ANDROID RANSOMWARE ATTACK DETECTION IN SMART HEALTH CARE MONITORING SYSTEM

A PROJECT REPORT

Submitted by

ABDUR RAHMAN M

(2023246030)

A report for the phase-I of the project
submitted to the Faculty of

INFORMATION AND COMMUNICATION ENGINEERING

in partial fulfillment
for the award of the degree
of

MASTER OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY
COLLEGE OF ENGINEERING, GUINDY
ANNA UNIVERSITY
CHENNAI 600 025

DECEMBER 2024

ANNA UNIVERSITY

CHENNAI - 600 025

BONA FIDE CERTIFICATE

Certified that this project report titled **ANDROID RANSOMWARE ATTACK DETECTION IN SMART HEALTH CARE MONITORING SYSTEM** is the bona fide work of ABDUR RAHMAN M who carried out project work under my supervision. Certified further that to the best of my knowledge and belief, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or an award was conferred on an earlier occasion on this or any other candidate.

PLACE:
DATE:

Dr. D. SANGEETHA
ASSISTANT PROFESSOR (Sl.Gr)
PROJECT GUIDE
DEPARTMENT OF IST, CEG
ANNA UNIVERSITY
CHENNAI 600025

COUNTERSIGNED

Dr. S. SWAMYNATHAN
HEAD OF THE DEPARTMENT
DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY
COLLEGE OF ENGINEERING, GUINDY
ANNA UNIVERSITY
CHENNAI 600025

ABSTRACT

The integration of smart healthcare systems with Android-based devices has revolutionized the monitoring and management of patients' health data. Wearable devices, connected to smartphones, provide real-time health information, enabling efficient healthcare delivery. However, this interconnected ecosystem is increasingly vulnerable to ransomware attacks, which can compromise sensitive health data, disrupt services, and pose critical risks to patient safety. To address this issue, this project proposes a robust ransomware attack detection mechanism for Android-based smart healthcare monitoring systems.

The proposed system leverages advanced machine learning (ML) techniques to identify and mitigate ransomware threats in real time. It involves collecting and analyzing behavioral patterns of Android applications and detecting anomalies that may indicate ransomware activity. Key features include monitoring file access behaviors, encryption processes, network traffic patterns, and permissions requested by apps. The system employs a lightweight ML model optimized for resource-constrained devices to ensure minimal impact on performance and battery life.

This work aims to enhance the security and reliability of smart healthcare monitoring systems, ensuring uninterrupted service delivery and safeguarding patients' sensitive health data from ransomware attacks. The outcomes of this project will provide a scalable and practical solution for securing Android-based healthcare applications in today's rapidly evolving threat landscape.

ABSTRACT TAMIL

ACKNOWLEDGEMENT

I would like to express my deep sense of appreciation and gratitude to my project guide **Dr. D. SANGEETHA,** Assistant Professor, Department of Information Science and Technology, College of Engineering, Guindy, Anna University, Chennai for her invaluable support, supervision, guidance, useful suggestions and encouragement throughout this phase. Her moral support and continuous guidance enabled me to complete my work successfully

I thank **Dr. S. SWAMYNATHAN,** Professor and Head of the Department of Information Science and Technology, College of Engineering, Guindy, AnnaUniversity, Chennai for the prompt and limitless help in providing the excellent computing facilities to do the project and to prepare the thesis.

Wearegrateful to the project committee members **Dr. S. SRIDHAR,** Professor, **Dr. G. GEETHA,** Associate Professor and **Dr. D. NARASHIMAN,** Teaching Fellow, Department of Information Science and Technology, College of Engineering, Guindy, Anna University, Chennai for their review and valuable guidance throughout the course of our project.

We also thank the faculty member and nonteaching staff members of the Department of Information Science and Technology at College of Engineering Guindy, Anna University, Chennai for their valuable support throughout the course of our project work.

ABDUR RAHMAN M

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

BLE	Bluetooth Low Energy
API	Application Programming Interface
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UI	User Interface
MAL	Malware
RND	Ransomware Detection
FIM	File Integrity Monitoring
RPN	Region Proportional Networks
RAT	Ransomware Attack
APK	Android Package
EHR	Electronic Health Records
AV	Antivirus
NLP	Natural Language Processing
HIDS	Host-Based Intrusion Detection System
PID	Patient Identification Data

CHAPTER 1

INTRODUCTION

The increasing adoption of smart healthcare systems has transformed the way healthcare services are delivered, monitored, and managed. Android-based platforms, coupled with wearable devices, allow for continuous patient health monitoring, providing timely and accurate health data to healthcare providers. These systems improve patient care, reduce hospital visits, and enable remote health management. However, the rapid proliferation of these interconnected systems has introduced significant cybersecurity challenges, particularly in the form of ransomware attacks.

Ransomware is a type of malware that encrypts data and demands payment for its release. In a healthcare context, such attacks can have devastating consequences, including loss of critical patient information, disruption of healthcare services, and potential risks to patient safety. Android devices, being widely used and relatively less secure, are an attractive target for ransomware attackers. The combination of sensitive health data and inadequate security mechanisms creates a vulnerable environment for ransomware exploits.

This project aims to develop an effective ransomware attack detection system specifically tailored for Android-based smart healthcare monitoring frameworks. By leveraging machine learning algorithms, the proposed solution identifies malicious activities in real time, preventing data loss and ensuring the integrity of the healthcare system. The focus is on analyzing application behavior, file access patterns, and encryption processes to detect anomalies associated with ransomware activity.

1.1 BACKGROUND OF SMART HEALTH CARE SYSTEMS

Smart healthcare systems utilize advanced technologies such as IoT devices, mobile applications, and cloud computing to deliver patient-centric healthcare solutions. Wearable devices, including smartwatches and fitness trackers, monitor vital signs such as heart rate, blood pressure, and glucose levels. These devices connect to Android smartphones to store, analyze, and share health data with healthcare providers in real time, enabling early diagnosis and preventive care. Despite their benefits, these systems rely heavily on secure data transmission and storage, making them vulnerable to cyber threats.

1.1.1 Overview Of The Smart Health Care Systems

Definition and key features of smart healthcare systems. Role of technology in enhancing patient care and efficiency.

1.1.2 Wearable Devices in Healthcare

Wearable devices have become an integral part of modern healthcare systems, offering real-time monitoring and management of various health parameters. These devices include smartwatches, fitness trackers, continuous glucose monitors, and wearable ECG monitors. By continuously collecting data on metrics such as heart rate, blood pressure, activity levels, and blood glucose, wearable devices enable early detection of health anomalies and support preventive care.The integration of wearable devices with Android platforms enhances their functionality by enabling seamless data transmission, analysis, and storage. Through dedicated healthcare applications, data from these devices can be visualized, analyzed, and shared with healthcare providers, empowering them to make timely and informed decisions. Additionally, wearables contribute to personalized healthcare by tailoring insights and recommendations based on individual health data.

1.1.3 Android as a Platform for Healthcare

Android has emerged as a dominant platform in the realm of smart healthcare systems due to its accessibility, flexibility, and widespread adoption. Its open-source nature allows developers to create customized healthcare applications tailored to specific needs, making it a preferred choice for integrating wearable devices and other health-monitoring technologies.

1.1.4 Interconnectivity in Smart Healthcare

Interconnectivity is a cornerstone of modern smart healthcare systems, enabling seamless communication between devices, applications, and cloud services. Wearable devices, such as fitness trackers and health monitors, are designed to transmit real-time data to Android-based applications, which process and display this information for users and healthcare providers.

The interconnected ecosystem allows for continuous health monitoring, early anomaly detection, and remote patient management. For example, wearable devices can send alerts to caregivers or physicians in case of abnormal health readings, ensuring timely intervention. Additionally, integration with cloud services provides secure data storage and access, enabling healthcare providers to review patient histories and trends remotely.

