Saudi, M. M., Cullen, A. J. & Woodward, M. E. 2011. Efficient STAKCERT KDD Processes in Worm Detection. *World Academy of Science, Engineering and Technology*, 55(7), pp.376–380.

Savola, R. M. 2009. A Security Metrics Taxonomization Model for Software-Intensive Systems. *Journal of Information Processing Systems*, 5(4), pp.197–206. Available at: http://koreascience.or.kr/journal/view.jsp?kj=E1JBB0&py=2009&vnc=v5n4&sp=197.

Savola, R. M. 2013. Quality of security metrics and measurements. *Computers & Security*, 37, pp.78–90. Available at: 10.1016/j.cose.2013.05.002.

Schmidt, A.-D., Bye, R., Schmidt, H.-G., Clausen, J., Kiraz, O., Yuksel, K. A., Camtepe, S. A. & Albayrak, S. 2009. Static Analysis of Executables for Collaborative Malware Detection on Android. In *2009 IEEE International Conference on Communications*. IEEE, pp. 1–5. Available at: http://ieeexplore.ieee.org/document/5199486/.

Shabtai, A. & Elovici, Y. 2010. Applying Behavioral Detection on Android-Based Devices. In *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*. pp. 235–249. Available at: http://link.springer.com/10.1007/978-3-642-17758-3_17.

Shamala, P., Ahmad, R. & Yusoff, M. 2013. A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, 18(1), pp.45–52. Available at: http://dx.doi.org/10.1016/j.jisa.2013.07.002.

Shameli-Sendi, A., Aghababaei-Barzegar, R. & Cheriet, M. 2016. Taxonomy of information security risk assessment (ISRA). *Computers & Security*, 57, pp.14–30. Available at: http://dx.doi.org/10.1016/j.cose.2015.11.001.

Sharma, A. & Sahay, S. K. 2016. An effective approach for classification of advanced malware with high accuracy. *International Journal of Security and its Applications*, 10(4), pp.249–266.

Shezan, F. H., Afroze, S. F. & Iqbal, A. 2017. Vulnerability detection in recent Android apps: An empirical study. In *2017 International Conference on Networking, Systems and Security (NSysS)*. IEEE, pp. 55–63. Available at: http://ieeexplore.ieee.org/document/7885802/.

Shijo, P. V. & Salim, A. 2015. Integrated Static and Dynamic Analysis for Malware Detection. *Procedia Computer Science*, 46(Icict 2014), pp.804–811. Available at: http://dx.doi.org/10.1016/j.procs.2015.02.149.

Singh, L. & Hofmann, M. 2017. Dynamic behavior analysis of android applications for malware detection. In *2017 International Conference on Intelligent Communication and Computational Techniques (ICCT)*. IEEE, pp. 1–7. Available at: http://ieeexplore.ieee.org/document/8324010/.

Singh, V. & Sharma, K. 2016. Smartphone Security. *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16*, pp.1–3. Available at: http://dl.acm.org/citation.cfm?doid=2905055.2905214.

Skovoroda, A. A. & Gamayunov, D. Y. 2017. Automated static analysis and classification of Android malware using permission and API calls models. *Prikladnaya diskretnaya matematika*, (36), pp.84–105. Available at: http://journals.tsu.ru/pdm/&journal_page=archive&id=1591&article_id=35291.

Sokolova, K., Perez, C. & Lemercier, M. 2017. Android application classification and anomaly detection with graph-based permission patterns. *Decision Support Systems*, 93, pp.62–76. Available at: http://dx.doi.org/10.1016/j.dss.2016.09.006.

Sridevi, R. & Jagajothi, G. 2014. Apoptosis Inspired Intrusion Detection System. *International Journal of Computer and Information Engineering*, 8(10), pp.1890–1896.

Statista 2016. • Smartphone Market Share Malaysia 2015-2016 | Statistic. Available at: https://www.statista.com/statistics/461191/smartphone-vendor-shares-malaysia/ [Accessed August 23, 2018].

Sterritt, R. 2011. Apoptotic computing: Programmed death by default for computer-based systems. *Computer*, 44(1), pp.59–65. Available at: http://ieeexplore.ieee.org/document/5688151/.

Sterritt, R. & Hinchey, M. 2018. Apoptotic Computing: Programmed Death by Default for Software Technologies. In *Software Technology: 10 Years of Innovation in IEEE Computer*. Hoboken, NJ, USA: John Wiley & Sons, Inc., pp. 91–106. Available at: http://doi.wiley.com/10.1002/9781119174240.ch5.

Stoneburner, G., Goguen, A. & Feringa, A. 2002. *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*, Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.6062&rep=rep1&type=pdf.

Suarez-Tangil, G., Dash, S. K., Ahmadi, M., Kinder, J., Giacinto, G. & Cavallaro, L. 2017. DroidSieve. *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy - CODASPY '17*, pp.309–320. Available at: http://dl.acm.org/citation.cfm?doid=3029806.3029825.

Sun, L. 2016. Significant Permission Identification for Android Malware Detection. *Computer Science and Engineering: Theses, Dissertations, and Student Research*. Available at: http://digitalcommons.unl.edu/computerscidiss/104 [Accessed November 8, 2016].

Sun, M., Li, X., Lui, J. C. S., Ma, R. T. B. & Liang, Z. 2017. Monet: A User-Oriented Behavior-Based Malware Variants Detection System for Android. *IEEE Transactions on Information Forensics and Security*, 12(5), pp.1103–1112.

