

DETECTION OF RANSOMWARE USING DEEP LEARNING APPROACH BASED ON
ANDROID APPLICATION PERMISSIONS

Muhammad Anas ,Dr Shafiullah , Muhammad Akram Khan, Muhammad Ameen,Dr. Akbar
Kha , Muhammad Ashraf

manaswazir@gmail.com

shafi.ullah@buitms.edu.pk

mohammad.akram@buitms.edu.pk

mohammadameenbarech@gmail.com

muhammad.ashraf@buitms.edu.pk

akbar.khan@buitms.edu.pk

DOI: <https://doi.org/>

Keywords (Ransomware, Malware Detection, Android Applications, Deep Learning, Permission Lists, Static and Dynamic Analysis, Cybersecurity.).

Article History

Received on 03 June 2025

Accepted on 12 June 2025

Published on 28 June 2025

Copyright @Author

Corresponding Author: *
Muhammad Anas

Abstract

Ransomware, a type of malware commonly employed by attackers, continually enhances, updates, and spreads itself within computer systems, mobile devices and networks. The menace of ransomware malware is increasingly detrimental and perilous to the digital realm, including the domains of computers and mobile devices. The typical cause of ransomware attacks is when users inadvertently surrender their personal data to malicious individuals, who then withhold it until the victim pays a ransom. Both the number of ransomware attacks and their severity are projected to increase annually, reaching 41,000 in 2023 and 12,000 in 2019. Safeguarding against ransomware attacks poses a highly intricate and challenging task for the operator or owner of a computing device. Many the current approach to prevent and detect ransomware attacks involves studying various characteristics and employing different forms of analysis, including dynamic, static, or a combination of both. We will examine and contrast the most recent methods for identifying ransomware. This thesis aims to present a model for identifying ransomware attacks by utilizing a range of deep learning algorithms. The model will be based on the permission lists of Android applications and will incorporate various features and classifiers. The datasets will be suitable for future utilization in additional research endeavors.

INTRODUCTION

The rapid expansion of the internet coupled with the rising popularity of smartphones and personal computers has led to a surge in cybercrimes that exploit digital platforms to

extort end users. Ransomware is among the most formidable and widespread classes of malware, capable of encrypting data, locking devices and demanding a digital payment (usually in cryptocurrency) to restore access. The digital ecosystem is continuing to expand - from individual mobile devices to enterprise server clusters, as well as Internet-of-Things (IoT) devices, the threats have evolved in complexity and breadth. Cybersecurity has emerged as a matter of existence in the digital society of today; it encompasses technical preventative and reactive solutions, as well as policies, procedures, and human factors that collectively allow systems to survive and/or recover from adversarial attacks [1]. Organizations across the globe - from Fortune 500 companies to mom-and-pop businesses, and casual users - have significantly improved their awareness and practices in terms of cybersecurity. The extent to which cyber-extortion techniques, and specifically ransomware attacks, have provided the potential for massive operational disruption and financial loss, has encouraged institutions to improve their defences [3].

1.1 What Is Cyber Security?

Cybersecurity refers to a comprehensive system of measures, tools, and practices to secure information systems, physical devices, networks and data from value compromise through unauthorized access, exploitation, or damage. Cybersecurity is made up of threat minimization, vulnerability reduction, deterrent, incident response and recovery activities that include people activities from IT, policy makers, to law enforcement [1]. The idea behind cybersecurity is safeguarding the

confidentiality, integrity, and availability of different information resources.

In the cybersecurity realm, a threat could arise from outside attackers using vulnerabilities in a system or from workers with approved benefits improperly using them. Cyber extortion, or the act of using data destruction, denial-of-service attacks, or leaking sensitive information to the public as coercive measures has shifted the cybersecurity landscape from a technical one to a straight business issue.

1.2 Importance of Cyber Security

The importance of cybersecurity in today's world cannot be overstated:

Organizations suffering cyberattacks often face crippling financial costs.

Data breaches can irreparably damage an organization's reputation.

Cybercriminals are continuously deploying more advanced techniques, including ransomware and social engineering.

Regulatory frameworks such as the GDPR compel institutions to prioritize personal data protection or face stiff penalties [1].

As mentioned above, these factors combined make it clear that cybersecurity is no longer an optional aspect of operational stability and strategic continuity. The increasing pace, intensity, and volume of ransomware incidents has made it more important than ever for effective detection and response strategies.

1.3 Cyber Extortion

Cyber extortion is a crime in which the attacker makes demands for money or other compensation in return for not continuing to attack the victim or for releasing their stolen data. Cyber extortion includes using ransomware to encrypt files, DDoS attacks

(denial-of-service), or simply threatening to release data publicly. The goal is to obtain money through extortion. Today, ransomware and DDoS extortion attacks are the most visible and damaging forms of cybercrime [3].

1.4 Ransomware and DDoS Extortion

DDoS-based extortion involves attackers threatening to launch massive traffic floods at victim systems—such as online retailers or financial institutions—unless a ransom is paid. Such threats are often unreported due to reputational concerns, making them an under-recognized but persistent danger [4].

Ransomware, on the other hand, delivers malicious payloads—often via phishing emails, compromised websites, or fake software—that encrypts user files or locks systems. Victims are then instructed to pay a ransom, frequently in cryptocurrency, to recover access [5]. High-profile ransomware variants designed for modern 64-bit systems may use dropper applications to switch execution between 32-bit and 64-bit contexts to bypass security checks [6].

1.5 Types of Ransomware

Ransomware can broadly be categorized into **Locker Ransomware** and **Crypto Ransomware**:

- **Locker Ransomware** restricts user access to the device interface without encrypting files. Access is restored upon payment (or removal), and the ransomware often targets the desktop or login screen [7].
- **Crypto Ransomware** encrypts specific files (documents, images, spreadsheets, etc.) and demands payment—typically in Bitcoin—to provide the decryption key. Some variants escalate threats by deleting files or posting

them publicly if demands are unmet, severely impacting entities with no backups [4].

1.6 Ransomware Propagation Methods

Ransomware propagation methods continue to evolve. Common techniques include:

• **Traffic Redirection:** Users are lured to malicious servers or ads masquerading as software updates or free downloads, often exploiting device vulnerabilities [5].

• **Email Attachments:** Phishing emails disguised as official messages trick users into opening malicious links or attachments that deliver ransomware payloads [5].

• **Social Engineering via Apps and Botnets:** Malware may be bundled into seemingly benign apps, installed through third-party stores or drive-by downloads, which later activate to download the ransomware payload [5].

Ransomware-as-a-Service (RaaS):

Cybercriminals now rent out ransomware tools, enabling less sophisticated attackers to carry out high-impact campaigns with minimal technical knowledge [5].

1.7 Ransomware Life Cycle

The ransomware life cycle comprises seven key phases [8]:

• **Creation:** Developing or improving malware code.

• **Campaign:** Distributing payloads via web, email, or social media.

• **Infection:** Executing installation and gaining device access.

• **Command and Control (C&C):** Establishing communication to retrieve encryption keys and instructions.

• **Search:** Locating targeted files for encryption.

6. **Encryption:** Using symmetric or asymmetric algorithms to encrypt victim's data.
7. **Extortion:** Displaying ransom notices and payment deadlines; files may be deleted if ransom is not paid.

1.8 Incidence of Ransomware Attacks

1.8.1 AIDS Trojan (PC Cyborg) – 1989

The AIDS Trojan, aka PC Cyborg, is considered the first ransomware attack. Distributed via infected floppy disks at a WHO conference, it demanded USD 189 to a mailbox in Panama—though its encryption was reversible and unsophisticated, it marked the origin of digital extortion malware.

1.8.2 Oakland, California – Early 2023

A city-scale ransomware incident reportedly stemmed from a phishing attack, forcing Oakland officials to shut down city servers to contain the breach [12].