1.1.5 Challenges in Smart Healthcare Systems

Smart healthcare systems face a range of challenges that impact their effectiveness and security. One of the primary concerns is data security and privacy, as healthcare data is highly sensitive and vulnerable to breaches, especially in the face of cyber threats like ransomware. Ensuring secure communication, encryption, and compliance with regulations such as HIPAA is crucial. Another challenge is interoperability, as integrating diverse healthcare devices and platforms often involves compatibility issues, which can complicate communication and data exchange. The accuracy and reliability of data from wearables and monitoring systems are also critical, as corrupted or inaccurate data can lead to incorrect diagnoses and treatments. Additionally, user adoption remains a significant hurdle, as patients and healthcare providers may resist adopting new technologies, especially if they are complex or unreliable.

1.2 CYBER SECURITY CHALLENGES IN SMART HEALTH CARE

The integration of healthcare systems with digital platforms introduces various cybersecurity risks. Hackers often target healthcare systems due to the high value of patient data. Unauthorized access, data breaches, and malware attacks can compromise the privacy, integrity, and availability of critical health information. Among these threats, ransomware has emerged as a significant concern, given its potential to encrypt vital data and disrupt healthcare services.

1.2.1 Data Security and Privacy

Data security and privacy are paramount in any healthcare system, but they become even more critical in smart healthcare systems that use wearable devices, mobile applications, and interconnected networks. Healthcare data, which includes sensitive personal and medical information, must be protected against unauthorized access, data breaches, and cyberattacks. With ransomware attacks becoming increasingly common, the security of these systems is at risk, potentially compromising patient care and violating patient privacy.

1.2.2 Interoperability

Interoperability refers to the ability of different healthcare devices, platforms, and systems to communicate with each other seamlessly. In a smart healthcare system, numerous devices—such as wearable health trackers, patient monitoring systems, and hospital management software—must work together to provide cohesive care. However, lack of standardized protocols or incompatible data formats can create barriers to smooth data sharing, leading to fragmented patient care.

To overcome this challenge, developing common data exchange standards like HL7 (Health Level 7) or FHIR (Fast Healthcare Interoperability Resources) is essential. Moreover, the implementation of APIs (Application Programming Interfaces) and cloud-based platforms can help facilitate easier integration between diverse systems and devices.

1.3 RANSOMWARE AND ITS IMPLICATIONS

Ransomware is a type of malicious software (malware) designed to block access to a computer system or encrypt data until a ransom is paid. Attackers typically deliver ransomware through phishing emails, malicious downloads, or exploiting system vulnerabilities. Once installed, ransomware either locks users out of their devices (locker ransomware) or encrypts sensitive data (crypto ransomware), making it inaccessible until the ransom is paid, usually in cryptocurrency to ensure anonymity.

1.3.1 Disruption of Healthcare Services

Ransomware can shut down hospital operations by locking medical records, patient monitoring systems, or other critical software.Inability to access patient data can lead to delays in diagnosis and treatment, jeopardizing patient safety.

1.3.2 Compromised Patient Safety

Patient safety is the cornerstone of healthcare systems. However, ransomware attacks compromise this safety by disrupting access to critical medical data and systems, delaying diagnoses, and affecting timely treatment. The interconnected nature of smart healthcare systems exacerbates the impact, as ransomware can disable multiple devices and applications simultaneously. This disruption can have life-threatening consequences, particularly for patients relying on real-time monitoring and life-support systems.

1.3.2.1 Delayed Emergency Responses

Smart healthcare systems integrate emergency alert mechanisms, such as wearable devices that notify medical teams of abnormal vitals. Ransomware disrupting these systems can delay emergency responses, worsening patient outcomes.An attack that halts data transmission from a cardiac monitor may delay intervention for a patient experiencing a heart attack.

1.3.3 Stress and Anxiety for Patients

Ransomware attacks create chaos, leaving both healthcare providers and patients in a state of uncertainty. Patients in need of urgent care may experience heightened stress, which can exacerbate existing conditions. Meanwhile, staff may be overwhelmed trying to restore systems or implement manual workflows.During an attack, a patient with a chronic condition may lose access to telemedicine consultations, causing unnecessary anxiety and delays in care.

1.3.4 Misinformation Due to Data Corruption

Ransomware can corrupt or encrypt critical medical data, leading to incorrect diagnoses or treatment plans. For example, if patient allergies or medication records are unavailable, doctors might inadvertently prescribe harmful medications.An encrypted EHR system might omit a patient's history of drug allergies, resulting in life-threatening reactions to administered medication.

CHAPTER 2

LITERATURE SURVEY/RELATED WORK

2.1 OVERVIEW

This section reviews significant research related to Android malware detection, specifically ransomware attacks in the context of smart healthcare systems. We focus on methodologies that aim to identify and prevent malicious behaviors, examining key approaches like behavioral analysis, system monitoring, and the use of machine learning for detecting ransomware and other threats in mobile applications. We also highlight work relevant to wearable devices in healthcare monitoring and the challenges of maintaining security in IoT-based systems.

2.2 EXISTING SYSTEMS

This section presents an overview of existing systems and methodologies used for detecting Android malware, particularly focusing on approaches relevant to identifying ransomware attacks in healthcare systems. The key methodologies can be grouped into static analysis, dynamic analysis, behavior-based detection, and machine learning-based approaches. [**?**].

2.2.1 Android Malware Detection Approaches

Various techniques have been developed for detecting malicious Android applications, with a focus on understanding and preventing the actions of malware such as ransomware. These can be broadly categorized into static analysis, dynamic analysis, and behavior-based approaches.

2.2.2 Static and Dynamic Analysis Methods

Traditional approaches like static and dynamic analysis focus on analyzing Android app code and behavior during execution. Tools that employ static analysis examine the app's source code, API calls, and permissions to identify potential threats [6][7]. However, these methods are often limited in their ability to detect sophisticated or evolving malware. Dynamic analysis, which involves monitoring the app's behavior at runtime, is more effective in identifying malicious activities such as unauthorized data access or system manipulation. However, dynamic analysis can be resource-intensive and may not always capture long-term or intermittent attacks.

2.2.3 Behavior-Based Malware Detection

A more recent approach, behavior-based malware detection, focuses on identifying malware by analyzing its actions rather than the code itself. Systems like MADAM utilize multi-level monitoring, analyzing behaviors at the kernel, application, user, and package levels to detect suspicious activity indicative of malware [6]. These methods have shown high accuracy in detecting real-world malware, including ransomware, with minimal overhead. Behavior-based systems are particularly effective for detecting unknown or evolving malware variants, which are common in dynamic environments like healthcare monitoring systems [5].

2.2.4 Ransomware Detection in Healthcare Systems

Ransomware attacks, which encrypt sensitive data and demand payment for decryption, pose a significant threat to healthcare systems. These systems often contain sensitive medical data, making them attractive targets for cybercriminals. Ransomware detection in Android-based healthcare systems often requires an integrated approach that combines system-level monitoring with anomaly detection. Several studies have focused on the detection of ransomware within mobile systems by analyzing system and application behaviors. For example, the SherLock dataset, created by monitoring Android devices under attack, has been used to analyze smartphone security and develop malware detection algorithms [5]. By leveraging labeled data from both benign and malicious applications, this dataset enables researchers to train models capable of identifying ransomware based on behavioral patterns, without requiring root access to the system. This aligns well with the need for non-invasive, scalable detection methods in healthcare monitoring devices.

2.2.5 Machine Learning and AI in Malware Detection

Machine learning (ML) techniques are increasingly applied to ransomware detection in Android devices. Approaches such as deep learning, decision trees, and support vector machines have been explored for classifying apps as benign or malicious based on features extracted from app behaviors or API calls [8][9]. EveDroid, for instance, uses a neural network model to detect new malware based on event groupings, which enables it to detect evolving threats such as ransomware despite changes in app behavior over time [8]. The combination of ML and behavior-based analysis offers an effective and adaptive solution to ransomware detection, particularly in dynamic environments like smart healthcare systems, where apps and attacks constantly evolve.

