1.INTRODUCTION

Malware or Malicious Software is a software that can infiltrate the operating system so that it can damage the system and also steal important files on the system [1], [2]. Malware includes Computer Viruses, Trojan Horses, spyware, dishonest adware, crimeware, and other malicious and unwanted software. [3]–[5] New malware continues to emerge as technology evolves, both in terms of platform and operating system by exploiting security loopholes and user negligence. This has left more and more parties harmed. Malware can infect all types of operating systems [6]–[9].

The android system is an operating system based on linux for mobile phones, such as smartphones and tablet PCs [9]–[12]. The Android system has some advantages, such as an open source operating system, multitasking, and the ease of notifications to the number of applications or software that can be detected using the Android system [3]. The evolution of Android devices and apps has rapidly changed us in our daily lives. Web browsing, social media, and internet banking are the examples of Android services using an internet connection and multiple access permissions [13]. Therefore, Android devices have played an important role and become an important part of human life. Therefore, there are several negative impacts of using Android devices, one of which is cyber crime. Its crime is committed by using a computer or other means of communication to inflict fear and anxiety on people or damage, harm, and destroy property. Cybercrime has two categories: computer-aided and computer-focused cybercrime. Some examples of computer-aided cybercrimes are child pornography, fraud, money laundering, and cyberbullying. Meanwhile, the examples of computer-focused cybercrime are hacking, phishing, and website destruction [14]–[17].

The topics and limitations of the problems used in the final project research included how to implement the Reverse Engineering methods to obtain information (System Call) contained in the Remote Access Trojan malware. The operating system used only the Android operating system with a dataset in the form of 40 types of Android Remote Access Trojan malware and 40 Android applications. Summary of releated research can be seen in Table 1.

Table 1. Summary of Related Research

No	Heading	Author / Year	Research Results	Excess	Deficiency
1	The Use of Machine Learning Techniques to Advance the Detection and Classification of Unknown Malware	Shhadat et al. (2020) [18]	Analyzed many machine learning algorithms in malware detection and classification. Implemented various models for malware detection and classification using the implementation provided by sklearn, namely: K-nearest Neighbors (KNN), Support Vector Machine (SVM), Bernoulli Naıve Bayes (Bernoulli NB), J48 Decision Tree (DT), Random Forest (RF), Logistic Regression (LR), and Hard Voting	For very high accuracy results in all binaries and multi-classifiers.	The datasets used is less vary with unbalanced compariso ns.

			(HV). On certain classification algorithms used LG, SVM, Bernoulli NB and DT.		
2	Android Malware Detection using Feature Selections and Random Forest	Eom et al. (2018) [19]	Used the Random Forest method to detect Android malware. The accuracy results obtained a high value. To demonstrate an approach to detection accuracy. This study calculated OOB (Out-of-Bag) errors using detection metrics, including false positives and false negatives.	In the experiments carried out, the results of accuracy were above average.	Uneven distributi on of features to conduct research trials.
3	Android Malware Detection using Feature Selections and Random Forest	Bhatia et al. n.d. (2017) [20]	Dynamic analysis of malware used system call (syscall) analysis that could be used efficiently to classify unknown applications as malicious or not. This research serves to detect and monitor the behavior of malicious applications that use complex incognito techniques.	The dataset used in this study was balanced in number and had high accuracy results.	How to get system call (syscall) data is done one by one manually
4	Mobile Malware Attacks: Review, Taxonomy & Future Directions	Qamar et al. (2019) [21]	A review of smartphone malware attacks, vulnerabilities, detection techniques, and security solutions on Android.	There are guidelines to reduce or even avoid the harmful effects of intruders and hackers.	There are guidelines to reduce or even avoid the harmful effects of intruders and hackers .
5	A Taxonomy on Recent Mobile Malware: Features, Analysis Methods, and Detection Techniques	Alimardan i et al. (2018) [7]	A review of mobile malware (features, methods of analysis and detection techniques).	Learn related data sets (features, analysis methods, and detection techniques) that are acceptable and reserved	Dataset retrieval was only based on common parameters (trusted and often used).

				for researchers.	
6	Malware Detection: A Framework for Reverse Engineered Android Applications through Machine Learning Algorithms	Urooj et al. (2022) [22]	Using Android reverse engineering application features and machine learning algorithms to find vulnerabilities that exist in Android applications.Analysis used to detect malicious Android applications using static analysis.	Using a model that combines a more innovative static feature set with a malware sample dataset. Using ensemble learning with Machine Learning algorithms namely, AdaBoost, Support Vector Machine (SVM), etc.	It is only limited to static analysis and has slow processing techniques that cause this research to produce less accurate results.
7	Analysis, Detection, and Classification of Android Malware through System Calls	Shakya et al. n.d. (2022) [23]	The results of K-Nearest Neighbor and Decision Tree modeling provide the highest accuracy in malware detection and Family Classification, respectively.	The process for analyzing was carried out by static analysis methods.	The malware datasets used did not vary and did not have a numerous number or limited.
8	Mobile Malware Detection Techniques using System Calls	Aranitasi et al. (2022) [6]	Recognized the abnormal behavior of the Android operating system due to malware attacks based on system call identification (syscall).	Using mathematical methods to perform system analysis call (syscall).	There was no validation between the method and the consumed dataset.
9	Mobile Malware Detection Techniques using System Calls	Rashmitha et al. n.d. (2022) [24]	The reverse engineering used successfully found system vulnerabilities, researched malware, and analyzed the complexity of software algorithms serves to protect data hacking.	The characteristics of the resulting malware are quite complete and informative.	The analysis only used static analysis and time-consuming research which was quite a long time.
10	Mobile Malware Detection	Anupama et al.	Used Support Vector Machine (SVM)	The analysis features used	The malware datasets did

	Techniques using System Calls	(2022) [25]	models for static analysis features and Random Forest models for dynamic analysis features. Models used for dynamic analysis features are vulnerable to attacks, but they showed higher resilience than classifiers created based on static analysis features.	were more than one, there were dynamic analysis and hybdrid analysis.	not vary and did not have large or limited numbers.

In this study, the researcher conducted an analysis of malware detection, particularly Remote Access Trojan malware on the Android operating system. The dataset used by the researcher is 40 types of Android Remote Access Trojans malware and 40 Android applications. The researcher used the Reverse Engineering method with dynamic testing. This method was used because it could work very detailed and was used to extract information data contained in malware. In addition, the use of the Reverse Engineering method is also useful for discovering the technological principles of a device, object, or system from the analysis of its structure, function, and operation that is commonly used for maintenance or creating new programs equally without copying anything from the original. The information data used is a type of System Call (Syscall) in every malware and application used as a dataset.