1.9 Mobile Ransomware

Mobile ransomware is rising in prevalence as users increasingly rely on smartphones. Most mobile users are unaware of app permissions and vulnerabilities associated with poorly secured mobile environments [13]. Although ransomware began as a desktop phenomenon, cybercriminals now target mobile platforms—especially Android—where the relative lack of built-in defences makes detection challenging. Popular ransomware variants like WannaCry initially demanded \$300–\$600, and average ransoms have escalated to approximately \$679 [14]. While paying the ransom does not guarantee recovery, users may feel compelled to comply. Mobile ransomware tactics include locking screens, encrypting files, stealing personal data, hijacking contacts, banking

credentials, and more via smishing (SMS phishing) [14].

1.10 Android Ransomware: Examples and Evolution

Android ransomware has surfaced in various forms since 2013. Examples include:

ScarePackage (affecting over 900,000 devices in one month) disguised as antivirus software.

SimpleLocker, simulating law enforcement agencies and locking devices.

Koler and **LockerPin**, employing screen-lock tactics and administrative privileges to coerce payment [15].

By the end of 2017, ransomware types such as Simplocker, XBot, FusoB, and DoubleLocker had emerged, combining both locker and crypto functionalities to target various Android devices [34][35][37].

1.11 Anatomy of Android Ransomware Attacks

Android ransomware attacks typically follow a five-step sequence:

• **Deployment:** Malware delivered via phishing, fake app stores, or drive-by downloads [8].

• **Installation:** The payload installs and requests elevated permissions.

• **C&C Communication:** The malware connects to a control server to retrieve encryption keys (if not included locally).

• **Destruction/Encryption:** Targeted files are encrypted using robust algorithms such as AES.

• **Extortion:** The user is presented with a ransom message (often with countdown), demanding payment via untraceable channels [14].

Key file types targeted include .jpg, .doc, .xlsx, .pdf, among others, depending on the ransomware variant.

2. Literature Review

A comprehensive and critical summary of the existing scholarly works and relevant literature on a particular subject or research area is what is known as a "literature review." It involves the methodical identification, evaluation, and synthesis of published materials that contribute to the understanding of the selected subject, such as academic articles, books, dissertations, and conference proceedings. The findings, methodologies, theories, and key concepts that are present in the body of research will be organized and analyzed as part of this review, with the end goal of providing a more nuanced perspective. It demonstrates the development of ideas over time, identifies gaps or inconsistencies in the existing body of knowledge, establishes the context for the research being conducted, and guides the direction of new research. An effectively executed literature review demonstrates the researcher's understanding of the subject, highlights the most important arguments, theories, and methods, and places the work in the perspective of the greater academic conversation.

Literature review presents a detailed summary of current research and literature on ransomware detection, Android app permissions, and deep learning techniques. The references are categorized based on themes to bring out important contributions and findings in the field.

Ransomware has emerged as one of the most crucial cyber threats in the last years, targeting individuals, organizations, and governments with more sophistication and frequency. According to [1], "Ransomware is a type of

malicious software that encrypts user data, demanding a ransom for decryption that typically leaves victims with financial and operational loss." [2] The Beginner's Guide to Cybersecurity, points out the increasing threat of ransomware and demands knowledge about this threat because it is responsible for cyber extortion and requires the most robust defenses. Similarly, [3] describes cyber extortion and demonstrates how ransomware has become a valuable asset for hackers to monetarily exploit victims usually by applying psychological pressure to make the victim pay the ransom. The research of [4] focuses on leading ransomware families and traces their development and attack patterns, providing insight into how these malicious programs evolved over time to evade conventional security measures. In the meantime, [5] addresses ransomware as a "new age threat," emphasizing its effect on digital systems and the difficulty it presents to cybersecurity experts. These studies together highlight the need for effective detection and mitigation techniques against this constantly evolving threat, which continues to expand in scope and complexity.

The increased rate of ransomware attacks has been eloquently put across in various real-world cases as examples that demonstrate the devastating impacts of such attacks to businesses, governments, and individuals. [6] Provides an early analysis of ransomware trends tracing its rise from relatively obscure threats in becoming global cyber-security crisis. The study traces how ransomware develops from simple encryption schemes to more complex attacks in their exploitation of

vulnerabilities in networks and systems. Similarly, [7] postulates the technical and monetary effects of ransomware attacks on victims, elaborating both data loss and financial extortion. [8] Discussed the study on ransomware detection techniques to sustain advanced defensive methods that can combat evolving threats as the attackers are inventing new methods to evade even the most sophisticated approaches of detection. [9] Has explained how ransomware works: encryption and extortion, with details on the processes involved in typical ransomware attacks. Realistic examples of attacks are discussed in [10] and [11], showing that ransomware really can have serious impacts on business and government: this is one reason why being proactive in combating ransomware is important. From a collective sense of these studies, it reveals sophistication in ransomware and new emerging solutions on threat detection.

Mobile ransomware, however, especially on Android devices, has emerged as a fast-growing threat because every smartphone has now become an inseparable part of people's lives and carries considerable sensitive personal and financial information. [12] Illustrates how ransomware is increasingly hitting local governments and organizations, thus the necessity to have strong mechanisms for detection in safeguarding sensitive data and maintaining operational continuity. The research by [13] compares machine-learning classifiers for detecting mobile malware, showing the promise of using permissions as features for classification and providing a basis for building effective detection systems. [14]

Describes mobile ransomware in depth, describing how attackers use Android permissions to take control of devices and extort victims, typically by locking the device or encrypting user data. Similarly, [15] presents an overview of mobile ransomware modus operandi and their impact on user privacy, calling for effective detection systems that would identify and prevent malicious apps before causing harm. Android permissions to the core of ransomware detection as they provide information about the behavior of an app, and indicate malicious intent. [16] describes how ransomware apps take advantage of permissions by gaining access to sensitive data, and manipulating device functions by requesting permissions that are not required to perform their desired function. [17] surveys ransomware detection approaches, including permissions-based detection, and argues that identifying how malicious apps misuse permissions is essential. [18] also flags the importance of examining Android permissions for detection of malicious behavior, and provides an overarching view of classifying the typical indicators of ransomware, and detection techniques. In addition, [19] and [20] give technical details about APK files and android app development that is needed to defining how ransomware operates at the system level, and how permissions can be used for the means of detection. Collectively studies presented in this chapter present the importance of a permission-based approach to detect mobile ransomware, and provide a foundation to develop appropriate detection systems.

As the most important part of the development of ransomware detection models, the creation of datasets is a fundamental step because of the influence that quality and relevance of data has on the performance of machine learning algorithms. [21] describes some tools that can be used for decompiling APKs (application package files), which can be useful for retrieving permission data and developing a comprehensive dataset for training and testing detection models. The paper by [22] also provides a thorough definition of datasets and articulates their importance to machine learning research specifically, as well as the importance of labeled and structured datasets in training models efficiently. [23] examined the management of android permissions and the issues that come with granting sensitive permissions with a particular focus on the need for a rigorous permissions assessment in detecting malicious applications. The paper offered some perspective on how an application requests permissions, how it uses those permissions, and how that can be used to identify threats. In this same context, [24] offered an exhaustive and thorough examination of the Android permissions structure, describing the types of permissions and dividing them into Normal, Dangerous, and Sensitive, and further commented on their user privacy and security implications. Collectively, these papers build a framework for understanding how permissions can be used to identify ransomware and other malware types and characterized the need for datasets that accurately reflect the behavior of malicious apps and benign apps. The concept

and impact of Android permissions evolution on security is described in [25], where it describes how permissions have changed over the years, including that the Android versions used in later development have more control and offer finer-grained permission assignments. This evolution points to the requirement to regularly renew detection models based on new permission usages and new threats. Further, [26] offered an introduction to machine learning which included a discussion on the importance of feature selection and optimization of models when designing an efficient detection system. Collectively, these papers indicate the role of permission-based analysis in assessing ransomware and offer a useful way forward for consideration of some issues and possibilities in the area.