2.3 IoT and Security in Healthcare

The Internet of Things (IoT) plays a crucial role in modern healthcare, with wearable devices and connected sensors enabling real-time monitoring of patient health. However, the integration of IoT devices into healthcare systems also introduces security vulnerabilities, particularly regarding data privacy and device integrity. Existing research highlights the need for enhanced security in IoT-based healthcare applications to prevent attacks that could compromise patient data or disrupt critical health monitoring services [10].As healthcare systems become more interconnected through IoT, ensuring the integrity and security of these devices becomes paramount. Research suggests that a comprehensive security framework that integrates behavioral analysis, machine learning, and real-time monitoring is essential for detecting and mitigating threats like ransomware in connected healthcare environments [10]. Additionally, advancements in big data analytics can help process the large volumes of data generated by IoT devices, enabling more effective detection of anomalies or malicious activities. The integration of machine learning (ML) techniques has greatly advanced malware detection, particularly for Android apps. Approaches such as deep learning, random forests, and neural networks have been applied to classify apps based on their behaviors or API calls. EveDroid, a machine learning-based malware detection system, represents an innovative approach by utilizing event-based analysis rather than focusing solely on individual API calls. It groups related events into clusters and uses a neural network to mine semantic relationships between them, enabling detection of malware even as it evolves and adapts over time. This ability to detect unknown or newly evolved malware makes EveDroid particularly suitable for dynamic environments like Android-based healthcare monitoring systems, where new apps are constantly being introduced, and threats evolve rapidly.

2.4 HYBRID APPROACHES FOR RANSOMWARE DETECTION IN IOT-INTEGRATED HEALTHCARE SYSTEMS

The integration of IoT-based medical sensors with Android devices has significantly improved healthcare services, enabling seamless sharing of patient data with cloud-based systems. However, this connectivity introduces substantial security challenges, particularly the rising threat of ransomware attacks targeting healthcare data and patient privacy. Existing ransomware detection methods primarily utilize static analysis, focusing on application permissions and suspicious code, or dynamic analysis, monitoring runtime behaviors. While effective to some extent, these methods struggle with complex ransomware families and achieving high accuracy. To address these challenges, recent approaches highlight the importance of leveraging threatening text as a detection feature, extracted both statically from code and dynamically from runtime application images. Hybrid methods combining static and dynamic techniques, supported by machine learning classifiers, have shown promise in improving accuracy and cross-family classification of ransomware, such as encryption-based and lock-based variants. Experimental results of these methods demonstrate significant advancements, achieving up to 94

2.5 LITERATURE SURVEY SUMMARY

The review of existing literature on Android malware detection, specifically for ransomware attacks in smart healthcare systems, reveals a range of promising methodologies and insights. The evolution of mobile malware, especially ransomware, requires continuous adaptation in detection techniques due to the dynamic nature of both Android applications and their corresponding threats.Traditional Android malware detection methods primarily rely on static and dynamic analysis. Static analysis methods examine the code of an app to identify malicious patterns, such as suspicious permissions or potentially harmful API calls. Dynamic analysis, on the other hand, observes the app during execution, capturing its runtime behavior. While these methods are effective, they have limitations. Static analysis may fail to detect malware that obfuscates its code, and dynamic analysis can be computationally expensive and sometimes miss subtle, long-term attack behaviors.In contrast, behavior-based malware detection, a more recent approach, shifts the focus from code inspection to the actual activities performed by apps on the device. This method identifies malware by monitoring actions such as unauthorized data access or system resource manipulation. These approaches are effective for detecting malware like ransomware, which often relies on unusual system behavior to encrypt files or demand ransom. Systems like MADAM use multi-level monitoring (kernel, application, user) to analyze Android app behaviors comprehensively, improving detection accuracy. This trend towards behavior-based detection is crucial in environments like healthcare, where both benign and malicious apps may exhibit similar permission and resource access patterns but differ in terms of behavior. Ransomware poses a unique challenge in healthcare due to the sensitive nature of medical data. Attacks targeting healthcare systems often aim to lock critical data, demanding a ransom for decryption. Given the importance of real-time monitoring and data integrity in healthcare, existing research emphasizes the need for real-time detection of ransomware. Traditional detection methods, including signature-based detection, are not always sufficient because they rely on known patterns or signatures of malware. As a result, new, more robust methods, such as using behavior analysis combined with machine learning, are becoming increasingly necessary. The SherLock dataset, for example, has been used to monitor Android devices and provide a comprehensive data set for training models capable of detecting ransomware and other malicious activities. This dataset includes real-world Android app data, which allows for training of models that can identify ransomware behaviors with minimal system interference, making it ideal for applications like smart healthcare devices.

CHAPTER 3

SYSTEM ARCHITECTURE

The system architecture for the Android Ransomware Attack Detection in Smart Healthcare Monitoring System is designed to ensure the security, integrity, and availability of both healthcare data and critical patient care services. The architecture is layered to provide modular, scalable, and resilient functionality that not only supports real-time health monitoring but also protects against potential ransomware threats that may compromise system operations.

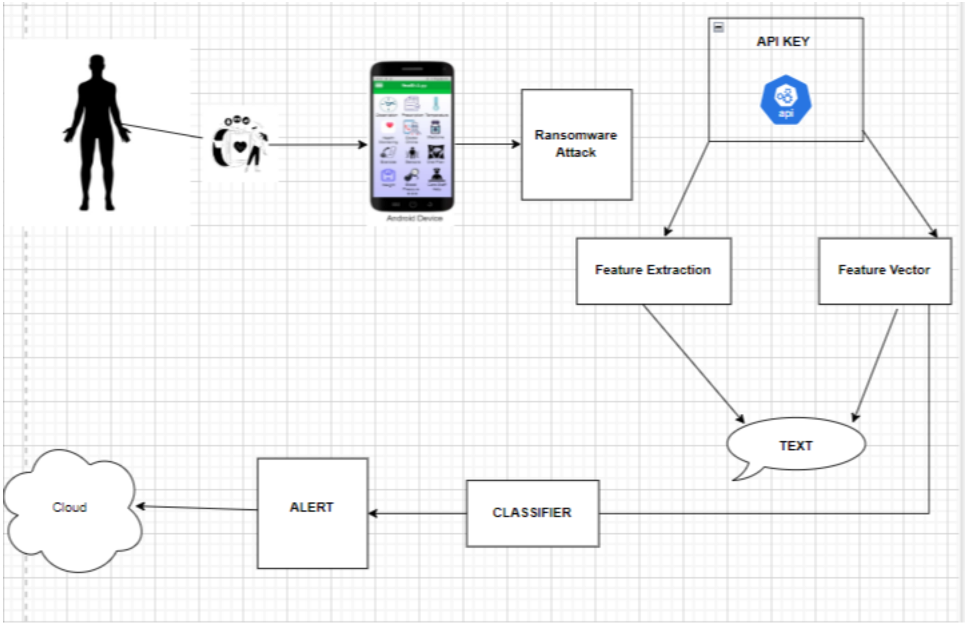


Figure 3.1: System Architecture

3.1 DATASET AND IMPLEMENTATION

This section explains the dataset used in our proposed meth odology. In the literature, authors have used datasets for experi ments that consist of two categories: The Android ransomware dataset and the benign application dataset. The first dataset of ransomware variants was collected from RansomProber (Public) , which is freely available and contains 2000 ransom ware applications. The second dataset we collect is from various Internet resources id-ransomware.blogspot, which contains 1,713 ransomware pattern variants with threats and 1,000 ransomware application authorizations . The benign application dataset collected via the open-source apkpure crawler5 from the Google Play store consists of 2,700 benign, most popular applications. For all datasets, we considered only those sam ples whose family seems to be coherent with ransomware The proposed technique uses both the static and dynamic aspects for the evaluation. Therefore, the experimental setup used includes the appropriate hardware and software resources to facilitate the corresponding experiments. To retrieve dynamic features and characteristics on the sandbox, Genymotion Android emulator is used that execute each application on an Android emulator and captured all screenshots and videos clips, image files from the resources folder, and extract threatening messages and words. APK tool Mobsf is used for decompilation. Mobsf is an automated, all-in-one mobile application for cross platform used for pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. The graphical representation of the obtained results for the Decision Tree classifier with y-axis represents percentage.The achieved accuracy for this classifier is about 91and recall remain significant. The decision tree classifier pro vided an accuracy of 93.83correctly recognized patterns (out of all recognized app pat terns), while the high recall value of 85.11overall correct classification for the full dataset used. Also, a higher True-Positive Rate (TPR), i.e., up to 90, highlights the effectiveness of the Decision Tree-based classification (a higher number of detected ransomware was actually ransomware). The achieved accuracy for this classifier is 92remarkable values for precision and recall. However, these results are lower compared to the Support Vector Machine based classification of ransomware and benign applications.

