**Sit 382 Blockchain malware detection**

Chengzu Dong

215392074

Table of Contents

[Abstract 1](#_Toc521234049)

[Introduction 1](#_Toc521234050)

[Content 1](#_Toc521234051)

[Summary 1](#_Toc521234052)

[Reference 1](#_Toc521234053)

# Abstract

For solving the issue of detecting malicious codes in malware and extracting the corresponding evidences in Android mobile devices. A team in China build a consortium blockchain model, which is made of a detecting consortium chain shared by test members and a public chain shared by users. They implement feature modelling by utilizing statistical analysis method, so as to extract malware family features, including software package feature, permission and application feature, and function call feature. In addition, they create a fact-based of distributed Android malicious codes by blockchain technology. The results of experiment demonstrate that, compared with the previously published algorithms, the new method can reach higher detection accuracy in the shorter time with lower false-positive and false-negative rates. [5]

# Introduction

Blockchain has gained enormous attention for last few years because of de-centration technology, and it mainly used for cryptocurrency at the moment. However, Blockchain is a technology that it can be applied in many aspects such as IoT with Blockchain, security and Blockchain. There are many innovations and opportunities in Blockchain technology. Also, there are some challenges as well. For example, malicious code is the potential threaten to the Blockchain, it may cause cryptocurrency lost or other issues. For addressing the Blockchain malware vulnerability and avoiding the asset theft. This essay will introduce the Blockchain malware detection.

# Content

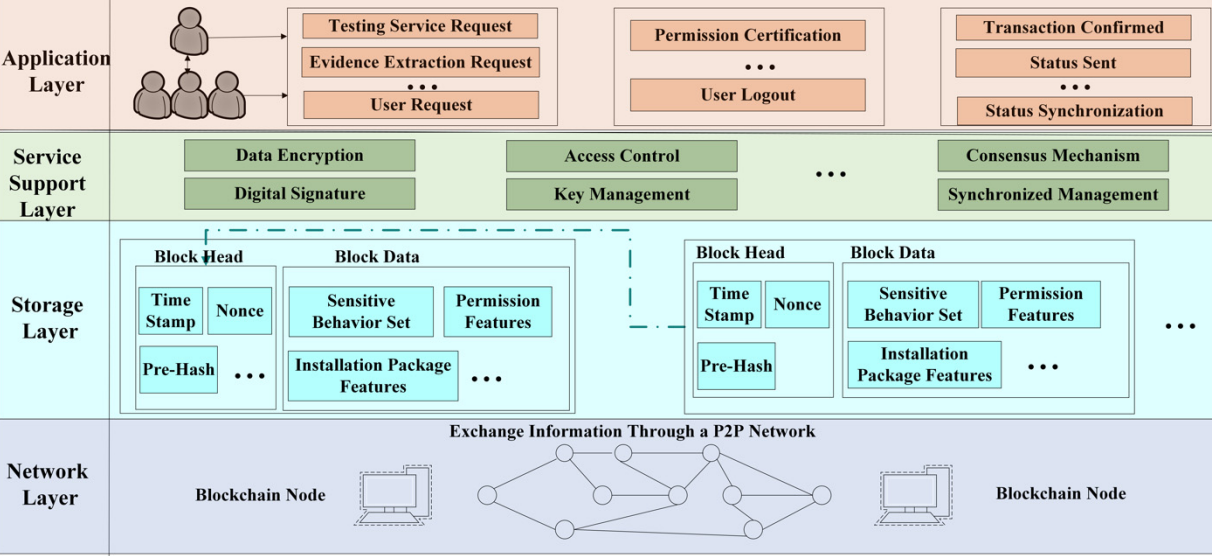
For the Blockchain technology, which can be divided into three parts. They are public chain, private chain and the consortium chain. The public chain that all the people can read and send transaction, and everyone can join the consensus process. For the private chain, customer can only join the consensus process from authorized organization. [4] In the consortium chain, only the super node can join the consensus process. Which has been preselected before the process and they have a copy of all data that in the distributed nodes. Today, some financial and non-financial systems have applied the consortium blockchain technology because of the flexibility of consortium chain.