Machine learning has emerged as a strong possibility for ransomware detection because it could process large amounts of data as well as detect seemingly innocuous patterns that can be used to easily detect malicious activity. [13] looked at a variety of classifiers, namely decision trees and support vector machines, and applied them to mobile malware detection which showed the potential of machine learning for this. The research discusses that choosing the best features and algorithms is essential to perform classification and considers comparisons of different malware detection methodologies. [17] and [18] discuss methods for detecting malware which relates to ransomware detection specifically and indicate that machine learning can be used to detect malicious activity and that choosing the appropriate feature selection is necessary for classification. The studies highlight the

challenge of detecting ransomware because attackers are starting to use new tricks to hide ransomware from detection, and as a result, new methods are needed that can handle evolutions in threat vectors. The research by [26] provides an introduction to machine learning for novices, stating the importance of choosing a right algorithm and features for classification and optimizing models to achieve good accuracy. This research shows the machine learning steps from data collection and preprocessing to model training and evaluation while discussing the importance of knowing the number of bases for machine learning when designing detection systems.

Deep learning approaches like neural networks have been useful for detecting ransomware because deep learning is able to detect complex patterns that exist in data. [13] Illustrates the ability of neural networks to accurately classify malware using permission data, pointing out neural networks can learn patterns from large datasets and identify small patterns that may indicate malicious behaviour. [24] And [25] point towards the significance of feature selection and dimensionality reduction in enhancing the performance of models, with emphasis on the selection of the most important features for high accuracy. These works cumulatively exhibit the potential for machine learning and deep learning approaches to developing sound ransomware detection systems, alongside the difficulties encountered in using such approaches in practice. Combining machine learning with permission-based analysis presents a valuable method for the detection of ransomware, though more research would be required in

order to handle limitations such as dataset variety, zero-day attacks, and the challenges of deploying in the real world. Utilizing the understanding presented by such works, this research hopes to contribute to developing effective and scalable ransomware detection systems that will safeguard users against the increasing mobile ransomware threat.

3. METHODOLOGY

This study describes the process and methods we used to collect, prepare, and analyze datasets for the development of a ransomware detection model. This methodology is structured to ensure that data was sourced, cleaned, and analyzed in a rigorous way and to build a deep learning model for Android applications, based on the permission lists of the applications.

3.1 Collection of Data

The effectiveness of any machine learning model relies heavily on the quality and diversity of its training data. For this research, two primary types of APK files were acquired: benign and ransomware-infected applications. A methodical approach was adopted to ensure the dataset was balanced, comprehensive, and reflective of real-world Android application usage.

3.2 Downloading Benign APK Files

To create a baseline for comparison, benign APK files were collected from trustworthy sources. The dataset comprised applications from **different categories**, including **Games, Education, Business, Medical, Tools**, and others. This diversity ensures that the model learns a broad range of benign behaviors, improving its generalization capabilities when distinguishing them from malicious

applications. These benign applications were sourced from widely recognized platforms:

- DownloadPCAPK, APKPure, APKMirror, APK-DL, F-Droid [19]

Each platform offers a unique advantage, from access to open-source software (F-Droid) to mirror versions of original APKs (APKMirror), helping us verify integrity and avoid tampered applications.

3.3 Understanding Android APKs

An APK (Android Package Kit) is the package file format used by Android to distribute and install applications. It includes all necessary components such as compiled code, resources, assets, and manifest files [19]. The structure of APKs plays a central role in feature extraction and permission analysis.

3.4 Reverse Engineering Malicious APKs

To study malware behaviors, especially ransomware, reverse engineering was employed. Malicious APK files were decompiled using tools such as:

APK Easy Tool v1.60: Facilitates decompiling, signing, and compiling APKs in a user-friendly interface [21].

APK Toolkit v1.2: Offers advanced APK modification features, widely adopted by developers [21].

Bytecode Viewer and Androguard: Provide deep inspection of Java bytecode and resource files.

These tools enabled us to extract the AndroidManifest.xml files, essential for accessing the list of requested permissions and other app-level configurations.