3.2 DATA COLLECTION AND PREPROCESSING

In the smart healthcare monitoring system, data collection plays a critical role in providing accurate and real-time health information. The system relies on wearable devices, such as smartwatches, fitness trackers, and medical-grade sensors, to collect a wide range of physiological data from patients. These devices are equipped with sensors that measure vital health metrics, including heart rate, blood pressure, blood glucose levels, body temperature, and physical activity. The data is captured continuously or at predefined intervals to monitor patients' health in real-time. The wearable devices are synchronized with the mobile application via Bluetooth or Wi-Fi to transmit the collected data securely for further processing.

3.2.1 Data Cleaning

The first step in preprocessing involves cleaning the raw data to eliminate any noise or outliers that could skew the analysis. Missing values in the dataset are handled using imputation techniques (e.g., using mean, median, or interpolation) to replace gaps in the data. Inaccurate or anomalous readings, such as sudden spikes or drops in sensor values that don't correspond to real physiological changes, are flagged and removed.

3.2.2 Data Transformation and Normalization

Once the data is cleaned, it is often necessary to transform it for better consistency and comparability. For instance, certain health metrics, such as heart rate or glucose levels, might be collected in different units or scales across various devices. To standardize these, the data is normalized or scaled so that all features are on a comparable range. This ensures that the analysis of the data does not favor one type of measurement over another due to differing scales.

3.2.3 Time-Series Alignment

Since wearable devices collect data over time, it is crucial to align the time-series data for synchronization. Wearables may record data at slightly different time intervals or have occasional connectivity delays. The preprocessing step ensures that the data from different devices is aligned, with timestamps matched accurately, allowing for meaningful comparisons and trend analysis.

3.2.4 Anonymization and Security

As health data is inherently sensitive, ensuring privacy and security is a top priority. To comply with regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation), personal identifying information is anonymized. This includes stripping away any personal identifiers (e.g., names, addresses) from the data, ensuring that only health-related information is stored and processed. Additionally, the data is encrypted both during transmission (using secure protocols like HTTPS) and at rest (using encryption algorithms) to protect patient privacy.

3.3 PREPROCESSING FOR RANSOMWARE ATTACK DETECTION

Beyond ensuring the integrity of health data, the preprocessing phase also involves preparing the data for ransomware attack detection. The system continuously monitors interactions with the mobile app and cloud server, looking for patterns that could indicate malicious activity. For example, an increase in data access requests, or an unusually high volume of data being transferred between devices and the cloud, could be signs of ransomware attempting to encrypt or steal sensitive health data.The preprocessing system identifies such irregularities by examining metadata, such as timestamps of data requests, frequency of user interactions, and system behavior. If an anomaly is detected, the system triggers alerts for further investigation. Additionally, historical data trends from health metrics and system activity are stored and analyzed to identify baselines, making it easier to spot deviations caused by ransomware.

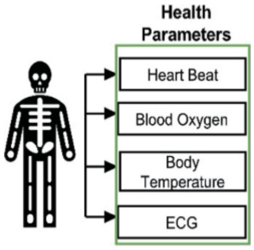


Figure 3.2: Health Parameters

3.3.1 Data Storage and Integration

After preprocessing, the data is securely stored in the cloud for long-term retention and further analysis. The system utilizes secure cloud storage solutions (e.g., AWS S3, Google Cloud Storage) with robust encryption and access control mechanisms. The data is integrated into the cloud analytics platform, where machine learning algorithms and other advanced analytics tools are used to monitor health conditions and detect potential cybersecurity threats, such as ransomware.

3.3.2 Data Collection Monitoring for Ransomware Indicators

Monitoring Data Access Patterns,Discuss how the system monitors the frequency, duration, and timestamps of data access requests from users and devices. Suspicious access patterns could indicate ransomware activities such as unauthorized data encryption or file access.Network Traffic Analysis,Detail how network traffic is analyzed to detect unusual data transmission behaviors, such as an unusually high volume of data being transferred, which could suggest ransomware attempting to exfiltrate or encrypt data. Log Data Collection,Explain how logs from the healthcare system (e.g., app logs, system logs, server logs) are continuously monitored. These logs help to detect anomalous behaviors such as rapid file access, failed login attempts, or suspicious data interactions.

3.3.3 Feature Engineering for Ransomware Detection

FeatureExtraction,Describe how key features relevant to ransomware detection are extracted from raw data. These may include factors like access frequency, transmission speed, and unusual patterns in data requests. These features are critical for identifying ransomware-like behaviors.Data Aggregation,Discuss how data from multiple sources (e.g., wearable devices, health data, system logs) is aggregated to form a comprehensive dataset. This aggregation allows the system to have a unified view of all activities and helps in detecting malicious anomalies more effectively.Dimensionality Reduction,Explain how dimensionality reduction techniques like Principal Component Analysis (PCA) or feature selection are applied to reduce the number of variables while maintaining the relevant information necessary for ransomware detection. Additionally, network traffic features, such as communication with external servers and protocol usage, are critical for identifying potential ransomware exfiltration attempts. Behavioral features, like abnormal data access at unusual times, or the rapid synchronization of wearable devices, also provide valuable insights. Aggregated statistical features, such as average data access frequency or variance in transmission rates, further help in detecting deviations from normal system behavior.

3.3.4 Real-Time Monitoring and Detection

Real-Time Data Processing, Outline the importance of processing data in real time to quickly identify potential ransomware threats. The system processes incoming data (e.g., from wearable devices, mobile apps) as it is received to allow for immediate detection of abnormal activities. Alert Generation and Threat Response,Explain how alerts are generated when anomalies are detected, indicating potential ransomware activity. These alerts allow administrators or healthcare professionals to take immediate action, such as isolating the infected system or initiating countermeasures. Event Correlation for Attack Detection,Discuss how the system correlates various events and interactions (e.g., failed logins, sudden spikes in data requests) to determine if these are part of a larger ransomware attack.

3.4 SECURITY AND PRIVACY CONSIDERATIONS IN DATA PREPROCESSING

Security and privacy considerations are critical when preprocessing data for ransomware attack detection, especially in healthcare systems where sensitive patient information is involved. Ensuring that personal and medical data is securely handled throughout the preprocessing stages is paramount to protect patient privacy and comply with regulations such as HIPAA and GDPR. During data collection, encryption techniques are employed to protect data both in transit and at rest, ensuring that unauthorized access is prevented. Furthermore, anonymization and pseudonymization methods are applied to sensitive patient data to remove personally identifiable information (PII), reducing the risk of exposure if the data is breached or misused. Additionally, access controls are implemented during data preprocessing to ensure that only authorized personnel can interact with or manipulate sensitive data, safeguarding against both internal and external threats. By implementing these security measures, healthcare systems can effectively maintain the confidentiality, integrity, and availability of sensitive data while still enabling effective ransomware detection and analysis. Moreover, the use of secure, privacy-preserving algorithms ensures that data privacy is maintained throughout the entire detection process, from data collection through feature extraction and analysis.