Taleby, M., Li, Q., Rabbani, M. & Raza, A. 2017. A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. *International Journal of Advanced Computer Science and Applications*, 8(10), pp.30–45. Available at: http://thesai.org/Publications/ViewPaper?Volume=8&Issue=10&Code=ijacsa&SerialNo=5.

Tansettanakorn, C., Thongprasit, S., Thamkongka, S. & Visoottiviseth, V. 2016. ABIS: A prototype of Android Botnet Identification System. In *2016 Fifth ICT International Student Project Conference (ICT-ISPC)*. IEEE, pp. 1–5. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7519221.

Tchakounte, F. 2014. Permission-based Malware Detection Mechanisms on Android: Analysis and Perspectives. *Journal of Computer Science and Software Application*, 1(2), pp.63–77. Available at: http://www.researchgate.net/profile/Franklin_Tchakounte/publication/271199472_Permission-based_Malware_Detection_Mechanisms_on_Android_Analysis_and_Perspectives/links/54c11b5c0cf2d03405c4de97.pdf.

Theoharidou, M., Mylonas, A. & Gritzalis, D. 2012. A Risk Assessment Method for Smartphones. In pp. 443–456. Available at: http://link.springer.com/10.1007/978-3-642-30436-1_36.

Thompson, N., McGill, T. J. & Wang, X. 2017. "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, 70, pp.376–391. Available at: https://doi.org/10.1016/j.cose.2017.07.003.

Tong, F. & Yan, Z. 2017. A hybrid approach of mobile malware detection in Android. *Journal of Parallel and Distributed Computing*, 103, pp.22–31. Available at: http://linkinghub.elsevier.com/retrieve/pii/S074373151630140X.

Vajdi, M., Torkaman, A., Bahrololum, M., Tadayon, M. H. & Salajegheh, A. 2016. Proposed new features to improve Android malware detection. In *2016 8th International Symposium on Telecommunications (IST)*. IEEE, pp. 100–104. Available at: http://ieeexplore.ieee.org/document/7881791/.

Wang, C., Xu, Q., Lin, X. & Liu, S. 2018. Research on data mining of permissions mode for Android malware detection. *Cluster Computing*. Available at: http://link.springer.com/10.1007/s10586-018-1904-x.

Wang, X., Zhang, D., Su, X. & Li, W. 2017. Mlifdect: Android Malware Detection Based on Parallel Machine Learning and Information Fusion. *Security and Communication Networks*, 2017, pp.1–14. Available at: https://www.hindawi.com/journals/scn/2017/6451260/.

Wang, Z., Cai, J., Cheng, S. & Li, W. 2016. DroidDeepLearner: Identifying Android malware using deep learning. In *2016 IEEE 37th Sarnoff Symposium*. IEEE, pp. 160–165. Available at: http://ieeexplore.ieee.org/document/7846747/.

Wu, D. J., Mao, C. H., Wei, T. E., Lee, H. M. & Wu, K. P. 2012. DroidMat: Android Malware Detection Through Manifest and API Calls Tracing. *Proceedings of the 2012 7th Asia Joint Conference on Information Security, AsiaJCIS 2012*, pp.62–69.

Xu, L., Zhang, D., Jayasena, N. & Cavazos, J. 2016. HADM: Hybrid Analysis for Detection of Malware. In *SAI Intelligent Systems Conference (IntelliSys)*. pp. 702–724. Available at: http://link.springer.com/10.1007/978-3-319-56991-8_51.

Yahaya, A., Mohd, M. & Abdullah, I. 2017. A Review and Proof of Concept for Phishing Scam Detection and Response using Apoptosis. *International Journal of Advanced Computer Science and Applications*, 8(6), pp.284–289. Available at: http://thesai.org/Publications/ViewPaper?Volume=8&Issue=6&Code=ijacsa&SerialNo=37.

Ye, Y., Wu, L., Hong, Z. & Huang, K. 2017. A Risk Classification Based Approach for Android Malware Detection. *KSII Transactions on Internet and Information Systems*, 11(2), pp.959–981. Available at: http://itiis.org/digital-library/manuscript/1609.

Yerima, S. Y., Sezer, S. & Muttik, I. 2014. Android Malware Detection Using Parallel Machine Learning Classifiers. In *2014 Eighth International Conference on Next Generation Mobile Apps, Services and Technologies*. IEEE, pp. 37–42. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6982888.

Yerima, S. Y., Sezer, S. & Muttik, I. 2015. High accuracy android malware detection using ensemble learning. *IET Information Security*, 9(6), pp.313–320. Available at: http://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2014.0099.

Yu, J., Huang, Q. & Yian, C. 2016. DroidScreening: a practical framework for real-world Android malware analysis. *Security and Communication Networks*, 9(11), pp.1435–1449. Available at: http://doi.wiley.com/10.1002/sec.1430.

Yusof, M., Mohd Saudi, M. & Ridzuan, F. 2017. A New Mobile Botnet Classification based on Permission and API Calls. *Seventh IEEE International Conference on Emerging Security Technologies*, pp.122–127.

Zainal, K. & Jali, M. Z. 2015. A Perception Model of Spam Risk Assessment Inspired by Danger Theory of Artificial Immune Systems. *Procedia Computer Science*, 59(Iccsci), pp.152–161. Available at: http://dx.doi.org/10.1016/j.procs.2015.07.530.

Zhou, Y. & Jiang, X. 2012. Dissecting Android malware: Characterization and evolution. *Proceedings - IEEE Symposium on Security and Privacy*, (4), pp.95–109.