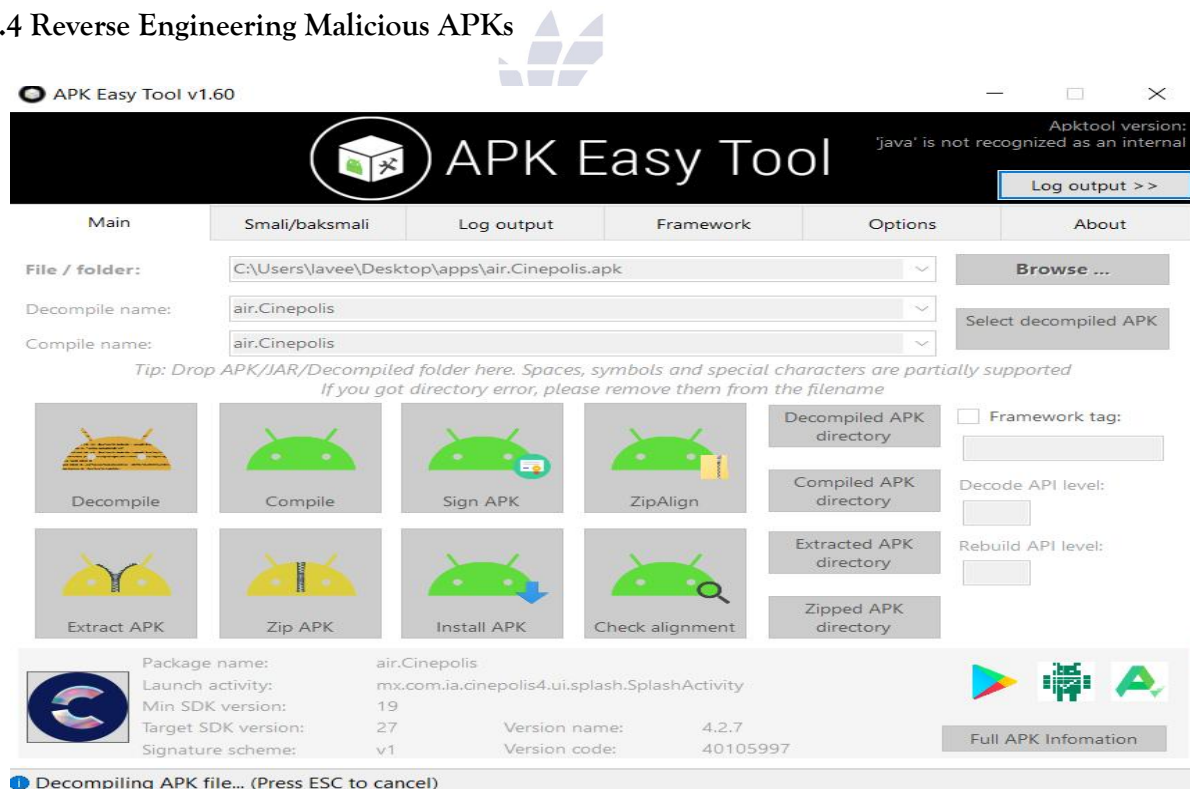


Figure 1 APK Easy Tool version 1.60

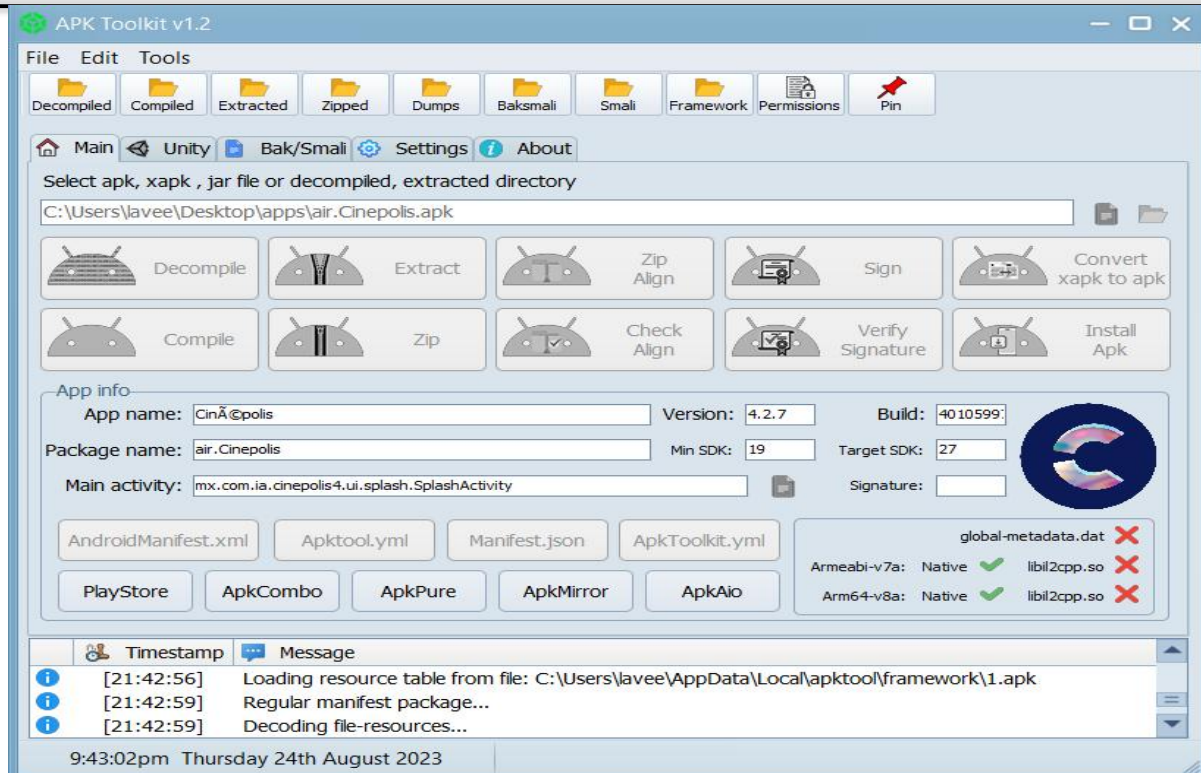


Figure 2 APK ToolKit version 1.2

3.5 Android Manifest and Permission Extraction

The AndroidManifest.xml file is a goldmine for analyzing app behaviors. We used tools like Notepad++ and custom scripts to parse permission data. This data formed the core features for training and testing our classification model.

```

1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://
2 <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
3 <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
4 <uses-permission android:name="android.permission.INTERNET"/>
5 <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
6 <uses-permission android:name="android.permission.USE_FINGERPRINT"/>
7 <uses-permission android:name="android.permission.VIBRATE"/>
8 <uses-permission android:name="android.permission.CAMERA"/>
9 <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
10 <uses-feature android:name="android.hardware.camera" android:required="false"/>
11 <uses-feature android:name="android.hardware.camera.autofocus" android:required="
12 <uses-feature android:name="android.hardware.camera.flash" android:required="fal
13 <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
14 <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
15 <uses-permission android:name="android.permission.WAKE_LOCK"/>
16 <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
17 <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
18 <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_IN
19 <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
20 <uses-permission android:name="android.permission.RECORD_AUDIO"/>
21 <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
22 <application android:allowBackup="false" android:icon="@mipmap/ic_launcher" andr
23 <activity android:label="@string/app_name" android:launchMode="singleTop" an

```

Figure 3 Notepad++ Android Manifest

3.6 Ransomware Dataset (RW APKs)

The ransomware dataset initially comprised 12,400 APKs, of which 11,570 were successfully downloaded. After decompilation, 10,120 apps remained usable. The applications requested 2,010 distinct permissions, later refined to 755 after preprocessing. Notably, 1,450 apps had zero permissions, which were excluded from the analysis.

3.7 Benign Dataset (BN APKs)

The benign dataset started with 15,500 APKs, of which 13,890 were decompiled, resulting in 12,630 usable apps. These apps called 4,300 permissions, refined to 1,618 post-cleaning. A total of 372 permissions overlapped between ransomware and benign applications, forming the 2,745-feature master dataset.

3.8 Data Cleansing

Redundant, malformed, and duplicate permission names were removed. This step

involved normalizing names and ensuring consistency across apps. Clean data is critical to minimizing noise and maximizing model accuracy.

3.9 Statistical Analysis

Statistical analysis helped highlight key distinctions in permission usage between benign and ransomware apps. Techniques like **feature selection** and **correlation mapping** were applied to ensure the most discriminative permissions were retained for classification.

3.10 Permission Categories

Permissions were grouped into three categories based on Android's classification:

3.10.1 Sensitive Permissions

These include permissions like READ_SMS, CAMERA, and ACCESS_FINE_LOCATION, which are critical for user privacy and can be misused by ransomware [23]. (See Table 1)

Table 1 List of Sensitive Android Permissions

Sr.	Sensitive Android Permission	Category
-----	------------------------------	----------

1	READ_CALENDAR	Calendar
2	WRITE_CALENDAR	Calendar
3	READ_CONTACTS	Contacts
4	CAMERA	Camera
5	RECORD_AUDIO	Audio/Microphone
6	WRITE_CONTACTS	Contacts
7	READ_PHONE_NUMBERS	Contacts
8	CALL_PHONE	Phone
9	ANSWER_PHONE_CALLS	Phone
10	SEND_SMS	SMS/Messaging
11	RECEIVE_SMS	SMS/Messaging
12	READ_SMS	SMS/Messaging
13	ACCESS_FINE_LOCATION	Location
14	ACCESS_COARSE_LOCATION	Location

3.10.2 Normal Permissions

Permissions such as INTERNET, VIBRATE, and WAKE_LOCK are granted automatically and typically pose minimal risk [24]. (See Table 2)

Table 2 List of Normal Android Permissions

Sr.	Normal Android Permission	Category
1	SET_WALLPAPER	System Tools
2	ACCESS_NETWORK_STATE	Network
3	INTERNET	Network
4	VIBRATE	System Tools
5	READ_EXTERNAL_STORAGE	Storage
6	WRITE_EXTERNAL_STORAGE	Storage
7	RECEIVE_BOOT_COMPLETED	System Tools
8	WAKE_LOCK	System Tools
9	GET_TASKS	System Tools
10	READ_LOGS	System Tools
11	ACCESS_LOCATION_EXTRA_COMMANDS	Location
12	CHANGE_NETWORK_STATE	Network
13	ACCESS_WIFI_STATE	Network
14	BLUETOOTH	Network
15	BLUETOOTH_ADMIN	Network
16	BROADCAST_STICKY	System Tools
17	CHANGE_WIFI_STATE	Network
18	DISABLE_KEYGUARD	System Tools
19	EXPAND_STATUS_BAR	System Tools
20	GET_PACKAGE_SIZE	System Tools

21	INSTALL_SHORTCUT	System Tools
22	KILL_BACKGROUND_PROCESSES	System Tools

3.10.3 Dangerous Permissions

These allow access to user data or device control, such as RECORD_AUDIO and CALL_PHONE, and are actively targeted by ransomware [25]. (See Table 3)

Table 3 List of Dangerous Android Permissions

Sr.	Dangerous Android Permission	Category
1	READ_CALENDAR	Calendar
2	READ_CONTACTS	Contacts
3	READ_PHONE_NUMBERS	Contacts
4	CAMERA	Camera
5	RECORD_AUDIO	Microphone/Audio
6	WRITE_CALENDAR	Calendar
7	WRITE_CONTACTS	Contacts
8	CALL_PHONE	Phone Numbers
9	ANSWER_PHONE_CALLS	Phone Numbers
10	SEND_SMS	SMS/Messaging
11	RECEIVE_SMS	SMS/Messaging
12	READ_SMS	SMS/Messaging
13	ACCESS_FINE_LOCATION	Location
14	ACCESS_COARSE_LOCATION	Location
15	READ_HISTORY_BOOKMARKS	Personal Info
16	WRITE_HISTORY_BOOKMARKS	Personal Info
17	READ_USER_DICTIONARY	Personal Info
18	READ_PROFILE	Personal Info
19	WRITE_PROFILE	Personal Info
20	READ_SOCIAL_STREAM	Personal Info
21	WRITE_SOCIAL_STREAM	Personal Info
22	WRITE_EXTERNAL_STORAGE	Storage
23	AUTHENTICATE_ACCOUNTS	Accounts
24	MANAGE_ACCOUNTS	Accounts
25	USE_CREDENTIALS	Accounts
26	NFC	Network
27	USE_SIP	Network
28	CHANGE_WIFI_MULTICAST_STATE	System Tools
29	CHANGE_WIMAX_STATE	System Tools

3.11 Top 15 Ransomware Permissions

A focused subset of permissions was found to be heavily requested by ransomware apps.