3.5 FLOW ARCHITECTURE

The flow architecture for detecting ransomware attacks in the Android-based smart healthcare monitoring system begins with the continuous collection of data from various sources, including wearable devices that track healthcare metrics, system logs that monitor user actions, and network traffic data to detect unusual behavior. This data is then processed in several stages to ensure privacy and security. Sensitive patient information is anonymized and encrypted during transmission, and noise is removed from the raw data through cleaning. Feature engineering is employed to extract meaningful insights, such as user access patterns, data transmission rates, and network communication behaviors, which are then normalized and scaled. The preprocessed data is analyzed for anomalies that could suggest ransomware activity, using statistical and time-series analysis. Machine learning models, trained to recognize ransomware behaviors, classify the data and detect deviations from normal system behavior. If an anomaly is identified, the system generates real-time alerts, notifying administrators of potential ransomware attacks. In response, the affected systems are isolated to prevent further damage, and recovery protocols, such as restoring from backups, are triggered. Throughout this process, detailed reports and audit logs are generated to document the attack and ensure that all actions taken are recorded for future analysis. This comprehensive architecture ensures that the healthcare system remains secure by continuously monitoring for ransomware and responding swiftly to any threats.

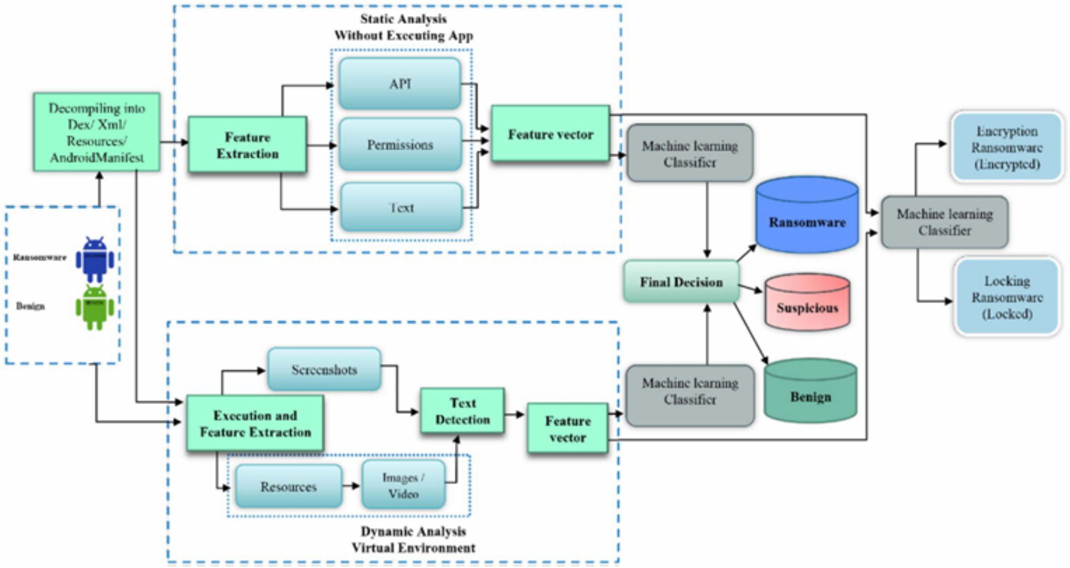


Figure 3.3: Proposed Architecture

3.6 INCIDENT RESPONSE AND RECOVERY

Incident response and recovery are critical components of the system architecture, ensuring that any detected ransomware attacks are swiftly contained and mitigated. Once ransomware behavior is identified, the system immediately initiates a series of predefined response protocols. First, it isolates the affected devices or systems from the rest of the network to prevent the ransomware from spreading further. This containment action helps to preserve the integrity of other parts of the healthcare monitoring system. Simultaneously, backup data restoration is triggered to recover any encrypted or lost information, minimizing downtime and ensuring that healthcare services are not significantly disrupted. The system also applies security measures such as updating software patches, strengthening firewall rules, and blocking suspicious external IP addresses to prevent further attack attempts. During this process, detailed logs are generated to document every action taken, which is essential for post-incident analysis and compliance audits. This structured incident response ensures that once an attack is detected, the system can rapidly recover, limiting the damage and restoring normal operations as quickly as possible.

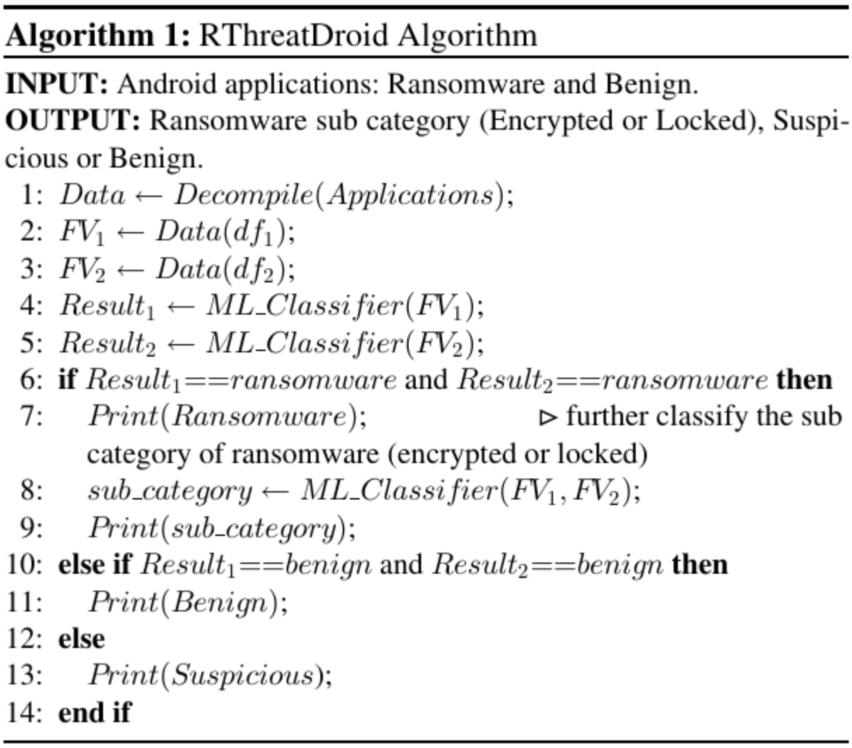
CHAPTER 4

IMPLEMENTATION

The implementation of the Android Ransomware Attack Detection in Smart Healthcare Monitoring System involves several stages, each targeting a critical aspect of the system's functionality, from data collection to real-time detection and response.

4.1 DEVELOPMENT OF THE ANDROID APPLICATION

App Design,The Android application is developed using Flutter, enabling cross-platform compatibility with wearables and healthcare devices. The UI of the app is designed to track and display real-time health data from connected wearable devices, including heart rate, glucose levels, and blood pressure. Integration with Wearable Devices,The app integrates with various wearable devices through Bluetooth or other wireless communication protocols. Data from these devices is collected and transmitted to the backend for analysis. APIs and SDKs specific to wearable devices (e.g., Fitbit, Apple HealthKit) are used to ensure seamless communication between the app and devices.Real-time Data Collection,The app continuously collects data from the wearables, logs user interactions, and monitors network traffic. System logs from both the app and the device are sent to the server for further processing.The UI design will incorporate a user-friendly interface that displays real-time health metrics such as heart rate, temperature, and activity levels, with visual indicators and notifications for abnormal readings. The application will feature secure data communication between the wearables and the system, ensuring that all health information is encrypted and stored securely. Additionally, the app will implement machine learning algorithms for detecting anomalies or potential security threats, such as ransomware, to safeguard the user's personal health data. Regular updates and maintenance will be planned to enhance functionality, improve security, and ensure the overall user experience.



Algorithm 1: RThreatDroid Algorithm

INPUT: Android applications: Ransomware and Benign.
OUTPUT: Ransomware sub category (Encrypted or Locked), Suspicious or Benign.