Importantly, Blockchain technology is famous for cryptocurrency. And most of cryptocurrency transactions happened on the platform of third party those who provide both of web service and mobile device access. This article will focus on the Blockchain malware detection in mobile devices. And there is two dominated operating system take over the majority of market share in mobile devices. But IOS is a closed platform compare with Android. Therefore, Android system is riskier than the IOS system. And according to the statistics of Kaspersky lab, they detected 8,526,221 malicious installation packages, 128,886 mobile banking Trojans and 261,214 mobile ransomware Trojans. [1] Google has developed the malware detect tool, but it does not work well. Because malware spreading is easier to occur in the open source platform.

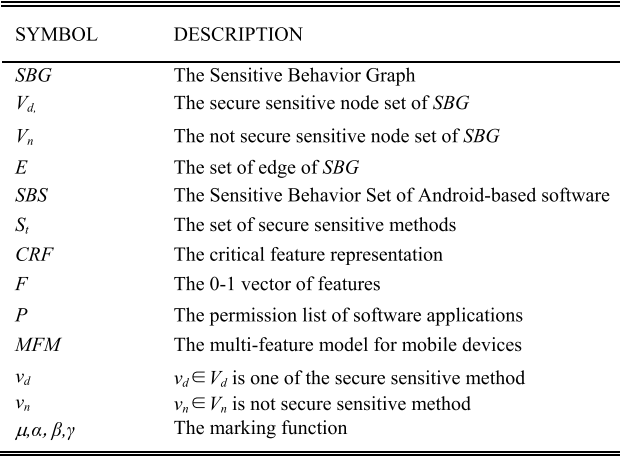
However, the malware detection is still possible to implement and there are some strategies for detecting malware in Blockchain system. For example, normally the anti-malware application will provide a quick bug repairing and maintenance service. But it would cost too much labour to keep updating the anti-virus software. Therefore, an automatic malware detection system is expected to be developed based on the machine learning concept. It can use self-taught leaning to detect malware intrusion. Also, users can detect malware intrusion through observing the phenomenon of device. If the device is running very slow compared with normal time. Or CPU and GPU usage are much higher than normal. The device may get malware attacked. Then users have to implement the efficient strategy to deal with the malwares.

In general, technically there are two categories of method to detect the malware in Blockchain system of Android-based. The first one is that static-based analysis, which can do the efficient analysis automatically, but it is not able to detect the malicious code in dynamic environment. The second one is dynamic-based analysis method for Android applications, which can retrieve the application running time information during the process. And they can deal with the encrypted code and obfuscated code. [3] But malware always has been well-pretended while most of the malware detection tool are not efficient and accurate. Nevertheless, there is a team in China has designed a framework for consortium Blockchain to detect malware and extract evidence in mobile devices. Which called CB-MDEE and it is made by mixed chains that including the consortium chain and public chain. [5] They build a model named Multi-Feature Model that using the fuzzy comparison approach based on Android system. They reduced the false-positive rate and enhance the possibility of malware detection. And they extract the specific function to the database while invent a malware detection algorithm. Then this team put malicious code in Android mobile device for testing their model is better than others. After the test result released, they compared with other existing algorithms. Then they found CB-MDEE have better performance on cost of time, accuracy of malware detection and recall rate.

The CB-MDEE model contains four layers, which are the network layer, storage layer, support layer and the application layer. In network layer, the nodes communicate through P2P network and there is not central node to manage the network. Each node sends data to the neighbour node. Then they spread the information literally in the network. All nodes continuously swap block data with their neighbour node. In the storage layer, the functions of malicious software have been saved. And each block has the malware data. They cannot change the data in blocks once the block data modified. The third layer is the support layer, which is the bridge between end consumer and malware. Also, it has the consensus mechanism features, encrypted data, digital signature, identity verification, access management, key control and synchronization management. For the application layer, the interfaces and programs have been supplied for applications. Normally, applications contain the evidence extraction and tracking. If the evidence has been submitted, a new block will be created, and the information of new block will be broadcasted.