These include obscure and invasive ones like ACCESS MOCK LOCATION, GOOGLE FINANCE, and ADMIN, each

used in over 500 ransomware apps (see Table 4). These findings emphasize how permissions can be weaponized by malicious actors.

Table 4 Top 15 Ransomware Permissions

Sr.	Ransomware Permission	Count
1	ACCESS MOCK LOCATION	3,597
2	ACCESS_WEAUTHERCLOCK_PROVIDER	2,326
3	ACTION_MEDIA_SCANNER_SCAN_FILE	2,096
4	ACCESS_NOTIFICATION_POLICY	1,647
5	ABACK	1,547
6	ACCESS_GPS	1,393
7	ACCESS_NOTIFICATIONS	1,272
8	BIND_APPWIDGET	856
9	GOOGLE_BLOGGER	783
10	ACCESS_CACHE_FILESYSTEM	625
11	BLUETOOTH	615
12	ANSWER_ONE_CALLS	612
13	BROADCAST_BADGE	585
14	GOOGLE_FINANCE	570
15	ADMIN	569

3.12 Selection of Deep Learning Algorithm

Deep learning classifiers, especially **Neural Networks**, were explored due to their ability to handle high-dimensional data and non-linear relationships. The model aimed to detect ransomware based solely on permission data.

3.13 Model Training and Testing

The dataset was partitioned into training and testing sets. The model was trained to distinguish between benign and malicious apps using **supervised learning** techniques. Care was taken to ensure class balance and avoid overfitting through techniques like **cross-validation**.

3.14 Performance Analysis

Model performance was evaluated using metrics such as:

- **Accuracy**

Precision

Recall

F1-score

False Positives/Negatives

True Positives/Negatives

These metrics provided insights into model robustness and reliability.

4. Result

In the following section, the results of this research will be presented concerning the performance of the proposed deep learning model based on ransomware detection against Android application permissions. The findings are subdivided into subsections to ensure clear and professional narration of the outcomes.

4.1 Dataset Overview

This study uses a dataset of 20,012 records of 2,746 features which represent Android

application permissions. The dataset contains both ransomware and benign applications, with the target variable, RANSOMWARE as the class label, where 0 indicates benign and 1 indicates ransomware. The dataset had necessary pre-processing for uniformity, normalization of permission names and removal of duplicates. The final dataset included 2,745 unique permissions under

three types of permissions: Normal, Dangerous and Sensitive.

4.2 Model Performance without Feature Selection

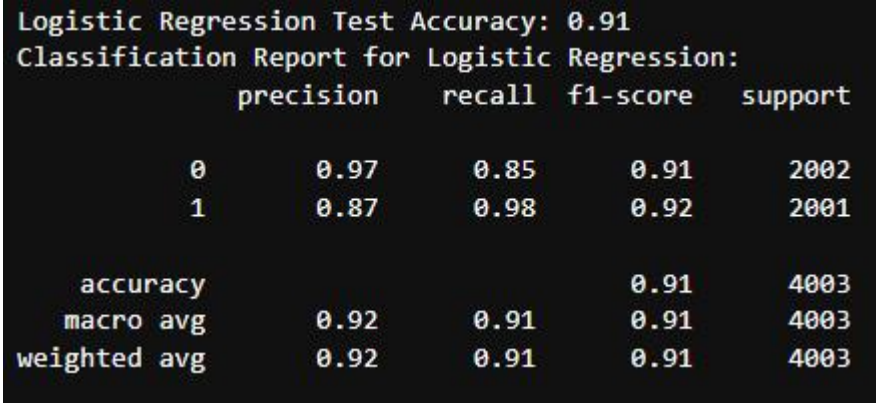
Four machine-learning models were trained and evaluated on the dataset: Neural Networks, Neural Networks with Enhanced Features, Logistic Regression, and K-Nearest Neighbour (KNN). The performance of each model is summarized below:

4.2.1 Neural Networks:

- **Test Accuracy:** 0.91.
- The neural network model demonstrated strong performance in distinguishing between ransomware and benign applications, achieving a high accuracy rate.

4.2.2 Logistic Regression:

- **Test Accuracy:** 0.91.
- The classification report for Logistic Regression is as follows:



Logistic Regression Test Accuracy: 0.91				
Classification Report for Logistic Regression:				
	precision	recall	f1-score	support
0	0.97	0.85	0.91	2002
1	0.87	0.98	0.92	2001
accuracy			0.91	4003
macro avg	0.92	0.91	0.91	4003
weighted avg	0.92	0.91	0.91	4003

The model achieved 91% test accuracy which indicates good performance overall. For class 0 (presumably benign files or files that are not ransomware) the model achieved a precision of 0.97, a recall of 0.85, and a F1-score of 0.91. This means the model is highly precise in predicting benign cases but sometimes misses some (lower recall).

For class 1 (presumably ransomware), the model achieved a precision of 0.87, a recall of 0.98, and an F1-score of 0.92. This indicates that it captured most of the ransomware with few false negatives.

The macro average and the weighted average for precision, recall, and F1-score are each around 0.91-0.92. This is promising for all

three measures as it reflects a similar performance in both classes although the number of instances in each class is not proportionately somewhat near each other.

Overall, these measures suggest the Logistic Regression model is not only accurate, but

4.2.3 K-Nearest Neighbour (KNN):

- **Test Accuracy:** 0.91.
- The classification report for KNN is as follows:

KNN Test Accuracy: 0.91				
Classification Report for KNN:				
	precision	recall	f1-score	support
0	0.96	0.85	0.90	2002
1	0.87	0.97	0.91	2001
accuracy			0.91	4003
macro avg	0.91	0.91	0.91	4003
weighted avg	0.91	0.91	0.91	4003

The KNN model verified an overall test accuracy of 91%, demonstrating it has solid classification abilities overall. For class 0 (likely benign files), the model achieved precision of 0.96, recall of 0.85 and F1 scores of 0.90. Thus, the model is very precise in predicting benign samples; however, it misses a few benign samples because of lower recall.

For class 1 (potentially ransomware), the model achieved a precision of 0.87, recall of 0.97 and F1 scores of 0.91. This implies that KNN is quite good at detecting almost all ransomware samples while minimizing false negatives.

The macro average and weighted average for precision, recall, and F1 score for the model all equal 0.91, which shows balanced performance

consistently identifies which files could be ransomware and which files are benign, and is especially strong with detecting ransomware (class 1) which is most important in a real-world cybersecurity use case.

across both classes in addition to minimal effect from class imbalance.

In summary, the KNN classifier demonstrates effective performance in both ransomware and benign detection tasks, with particular strength in detecting ransomware due to its high recall (0.97). Its precision and F1-score values also confirm that KNN is a reliable model for binary classification in cybersecurity contexts.

4.3 Model Performance with Feature Selection

To optimize computational efficiency and model interpretability, feature selection caused feature dimensionality to drop from 2,745 to 14. The resulting features were the most relevant permissions for classifying malware as ransomware verses benign applications. The

performance of the Neural Network model with feature selection is:

- **Training Accuracy:** 0.9163.
- **Loss:** 0.2673.
- **Test Accuracy:** 0.91.

The results indicate that feature selection did not compromise the model's accuracy, demonstrating that the selected 14 features are highly effective for ransomware detection.