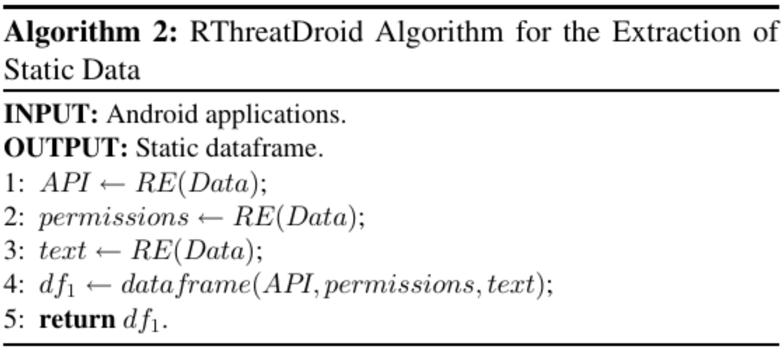
```
$Data \leftarrow Decompile(Applications)$;
$FV_1 \leftarrow Data(df_1)$;
$FV_2 \leftarrow Data(df_2)$;
$Result_1 \leftarrow ML\_Classifier(FV_1)$;
$Result_2 \leftarrow ML\_Classifier(FV_2)$;
if $Result_1 == ransomware$ and $Result_2 == ransomware$ then
    $Print(Ransomware)$;    ▷ further classify the sub category of ransomware (encrypted or locked)
    $sub\_category \leftarrow ML\_Classifier(FV_1, FV_2)$;
    $Print(sub\_category)$;
else if $Result_1 == benign$ and $Result_2 == benign$ then
    $Print(Benign)$;
else
    $Print(Suspicious)$;
end if
```

4.2 RANSOMWARE ATTACK DETECTION IN SMART HEALTHCARE SYSTEMS

In the implementation of the ransomware attack detection system, we first identified key points of vulnerability within the Android-based healthcare app. The system relies on monitoring both the device and wearable health data in real time. We utilized machine learning models trained on normal and malicious behavior to analyze system and network logs for ransomware activity. The detection process is based on identifying anomalies such as unusual system resource usage or data access patterns, which may indicate a ransomware attack. We integrated this detection framework into the Android app to ensure a proactive defense mechanism.

4.3 INTEGRATION OF WEARABLE DEVICES FOR HEALTH MONITORING

The wearable devices, such as fitness trackers and medical sensors, were connected to the Android app through Bluetooth and Wi-Fi. To implement this, we used Flutter for app development, which facilitated communication between the wearables and the mobile device. We utilized Bluetooth Low Energy (BLE) protocols to ensure seamless data transmission from the wearables to the mobile app. The data was sent to a cloud-based server for analysis, where health metrics like heart rate, blood pressure, and body temperature were continuously monitored. This integration also enabled tracking the devices' operational status to detect any anomalies that could suggest a ransomware attack.



Algorithm 2: RThreatDroid Algorithm for the Extraction of Static Data

INPUT: Android applications.
OUTPUT: Static dataframe.

```
$API \leftarrow RE(Data)$;
$permissions \leftarrow RE(Data)$;
$text \leftarrow RE(Data)$;
$df_1 \leftarrow dataframe(API, permissions, text)$;
return $df_1$.
```

4.4 TRAINING OF MACHINE LEARNING CLASSIFIER

Applications are given as input of which static as well as dynamicfeatures are retrieved by decompiling the applications. Later, we have extracted permissions and text from images and videos. All characteristics combine into a feature vector that are used to train machine learning models. After training the classifier based on the features applications were labeled ran somware as 1 and benign as 0 to form feature vector. We uti lized a variety of classifiers for both static and dynamic approaches (SVM, DT, NB, RF, LR) to train each feature vec tor. Once all models train, they can categorize applications and assign labels such as ransomware or benign applications. Dur ing pre-processing, we have to normalize all extracted pictures and words into specific pattern that can use further to identify ransomware i.e., before using pictures, the first step is to format the pictures by resizing them and changing their colors to black and white in order to identify their contents better. Moreover, removing duplicate data and content to allow processing effec tively. In addition, we have separated a text into smaller units called tokens during tokenization i.e, token can be either words, characters or subwords (n-gram characters). By noise removal means removing characters or digits or any piece of text that can interfere during processing

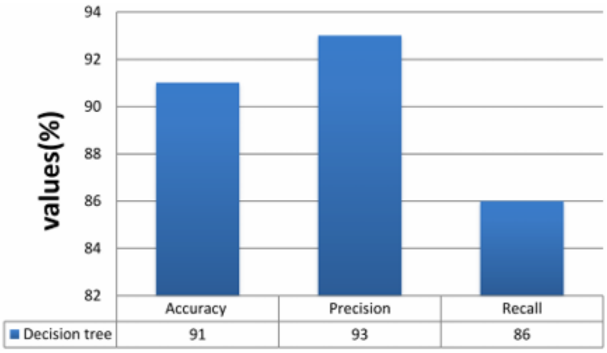


Figure 4.1: Evaluation results with decision tree

The graphical representation of the obtained results for the Decision Tree classifier with y-axis represents percentage.The achieved accuracy for this classifier is about 91, while the values for precision and recall remain significant. The decision tree classifier pro vided an accuracy of 93.83, showing the high percentage of correctly recognized patterns (out of all recognized app pat terns), while the high recall value of 85.11 indicates the overall correct classification for the full dataset used. Also, a higher True-Positive Rate (TPR), i.e., up to 90The obtained results for the Logistic Regression classifier. The achieved accuracy for this classifier is 91while the values for precision and recall are remarkable. How ever, these results are lower compared to Support Vector Machine and Random

Forest-based classification of ransom ware and benign applications. The AUC for TPR and FPR is higher than 85

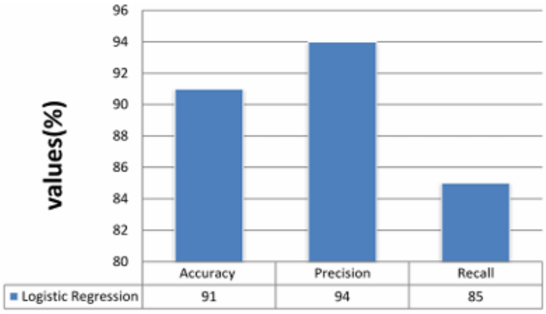


Figure 4.2: Evaluation results with logistic tree

The obtained results for theRandomForest(RF) classifier. The achieved accuracy for this classifier is 92remarkable values for precision and recall. However, these results are lower compared to the Support Vector Machine based classification of ransomware and benign applications. The AUC for TPR and FPR is higher than 85

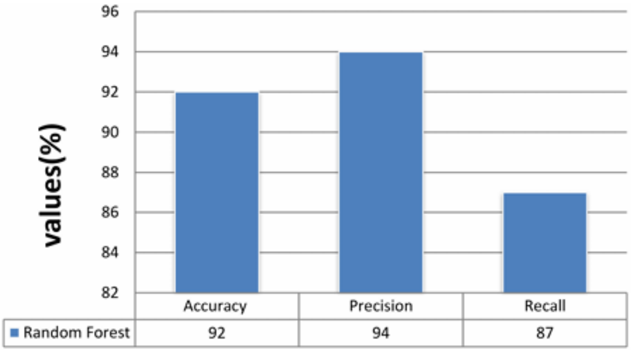


Figure 4.3: Evaluation results with Random Forest

The obtained results for the Support Vector Machine (SVM) classifier. The achieved accuracy for this classifier is 92.93, while the lower precision and higher recall rate show that the SVM-based experiments lead to morealse positives.That the AUC for TPR and FPR is more than 90, which is significant. the results (accuracy, precision, and recall) obtained with the ML classifier Naive Bayes. The accuracy achieved by Naive Bayes is low (i.e., approximately 90indicating low classification ability with respect to the features and datasets used. The AUC for TPR and FPR is less than 90, indicating lower accuracy of Naive Bayes.

