CHAPTER II
LITERATURE REVIEW

2.1 Review of Current Situation

Today's users are increasingly reliant on mobile apps for various tasks and activities, but with this increased reliance comes an increased risk of malware. To protect mobile apps, it is important for users to have a website that can validate installed apps to ensure that they are safe to use. Without this validation, users may not know if the installed apps are safe, putting their personal information and devices at risk.

One of the biggest challenges faced by users is that they may not know if an installed app is safe to use, as many apps in the market are not properly validated or have bad intentions. This can lead to the installation of apps that contain malware or other types of cyber threats. This can lead to loss of personal data, financial information, and other sensitive information.

To resolve this issue, machine learning is required that can validate the installed application, the application analyses the permissions requested by the installed application. This validation process is crucial to ensure that devices and personal information are protected from harmful malware. It is important for users to be aware of these apps and use them to keep their devices and personal information safe.

2.2 Review of Related Literature

2.2.1 Data Collection

Several systems and technologies related to the hospital management system have been carried out in several previous studies. The first research entitled "*The Malware Detection Approach in the Design of Mobile Applications"* has been conducted by *(Diab et al, 2022)*.

Data Analysis

This research focuses on developing an approach to detect malware and improve the security of mobile applications. The authors propose the use of machine learning algorithms to analyse various features and patterns in mobile apps, aiming to identify potential malware or security vulnerabilities. This research aims to improve the overall security of mobile apps and protect users from potential risks associated with malware.

According to this study motive this research is to detect malware early before infection by finding it at the application design level and not at the code level, where the virus is already corrupted the system. The method in this article uses a design-level malwarenetection method based on reverse engineering, a unified modelling language (UML) environment, and web ontology language (OWL). The proposed method detects the malware "Data_Send_Trojan" malware by designing a UML model that simulates the structure of malware.

2.2.2 Data Collection

The second research entitled “Detection and Visualization of Android Malware Behavior” has been conducted by (Tehrani et al, 2016).

Data Analysis

The study focuses on developing techniques to identify and analyze the behavior of malware on the Android platform. The authors propose a detection framework that combines static and dynamic analysis methods to capture and analyze the behavior of malicious applications. The research aims to improve the understanding of Android malware behavior and provide insights into their malicious activities. The visualization aspect of the study aids in presenting the detected malicious behavior in a visual format, enhancing the comprehension of malware activities.

According to this study, This system In this journal provides monitoring that aims to identify malicious Android apps without modifying the Android firmware.

It provides a visualisation graph where function calls corresponding to predefined malware behaviours are highlighted. It consists of four components, namely, embedded client, Sink, Web Service, and visualization.

2.2.3 Data Collection

The research entitled "The rise of machine learning for detection and classification of malware: Research developments, trends and challenges" has been conducted by (Gibert et al, 2020).

Data Analysis

The authors discuss various machine learning algorithms, such as decision trees, support vector machines, and deep learning models, that have been employed in malware detection. They explore the benefits and limitations of each approach and discuss the importance of feature selection and data preprocessing techniques for improving the accuracy of malware detection models.

The article highlights the emerging trends in the field, including the use of ensemble methods and the incorporation of dynamic analysis to enhance the detection capabilities. The authors also address the challenges faced in the development and deployment of machine learning-based malware detection systems, such as the availability of labeled training data, the adaptability to evolving malware techniques, and the potential for adversarial attacks.

According to this study, this system is key research development in the use of machine learning for malware detection has been the use of deep learning techniques. Deep learning algorithms, which are a type of machine learning algorithm, can learn and make decisions on their own, without the need for human input. This has made them particularly useful for detecting and classifying malware, as they can analyze large amounts of data and identify patterns that may not be visible to humans.

2.2.4 Data Collection

The research entitled "Ranking and Fraud Review Detection for Mobile

Apps using KNN Algorithm" has been conducted by (G. Mutylayamma, K.Komali, and G,Pushpa 2017).