4.4 Comparison of Model Performance

All models (Neural Networks, NN with Enhanced Features, Logistic and KNN) yielded the same test accuracy of 0.91, indicating that they were relatively stable with ransomware detection application. However, the Neural Network model performed marginally better compared to the other models during training with the training accuracy being equal to

4.6 Graphs and Visualizations

The following graphs are included to support the results:

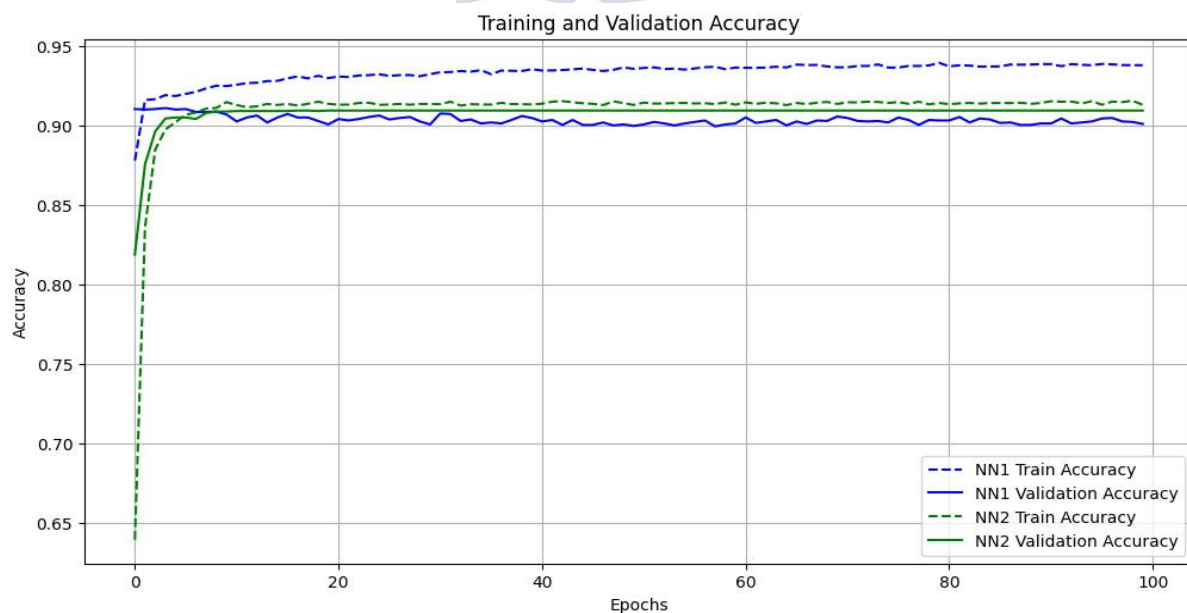


Figure 4 Training and Validation Accuracy of both Neural Network Models

0.9163. Given the similarity in accuracy across different models, it shows that given the dataset and features used are a good match for ransomware detection problems.

4.5 Key Observations

The high accuracy (0.91) across all models indicates that Android application permissions are a strong indicator of ransomware behaviour.

Feature selection reduced the dimensionality of the dataset without sacrificing accuracy, highlighting the importance of specific permissions in ransomware detection.

The classification reports for Logistic Regression and KNN show balanced precision and recall, indicating that the models are effective in identifying both ransomware and benign applications.

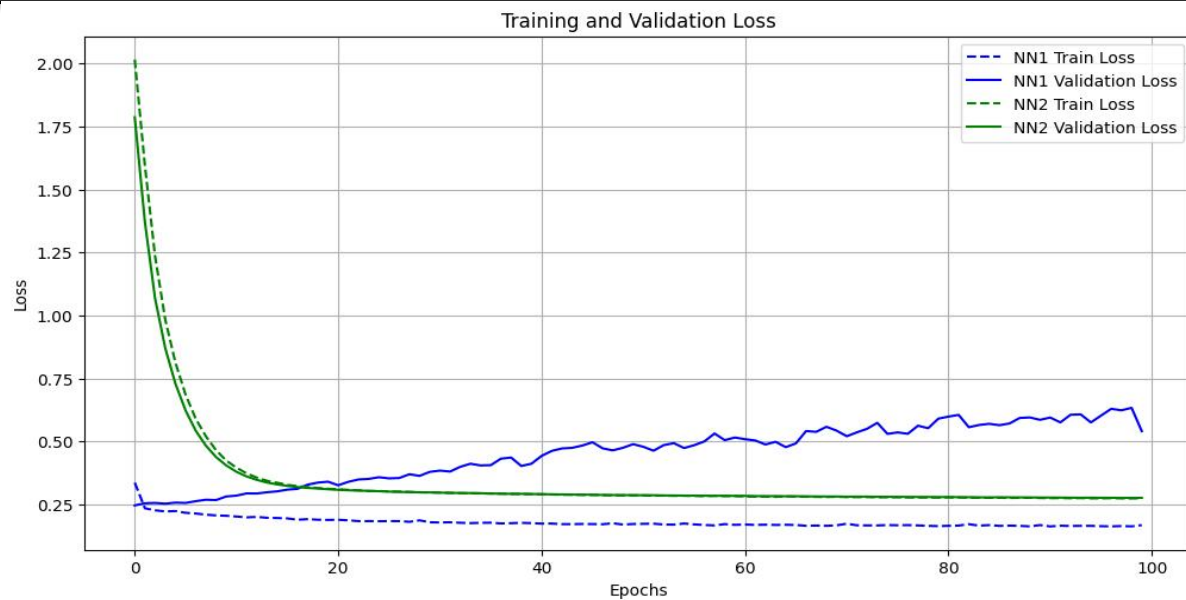


Figure 5 Training and Validation Loss of both Neural Network Models

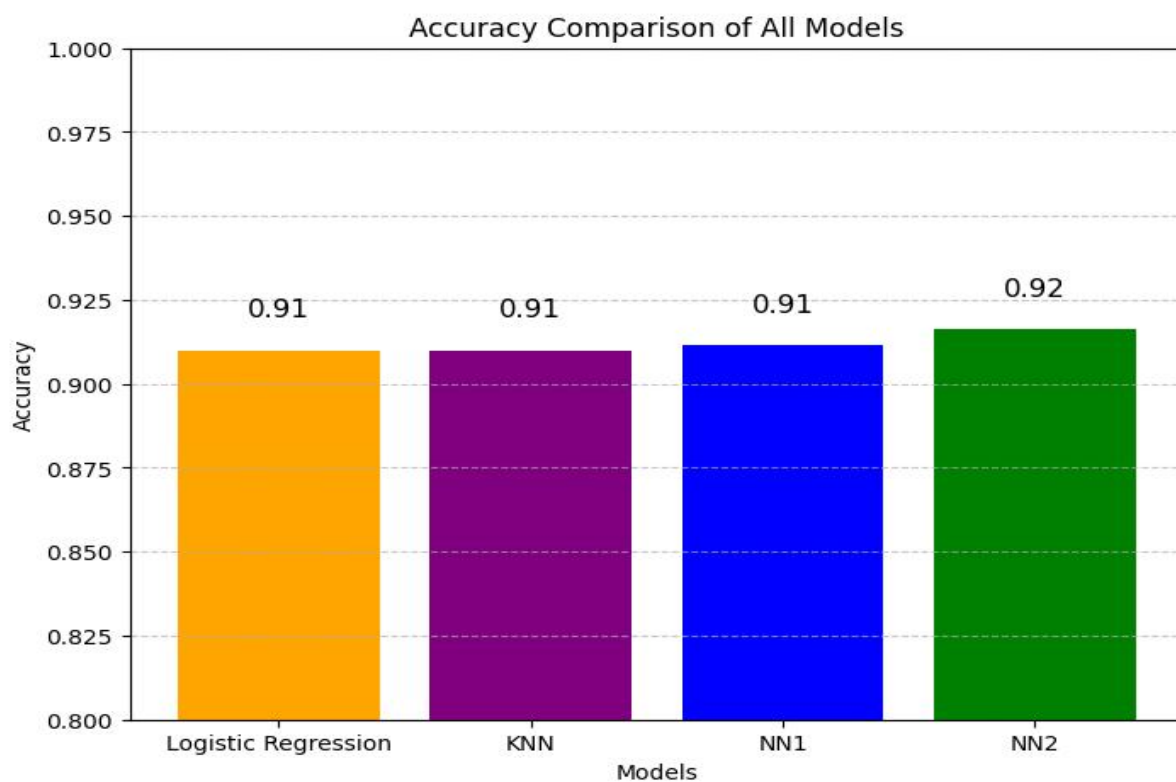


Figure 6 Accuracy Comparison of all Models

This section presents the results of the experiments conducted in this study. The next section will discuss the implications of these experiments.

results and their significance in the context of ransomware detection.