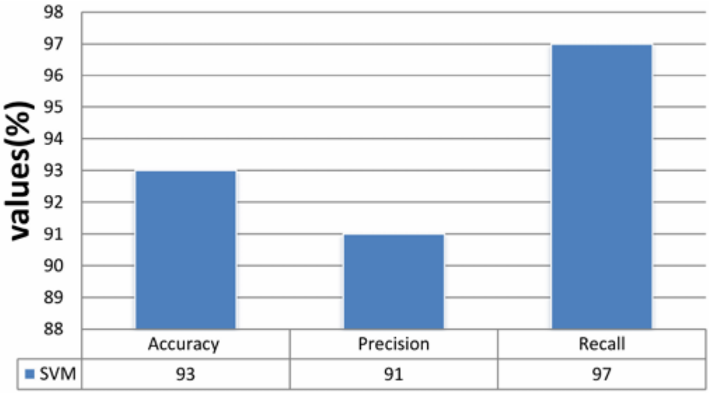


Figure 4.4: Evaluation results with Support Vector Machine

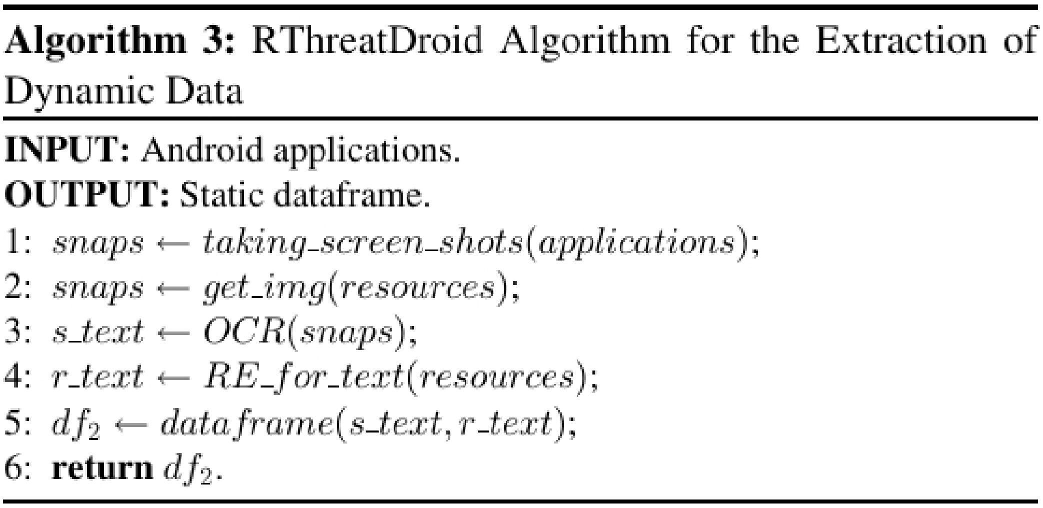
The comparative analysis performed with a related research work based on the ML approach called Randroid . The comparison was performed using the five different ML classifiers (i.e., Decision Tree, Random Forest, Na€ ıve Bayes, Support Vector Machine Classifier, and Logistic Regression). The best performance in terms of ML classifiers was achieved by SVM (for both the proposed and Randroid, was 5.204 less effective (i.e., lower accuracy) than our proposed system.

4.5 MACHINE LEARNING FOR RANSOMWARE DETECTION

For the ransomware detection module, we implemented a supervised machine learning model using Python and TensorFlow. We used historical data of normal and compromised devices to train the model, focusing on system logs and network behavior that typically occur during ransomware attacks. Features like CPU usage, memory utilization, file access patterns, and network traffic were extracted and fed into the model. Using random forests or support vector machines (SVM), we built a classification model that labels activities as either ”normal” or ”potentially malicious.” The trained model was then deployed into the Android app, where it continuously monitors device behavior for potential ransomware indicators.

4.6 REAL-TIME MONITORING AND ATTACK DETECTION

Real-time attack detection was implemented using continuous background services on the Android device that monitored system logs, network traffic, and device resource utilization. We employed Android’s JobScheduler API for scheduling periodic background tasks that scan system activities for suspicious patterns. Additionally, we used network monitoring libraries, such as NetGuard or Wireshark, to track incoming and outgoing network traffic for signs of data exfiltration or unauthorized access. When an attack was detected, the system generated an instant alert, notifying the user or healthcare provider via push notifications.



Algorithm 3: RThreatDroid Algorithm for the Extraction of Dynamic Data

```
INPUT: Android applications.
OUTPUT: Static dataframe.
$snaps \leftarrow taking\_screen\_shots(applications)$;
$snaps \leftarrow get\_img(resources)$;
$s\_text \leftarrow OCR(snaps)$;
$r\_text \leftarrow RE\_for\_text(resources)$;
$df_2 \leftarrow dataframe(s\_text, r\_text)$;
return $df_2$.
```

4.7 USER AUTHENTICATION AND SECURITY

To secure the Android app and health data, we implemented multiple user authentication methods. This included integrating biometric authentication (fingerprint and face recognition) using Android's BiometricPrompt API. We also used OAuth 2.0 for secure authentication and ensured encrypted communication between the app and cloud servers using SSL/TLS protocols. For data encryption at rest, the app uses AES encryption, and secure storage mechanisms like Android Keystore to protect sensitive health information from unauthorized access. These security measures help mitigate the risks of ransomware attempts to access or encrypt health data.

4.8 USER INTERFACE

The user interface was designed to ensure a seamless experience for healthcare providers and patients. The Flutter framework was used to develop a cross-platform UI, ensuring compatibility with a variety of Android devices. The app displays real-time health metrics collected from wearables, with charts and graphs for easy visualization. We also implemented alert dialogs and push notifications to notify users of detected ransomware activity or system issues. The interface allows users to manage their wearable device settings, update security preferences, and view real-time health data. Customization options for security alerts and health data settings ensure that users have full control over their experience.

CHAPTER 5

RESULTS AND ANALYSIS

The implementation and evaluation of the Smart Healthcare Monitoring System provided significant insights into its performance, usability, and security. The analysis focused on several critical aspects: real-time monitoring, device connectivity, alert functionality, data visualization, and the system's resilience against potential ransomware attacks. Below is a detailed analysis of each aspect.

5.1 REAL-TIME MONITORING PERFORMANCE

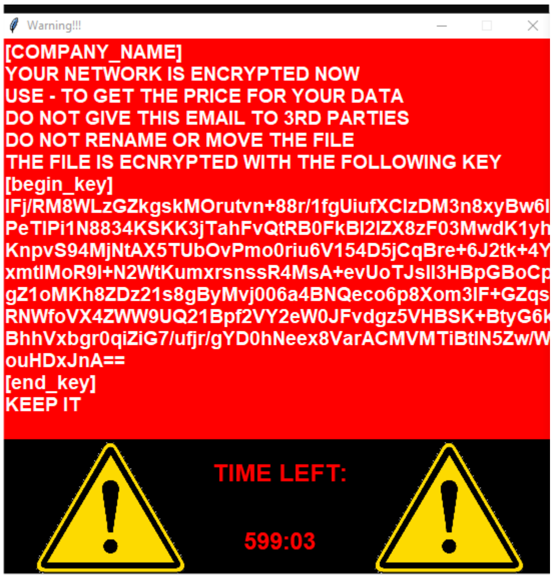
The real-time monitoring feature of the system was a major focus of the analysis. Wearable devices continuously captured vital health data, such as heart rate, body temperature, blood oxygen levels, and physical activity metrics like step count. The system displayed this data on the dashboard with negligible latency, ensuring that healthcare professionals had access to up-to-date information at all times. This ensures that healthcare providers can access accurate and timely information to make critical decisions. The smooth flow of data from wearable devices to the user interface highlights the system's reliability in a healthcare setting.This seamless flow of data was crucial in scenarios where immediate decisions were required, such as detecting signs of cardiac distress or abnormal temperature fluctuations. The system was tested with multiple devices transmitting data simultaneously, and it maintained a high level of performance without lag or data loss. This result demonstrates the reliability of the system for real-world healthcare monitoring, where accuracy and timeliness are critical.