Data Analysis

This paper presents an analysis of a mobile application ranking fraud detection model. The purpose is to address the problem of mobile app developers employing unethical means to enhance their apps' rankings. The paper introduces a variety of fraud detection techniques divided into three classes: web ranking fraud detection, online review fraud detection, and mobile application recommendation.

The proposed system includes the K-Nearest Neighbors (KNN) algorithm, which generates principles for the recommendation system to identify and restrict fraudulent evaluations. The KNN algorithm utilizes previous records to provide the user with more relevant results. The system employs the Mining Leading Session algorithm for handling complaints about the initial version of an application. This algorithm aids in identifying duplicate app versions by analyzing historical data. In addition, the system considers the publication date of the apps, enabling the administrator to detect fraudulently published apps and block them accordingly.

In this system, users can only provide feedback once, ensuring that new users seeking to acquire an app have a clear understanding of the available options.

2.2.5 Data Collection

The research entitled "Machine Learning Algorithms - A Review by (Batta Mahesh 2017).

Data Analysis

This article explains that Supervised and unsupervised learning are two common approaches in machine learning. Supervised learning is suitable when the amount of labelled data available for training is limited. On the other hand,

unsupervised learning tends to give better results when dealing with larger data sets. If you have access to very large data sets, deep learning techniques can be very effective. Reinforcement learning and deep reinforcement learning are additional concepts to consider to expand your knowledge of machine learning. Artificial neural networks are widely used and have diverse applications, but they also have limitations.

This article aims to explore various machine learning algorithms and their significance. Machine learning has become ubiquitous in our daily lives, whether we realise it or not. From receiving product recommendations while shopping online to having photos automatically updated on social media platforms, machine learning is at work. This article serves as an introduction to some common machine learning algorithms.

2.2.6 Data Collection

The research entitled “Trojan Horse in Mobile Devices”by (Daniel Fuentes , Juan A. Álvarez, Juan A. Ortega, Luis Gonzalez-Abril and Francisco Velasco 2010).

Data Analysis

This paper investigates the behavior of Trojan horses, a type of malware that creates a gateway for malicious users to obtain illicit access to the system, thereby possibly harming confidential or personal data. The expanding quantity of personal information stored on mobile devices, such as location data, emails, SMS messages, and photographs, increases the risk of Trojan horse infection. The objective was to demonstrate how readily a Trojan horse can exploit vulnerabilities and take phonebook information from another user. SMS with a predefined structure is used for communication between the attacker and the attacked device, allowing the attacker to send commands without the victim's knowledge. The Trojan horse is concealed within an audio, video, or image file.

Skulls is a Trojan horse that not only spreads itself, but also concentrates

on obtaining confidential information from users while remaining undetected. The behavior of the Trojan horse is then explained using mobile phone experiments in which the infection is introduced to retrieve the user's contact information. There is a presentation of experimental results and potential solutions to mitigate the effects of the infection.

2.2.7 Data Collection

The research entitled “A Survey on Identification Of Ranking Fraud For Mobile Applications by (Nandini B, A.Ananda Shankar 2016).

Data Analysis

This journal discusses leaderboards, which are becoming an important method for app promotion. A higher ranking on these leaderboards means increased downloads and revenue. However, developers have used manipulative tactics, such as hiring human water armies and bot-farms, to manipulate the ranking charts.

Ranking fraud does not occur consistently, so it is critical to identify specific times when it does occur. Measurable methods are needed to automatically detect ranking fraud and identify implicit cheating patterns. Using the "Mining Leading Sessions" approach, leading events and sessions can be distinguished by analyzing historical rating records only once. Gaussian approximation and classical maximum likelihood estimation (MLE) techniques can be used to identify ratings cheating.

2.2.8 Data Collection

The research entitled “Security Threats To Android Apps” by (Dongjing He 2014).