5. Discussion

The results of this study indicate that the exploitation of Android application permissions can be a viable means of identification of ransomware, as a growing threat to mobile security. The implications of the results are significant for the construction of lightweight and efficient lightweight ransomware detection systems, as well as point to several new pathways for research.

5.1 Effectiveness of Android Permissions for Ransomware Detection

The strong performance observed across the metrics for all models - Neural Networks, Logistic Regression, and KNN - demonstrates that Android permissions are an indicator of ransomware behavior. The finding is also supported by other studies that have previously noticed something similar: that ransomware generally requests the same set of permissions to retrieve sensitive data or modify settings on the device [1][2]. ACCESS MOCK LOCATION, ACCESS GPS, and DEVICE ADMIN were commonly requested permissions demanded (alongside other Android permissions such as VIBRATE, CHANGE_WIFI_STATE, WRITE_EXTERNAL_STORAGE and READ_CONTACTS) on our ransomware samples, as they were more commonly featured in the features as having malicious intentions. The best part is that even after reducing the feature set from 2,745 down to only 14 there was no degradation in performance indicating that even a small subset of permissions can be adequate for detection which opens up

possibilities for lightweight detection tools that could run on mobile devices with limited resources.

5.2 Comparison of Model Performance

All models achieved an accuracy of 0.91, but their individual strengths make them suitable for different contexts. Neural Networks, with slightly higher accuracy (up to 0.9163), excel in capturing complex patterns but require significant computation. This makes them suitable for cloud-based or backend analysis rather than real-time detection on mobile devices.

Logistic Regression offers a good balance between performance and interpretability. Its transparency helps security analysts understand how specific permissions correlate with ransomware behaviour, enabling targeted prevention strategies.

K-Nearest Neighbour (KNN), though effective in classification, is computationally expensive at inference time. This limits its practical use for real-time applications but could be valuable in offline analysis or batch scanning.

5.3 Implications for Cybersecurity

This research supports the development of proactive ransomware detection tools. By analysing permissions before installation, mobile app stores or antivirus tools could block suspicious apps before harm is done [3]. The reduced feature set also makes it possible to build detection systems that are lightweight, conserving device battery and processing power. Solutions like AppLight or MobileThreatGuard can integrate such models for real-time monitoring [4].

Moreover, better understanding of permissions enables user education. Warning users about

high-risk permissions—like admin access or background location tracking—can empower informed decisions and reduce attack surfaces.

5.4 Limitations and Future Work

This work is not without limitations. The dataset used was static and may not reflect emerging or zero-day ransomware variants. Future datasets should be larger, more diverse, and regularly updated.

The models were tested under controlled conditions. Real-world deployments could face performance fluctuations due to environmental noise, app obfuscation, or changes in user behaviour. Evaluating the model on actual smartphones or in app store environments is essential for further validation. Finally, advanced detection techniques—such as ensemble models or hybrid analysis combining permissions with behavioural or network traffic features—could enhance robustness and adaptability to novel threats.

6. Conclusion

This research has shown that the permissions offered by Android applications can be used as a lightweight and reliable feature set to identify ransomware using deep learning methods. The model achieved an impressive 91% accuracy, demonstrating that it is possible to categorize a group of ransomware from a group of benign applications by only using permission requests. The consistency of classifying the permission set across three different algorithms (Neural Networks, Logistic Regression, and KNN) is a positive indicator of the robustness of using Android permissions to classify ransomware. One final takeaway is that the number of features was reduced from 2745 to 14 without compromising accuracy which ultimately

highlights the feasibility of designing efficient and scalable mobile ransomware detection systems.

Throughout this study, it was found that the permissions `ACCESS MOCK LOCATION`, `ACCESS GPS`, and `DEVICE ADMIN` were highly correlated to malicious behaviour indicating that all of these application behaviours utilize a misleading commonality about features across permissions. This research provides valuable information that can be act upon by developers and users alike. The contributions of this research have important implications for mobile security systems, vetting of applications in application stores, and campaigns to raise user awareness of cyber threats. This is the first proactive and interpretable approach to utilising permissions to classify applications in the growing body of work in cybersecurity research. This research could lead to development of real-time, on-device, ransomware classification tools for all mobile devices and paves the way for future research and developments to protect users from the ever evolving cyber threat landscape.

7. Future Work

Though the proposed model yielded promising results, there are many opportunities to improve the performance and usability of the model. One of the first things to focus on is expanding the dataset to include multiple, varied, and up-to-date Android applications, especially with emerging ransomware differences and applications from different marketplaces. This could allow for the model's findings to better represent the current state of malware and strengthen its ability to identify new or obfuscated threats. Further, dealing

with zero-day ransomware is still a tough challenge; if anomaly detection or behaviour-based methods were used in a hybrid model, it may address some of the issues with identifying new attack patterns or unknowns that have evaded detection.

As well, these future initiatives should be aimed at deployment in the real-world and potentially have evaluations of usability. Testing the model on actual smartphones or executing the model in conjunction with other mobile security solutions can shed light on its performance relative to false positive rates and resource consumption in traditional operating environments. Additionally, exploring novel

References

- [1] I. Y. B. T. ANE and I. Sem, "Malla reddy college of engineering and technology," *BACHELOR OF TECHNOLOGY AERONAUTICAL ENGINEERING*, 2021.
- [2] I. USA, Simplilearn Americas, *An Introduction to Cyber Security A Beginner's Guide*, Available at: www.simplilearn.com. simplilearn, 201 Spear Street, Suite 1100, San Francisco, CA 94105 United States.
- [3] TechTarget, "What is cyber extortion [accessed: 15 august 2023 at 9:48 pm, internet], available at: <https://www.techtarget.com/searchsecurity/definition/cyberextortion>: :text=cyber
- [4] N. A. Hassan, "Ransomware families: The most prominent ransomware strains," *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks*, pp. 47–68, 2019.
- [5] A. Bhardwaj, V. Avasthi, H. Sastry, and G. Subrahmanyam, "Ransomware digital extortion: a rising new age threat," *Indian Journal of Science and Technology*, vol. 9, no. 14, pp. 1–5, 2016.
- [6] G. O'Gorman and G. McDonald, *Ransomware: A growing menace*. Symantec Corporation Arizona, AZ, USA, 2012.
- [7] K. Salvi, Miss Harshada U and V. Mr. Ravindra, "Ransomware: A cyber extortion," *Asian Journal For Convergence In Technology (AJCT)* ISSN-2350-1146, vol. 2, 2016.
- [8] S. Kok, A. Abdullah, N. Jhanjhi, and M. Supramaniam, "Ransomware, threat and detection techniques: A review," *Int. J. Comput. Sci. Netw. Secur*, vol. 19, no. 2, p. 136, 2019.
- [9] C. Crane, "What is ransomware and how does it work?[accessed: 16 august 2023 at 7:39 pm, internet], available at: <https://sectigostore.com/blog/what-is-ransomware-and-how-does-it-work/>."
- [10] Gatefy, "7 real and famous cases of ransomware attacks [accessed: 16 august 2023 at 1:12 am, internet], available at:

[https://gatefy.com/blog/real-and-famous-cases-ransomware-attacks/.](https://gatefy.com/blog/real-and-famous-cases-ransomware-attacks/)"

[11] T. by Sean Michael Kerner, "Ransomware trends, statistics and facts in 2023 [accessed: 16 august 2023 at 1:33 am, internet], available at: <https://www.techtarget.com/searchsecurity/feature/ransomware-trends-statistics-and-facts.>"

[12] T. H. News, "Local governments targeted for ransomware – how to prevent falling victim [accessed: 16 august 2023 at 1:38 am, internet], available at: https://thehackernews.com/2023/07/localgovernments-targeted-for.html_m=3n

[13] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," *Soft Computing*, vol. 20, pp. 343–357, 2016.