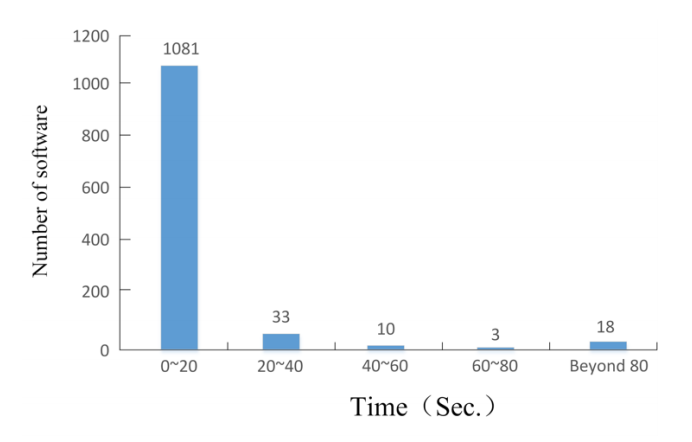
[5]

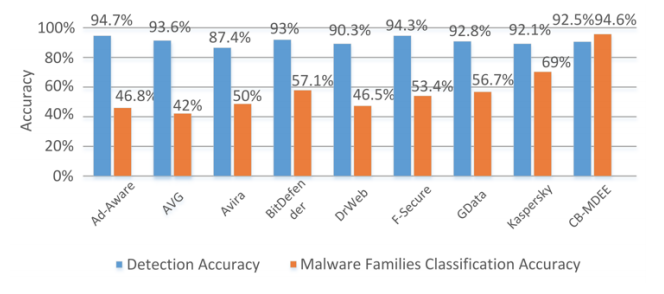
Also, there three parts in secure sensitive method, which are permission-protected, source/sink methods of data flows and other suspicious methods. For permission-protected method, the permission needs to be applied in Android system for visiting sensitive data in the system. For source/sink approach, it would create or send sensitive information. Because the Android system mainly operated by events and the intent mechanism to execute the Inter-Component Communication. Therefore, the SBG (sensitive behaviour graph) is added into the Inter-Component Communication. The symbol description of SBG has been shown in the figure below.

[5]

Even if the SBG of Android software can express the functions and behaviours. But there are too many features to produce a plenty of call function diagram. It will have very low extraction speed while extract feature. Therefore, the improvement should have during the process of extract sensitive behaviour set (SBS) based on SBG. The team in China extract the malware functions and build a multi-feature model for the Android based mobile devices. And they found the malware functions and features can be extract in installation files and SBS. It can be used for building a malware features centre and it will be easier to analyse the malware functions. Also, after analysing the malware features in the malware datacentre, it is high likely to increase the accuracy and efficiency of malware detection.

For check the CB-MDEE model, the experiment has been implemented and the result has been released in the diagrams below. In this experiment, 1145 samples are discovered and 1081 of software are utilised for feature detection and extraction. In addition, the CB-MDEE model of detection accuracy is 92.5% and the malware family classification accuracy is 94.6%, which is a decent result.



[5]

# Summary

To sum up, in this essay, the application and concept of Blockchain has been demonstrated. And the security challenge in Blockchain technology still needs to be solved. Especially the process of Blockchain malware detection in Android system. Also, how CB-MMDE model discover and classify malwares in Android mobile devices has been explained. And the process of building malware features datacentre has been mentioned. Moreover, the result of experiment of verifying CB-MMDE model released that the model of CB-MMDE can detect malware more effective and classify detected malware more accurately. In the future, this model is high likely adopted in the worldwide Blockchain malware detection based on Android system. And the security problem of Blockchain will be alleviated. People will pay more trust on the decentralised product of Blockchain technology in the coming future.

# Reference

[1] R.Uncheck(2017), *Mobile malware evolution 2016* [website].

Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8290934>

[2]Niyaz,Q.,Sun,W.,Javaid,A.Y. and Alam,M.(2015), *A deep learning approach for network intrusion detection system*.[online].

Available: <https://arxiv.org/pdf/1711.01353.pdf>

[3]J.Burket,L.Flynn,W.Klieber,J.Lim,W.shen,and W.Snavely(2017) *making didfail succeed: enhancing the CERT static taint analyser for Android app sets*.[website]

Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8290934>

[4]Z.ZHENG, S.XIE,H. DAI, AND H. WANG, an overview of blockchain technology: architecture, consensus, and future trends. [website]

Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8290934&tag=1>

[5]Jing. Gu, BIN. SUN, XIAO. DU, JUN. W, YI.Z, and ZI. W.(2017) Consortium Blockchain-based Malware detection in Mobile Devices.

Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8290934&tag=1>