Data Analysis

The research analyzes two dimensions of security threats to Android

applications. The report begins by analyzing the mobile health (mHealth) industry to determine the prevalence of security threats in this domain. The research revealed, through a three-stage analysis of mHealth apps, that many apps in this sector use insecure internet communications and third-party servers, posing dangers to user data.

Assuming that mobile applications are effectively protected by developers, this research investigates potential flaws in the Android operating system's fundamental security design. Specifically, this study analyzes a recently discovered danger known as side-channel data theft on Android devices.

To address this identified threat through the development and implementation of defense mechanisms aimed at mitigating the potential risks associated with this security threat, protecting user data and privacy within the mobile app ecosystem.

2.2.9 Data Collection

The research entitled “Security and Privacy Awarenes: A Survey for Smartphone User” by (Ifrat Jahan, Md, Lizur Rahman, Md Nawab Yousuf Ali 2019).

Data Analysis

This paper provides findings from a survey conducted to assess security and privacy awareness among smartphone users. The objective was to evaluate the extent of users' awareness regarding the security and privacy of their smart phones. A questionnaire was designed to measure the level of security awareness exhibited by the public. The survey aimed to determine whether there is a general sense of security satisfaction among smartphone users. Based on the survey results, a statistical model is presented to measure the level of awareness among Android users regarding their privacy.

2.2.10 Data Collection

The research entitled “Improving App Privacy: Nudging App Developers to Protect User privacy by (Rebecca Balebako, Lorrie Cranor 2014).

Data Analysis

This paper discusses the lack of research on the perspectives of application developers on privacy and security hazards posed by smartphones. The analysis of in-depth interviews and survey responses illuminates the compromises made by developers and the obstacles they face when implementing privacy and security best practices. The findings highlight the significance of educating and assisting app developers to prioritize privacy and security in their development processes.

2.3 Review of Related Product

2.3.1 Malwarebytes

Malwarebytes for android is a security application designed to protect Android devices from malware, ransomware, and other types of threats. It can scan and remove malicious software, block unwanted calls and texts. one of the scan methods used by collecting data on known malware samples and running the software on a test device, and the results of the test can be analysed to determine the detection rate and effectiveness of the software in removing malware.

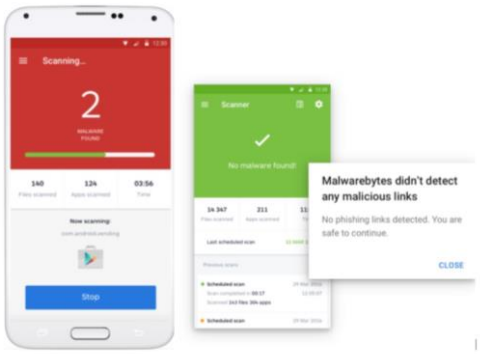

Figure 2.1 ProjectManager Dashboard Display

Figure 2.1 The app uses advanced detection algorithms to identify and remove malware, potentially unwanted programs (PUPs), and suspicious files that may threaten the device or user privacy. It uses a comprehensive malware database that is constantly growing. Another important feature of Malwarebytes for Android is its privacy audit functionality. It scans installed apps and identifies apps that may have excessive permissions or potentially intrusive behavior. This allows users to have better control over their privacy and make informed decisions regarding the apps they choose to keep on their devices.

2.3.2 Bitdefender Mobile Security

Bitdefender for Android is a comprehensive mobile security solution that offers powerful protection against malware, web threats and privacy intrusions. Its malware detection capabilities, web protection, privacy advisory and anti-theft features provide an all-in-one security solution for Android devices. With a user-friendly interface and regular updates, Bitdefender for Android helps users stay protected in the ever-evolving mobile threat landscape.