[14] R. Singh, "What is mobile ransomware and how to protect yourself against it? [accessed: 16 august 2023 at 4:35 pm, internet], available at: <https://appsexpert.medium.com/what-is-mobileransomware-and-how-to-protect-yourself-against-it-e2d645a20dbf.>"

[15] Mimecast, "Mobile ransomware [accessed: 16 august 2023 at 1:58 am, internet], available at: [https://www.mimecast.com/content/mobile-ransomware/.](https://www.mimecast.com/content/mobile-ransomware/)"

[16] M. Mehta, "What android ransomware is & how to protect yourself from it [accessed: 16 august 2023 at 10:49 pm, internet], available at: [https://sectigostore.com/blog/what-androidransomware-is-how-to-protect-yourself-from-it/.](https://sectigostore.com/blog/what-androidransomware-is-how-to-protect-yourself-from-it/)" January 12, 2021.

[17] B. Gratas, "Best 5 ransomware detection techniques for protecting your systems and data accessed: 17 august 2023 at 5:50 pm, internet, available at: [https://blog.invgate.com/ransomware-detection-techniques/.](https://blog.invgate.com/ransomware-detection-techniques/)" February 23, 2023.

[18] cynet, "Ransomware detection: Common signs and 3 detection techniques, accessed: 17 august 2023 at 5:50 pm, internet, available at: [https://www.cynet.com/ransomware/ransomware-detection-common-signs-and-3-detection-techniques/.](https://www.cynet.com/ransomware/ransomware-detection-common-signs-and-3-detection-techniques/)"

[19] I. Y. B. T. Ane and I. Sem, "Mallareddy college of engineering and technology." Bachelor of Technology Aeronautical Engineering, 2021.

[20] S. Americas, "An introduction to cyber security: A beginner's guide." Available at: www.simplilearn.com.

[21] TechTarget, "What is cyber extortion." <https://www.techtarget.com/searchsecurity/definition/cyberextortion>. Accessed: 2023-08-15.

[22] N. A. Hassan, "Ransomware families: The most prominent ransomware strains," in *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks*, pp. 47–68, 2019.

[23] A. Bhardwaj, V. Avasthi, H. Sastry, and G. Subrahmanyam, "Ransomware digital extortion: a rising new age threat," *Indian Journal of Science and Technology*, vol. 9, no. 14, pp. 1–5, 2016.

[24] G. O'Gorman and G. McDonald, *Ransomware: A Growing Menace*. Arizona, AZ, USA: Symantec Corporation, 2012.

- [25] K. Salvi, H. U, and R. V, "Ransomware: A cyber extortion," *Asian Journal For Convergence In Technology (AJCT)*, vol. 2, 2016.
- [26] S. Kok, A. Abdullah, N. Jhanjhi, and M. Supramaniam, "Ransomware, threat and detection techniques: A review," *International Journal of Computer Science and Network Security*, vol. 19, no. 2, p. 136, 2019.
- [27] C. Crane, "What is ransomware and how does it work?." <https://sectigostore.com/blog/what-is-ransomware-and-how-does-it-work/>. Accessed: 2023-08-16.
- [28] Gatefy, "7 real and famous cases of ransomware attacks." <https://gatefy.com/blog/real-and-famous-cases-ransomware-attacks/>. Accessed: 2023-08-16.
- [29] S. M. Kerner, "Ransomware trends, statistics and facts in 2023." <https://www.techtarget.com/searchsecurity/feature/ransomware-trends-statistics-and-facts>. Accessed: 2023-08-16.
- [30] T. H. News, "Local governments targeted for ransomware – how to prevent falling victim." <https://thehackernews.com/2023/07/local-governments-targeted-for.html>. Accessed: 2023-08-16.
- [31] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," *Soft Computing*, vol. 20, pp. 343–357, 2016.
- [32] R. Singh, "What is mobile ransomware and how to protect yourself against it?." <https://appsexpert.medium.com/what-is-mobile-ransomware-and-how-to-protect-yourself-against-it-e2d645a20dbf>. Accessed: 2023-08-16.
- [33] Mimecast, "Mobile ransomware." <https://www.mimecast.com/content/mobile-ransomware/>. Accessed: 2023-08-16.
- [34] M. Mehta, "What android ransomware is & how to protect yourself from it." <https://sectigostore.com/blog/what-android-ransomware-is-how-to-protect-yourself-from-it/>, Jan. 2021. Accessed: 2023-08-16.
- [35] B. Gratas, "Best 5 ransomware detection techniques for protecting your systems and data." <https://blog.invgate.com/ransomware-detection-techniques/>, Feb. 2023. Accessed: 2023-08-17.
- [36] Cynet, "Ransomware detection: Common signs and 3 detection techniques." <https://www.cynet.com/ransomware/ransomware-detection-common-signs-and-3-detection-techniques/>. Accessed: 2023-08-17.
- [37] MakeUseOf, "What is apk downloader." <https://www.makeuseof.com/tag/what-is-apk-file/>. Accessed: 2023-08-16.
- [38] "Android mobile app development application software apple push notification service png - free download." <https://imgbin.com/png/lupq0kr/android-mobile-app-development-application-software-apple-push-notification-service-png>. Accessed: 2023-08-17.
- [39] Vivek, "Decompile and modify apk files with apk easy tool." <https://www.droidviews.com/decompile-and-compile-apk-files-with-apk-easy-tool/>, Jan. 2019. Accessed: 2023-08-16.

- [40] "Data set." <https://en.wikipedia.org/wiki/dataset>, Sept. 2023. Accessed: 2023-11-26.
- [41] S. Biswas, W. Haipeng, and J. Rashid, "Android permissions management at app installing," *International Journal of Security and Its Applications*, vol. 10, no. 3, pp. 223–232, 2016.
- [42] I. M. Almomani and A. A. Khayer, "A comprehensive analysis of the android permissions system," *IEEE Access*, vol. 8, pp. 216671–216688, 2020.
- [43] X. Wei, L. Gomez, I. Neamtui, and M. Faloutsos, "Permission evolution in the android ecosystem," in *Proceedings of the 28th Annual Computer Security Applications Conference*, pp. 31–40, 2012.
- [44] O. Theobald, *Machine Learning for Absolute Beginners: A Plain English Introduction*. Scatterplot Press, 2017.
- [45] makeuseof, "What is apk downloader [accessed: 16 august 2023 at 9:24 pm, internet], available at: <https://www.makeuseof.com/tag/what-is-apk-file/>."
- [46] "Android mobile app development application software apple push notification service png - free download accessed: 17 august 2023 at 1:42 pm, internet, available at: <https://imgbin.com/png/lupq0kr/android-mobile-app-development-application-softwareapple-push-notification-service-png>."
- [47] Vivek, "Decompile and modify apk files with apk easy tool, accessed: 16 august 2023 at 10:55 pm, internet, available at: <https://www.droidviews.com/decompile-and-compile-apk-files-withapk-easy-tool/>," January 01, 2019.
- [48] "Data set, accessed: 26 november 2023 at 8:31 pm, internet, available at: https://en.wikipedia.org/wiki/data_set," September 21, 2023.
- [49] S. Biswas, W. Haipeng, and J. Rashid, "Android permissions management at app installing," *International Journal of Security and Its Applications*, vol. 10, no. 3, pp. 223–232, 2016.
- [50] I. M. Almomani and A. Al Khayer, "A comprehensive analysis of the android permissions system," *Ieee access*, vol. 8, pp. 216671–216688, 2020.
- [51] X. Wei, L. Gomez, I. Neamtui, and M. Faloutsos, "Permission evolution in the android ecosystem," pp. 31–40, 2012.