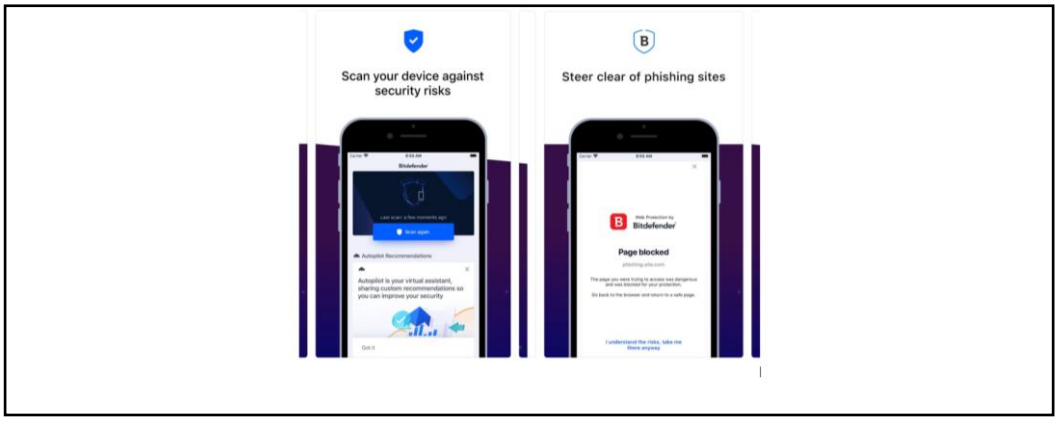

Figure 2.2 Bitdefender Mobile Security Display

Figure 2.2 Bitdefender for Android is a powerful malware detection and removal capability. The app uses advanced scanning algorithms to detect and

remove malware, viruses, and other malicious apps that may pose a risk to users' devices and data. It regularly updates its malware database to stay up to date with the latest threats. other features of Bitdefender protection for Android include robust web protection features. It scans URLs in real-time and blocks access to malicious websites, thus preventing users from accidentally visiting dangerous web pages that may contain malware or phishing attempts. This feature provides a safe browsing experience and protects against online threats.

2.3.3 AVG Antivirus and Security

Avg antivirus and security for android is a reliable and feature-rich mobile security application. Its malware detection, web protection, privacy scanner, and anti-theft features contribute to a safer and more secure Android experience. With regular updates and a user-friendly interface, AVG Antivirus and Security helps users protect their devices and personal information from various threats.

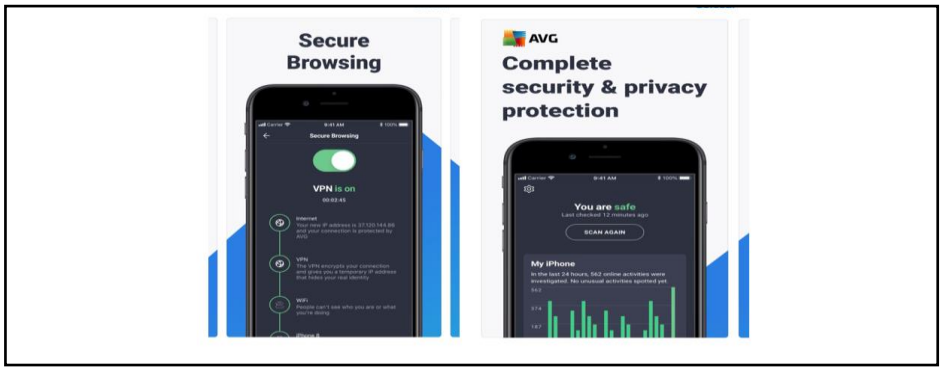

Figure 2.3 Time Tracking Display

Figure 2.3 One of the key features of AVG Antivirus and Security is its powerful malware detection and removal capabilities. It scans installed apps, files, and system settings in real-time to detect and remove malware and viruses. The app can utilise scheduled scans and on-demand scanning options to ensure your device stays protected from the latest threats. AVG Antivirus and Security features powerful web protection. It actively scans URLs in real-time and blocks access to malicious websites, so users don't fall victim to phishing attempts or visit websites

that may contain malware or malicious content. This helps ensure safe browsing and protects user data.