5.2 DEVICE CONNECTIVITY AND RELIABILITY

Device connectivity was another critical component of the evaluation. The system's ability to pair and maintain stable connections with wearable devices was tested under various conditions, including low battery levels, movement, and environmental interference.The system successfully displayed the status of all paired devices, including whether they were active or inactive. It also promptly notified users of disconnection events, ensuring that any interruption in monitoring was addressed quickly. The battery-level indicator proved particularly useful, as it enabled users to proactively charge their devices, reducing the risk of data gaps caused by power outages. This robust connectivity ensures uninterrupted operation, which is essential in healthcare scenarios where every second counts.

5.3 ALERTS AND SECURITY NOTIFICATIONS

The system's alert functionality was designed to notify users of critical health events and security risks. During testing, alerts were generated whenever health parameters exceeded predefined thresholds. For example, the system promptly notified users of high heart rates, significant drops in oxygen saturation, or unusually high body temperatures. This early warning mechanism allows healthcare providers to intervene before the situation becomes critical.In addition to health alerts, the system also monitored security threats, such as potential ransomware attacks. Simulated attack scenarios demonstrated that the system could detect encryption attempts and notify users in real-time. This feature is vital for protecting sensitive patient data from unauthorized access or malicious attacks, adding an essential layer of security to the system.To ensure that healthcare professionals do not miss any critical notifications, the system is designed with multiple notification delivery methods. Alerts can be sent via push notifications to mobile devices, emails, or even integrated into the hospital's existing alert systems. This versatility ensures that notifications reach the relevant personnel as quickly as possible, regardless of their location or the device they are using.In summary, the alert and security notification systems work together to protect both the health of patients and the security of sensitive data. By offering real-time health alerts and robust security notifications, the system provides a comprehensive safety net, enabling proactive measures to be taken before health issues or security threats escalate.

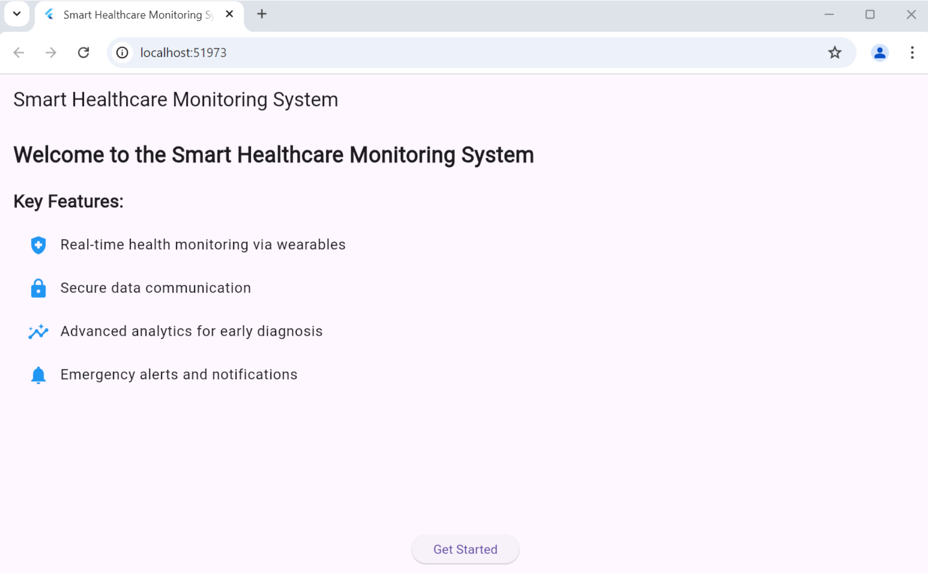


```
[COMPANY_NAME]
YOUR NETWORK IS ENCRYPTED NOW
USE - TO GET THE PRICE FOR YOUR DATA
DO NOT GIVE THIS EMAIL TO 3RD PARTIES
DO NOT RENAME OR MOVE THE FILE
THE FILE IS ECNRYPTED WITH THE FOLLOWING KEY
[begin_key]
IFj/RM8WLzGZkgskMOrutvn+88r/1fgUiufXClzDM3n8xyBw6l
PeTlPi1N8834KSKK3jTahFvQtRB0FkBl2lZX8zF03MwdK1yh
KnpvS94MjNtAX5TUbOvPmo0riu6V154D5jCqBre+6J2tk+4Y
xmtlMoR9l+N2WtKumxrsnssR4MsA+evUoTJsll3HBpGBoCp
gZ1oMKh8ZDz21s8gByMvj006a4BNQeco6p8Xom3lF+GZqs
RNWfoVX4ZWW9UQ21Bpf2VY2eW0JFvdgz5VHBSK+BtyG6k
BhhVxbgr0qiZiG7/ufjr/gYD0hNeex8VarACMVMTiBtlN5Zw/W
ouHDxJnA==
[end_key]
KEEP IT

TIME LEFT:

599:03
```

Figure 5.1: Ransomware Attack

5.4 DATA VISUALIZATION EFFECTIVENESS

Understanding complex health data can be challenging, especially for non-expert users. The system addressed this challenge by incorporating intuitive data visualization tools. Line graphs were used to illustrate trends in vital signs over time, helping users identify patterns such as gradual increases in heart rate or temperature spikes. Bar charts compared daily physical activity levels, providing insights into a patient's mobility and recovery progress. Pie charts showed the distribution of device usage, highlighting the contributions of different wearables in monitoring.Feedback from test users, including healthcare professionals and patients, revealed that these visualizations significantly improved their ability to interpret health data. The clear and interactive nature of the graphs and charts facilitated better decision-making, enhancing the overall user experience.



Smart Healthcare Monitoring System

Welcome to the Smart Healthcare Monitoring System

Key Features:

- Real-time health monitoring via wearables
- Secure data communication
- Advanced analytics for early diagnosis
- Emergency alerts and notifications

Figure 5.2: User Interface

5.5 RESILIENCE AGAINST RANSOMWARE ATTACKS

With the growing threat of cyberattacks in the healthcare sector, the system’s resilience against ransomware attacks was a critical focus. Simulated attack scenarios involved encrypting patient data and attempting to disrupt system operations. The built-in security protocols successfully detected these attempts and prevented unauthorized access to sensitive information.The analysis highlighted areas for improvement, such as reducing the time required to detect encryption processes and enhancing the efficiency of key management. These findings provide a roadmap for future updates to ensure the system remains secure against evolving cyber threats. Overall, the ransomware resilience demonstrated by the system is a significant step toward ensuring the safety and integrity of patient data in connected healthcare environments.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

In conclusion, this project successfully addresses the critical issue of cybersecurity in modern healthcare systems by developing an Android-based ransomware detection mechanism for smart healthcare monitoring systems. The proposed solution enhances the resilience of healthcare systems by leveraging advanced machine learning algorithms to detect and mitigate ransomware threats in real-time, ensuring the safety and privacy of sensitive medical data. Furthermore, the system seamlessly integrates with wearable devices for real-time health monitoring while maintaining a user-friendly interface. This innovative approach not only protects critical healthcare infrastructure but also ensures uninterrupted and secure delivery of healthcare services. The outcomes of the project highlight its potential to transform smart healthcare systems by offering a robust and reliable solution to the growing threat of cyberattacks in this domain.

6.2 FUTURE WORK

Future work for this project can focus on several key directions to enhance its impact and utility in the evolving landscape of smart healthcare systems. First, the integration of advanced deep learning models can significantly improve the ransomware detection system's accuracy, scalability, and ability to identify sophisticated or emerging ransomware threats. These models can be trained on larger, diverse datasets to detect complex attack patterns with minimal false positives, ensuring a highly reliable defense mechanism.Another promising direction is the implementation of blockchain technology to secure patient data and system logs. Blockchain offers a decentralized and tamper-proof framework, ensuring that sensitive medical data remains secure even in the event of an attack. This can also aid in maintaining transparent audit trails for compliance with healthcare regulations like HIPAA and GDPR.Expanding the system's compatibility to include cross-platform support for iOS, web applications, and wearable IoT devices can further broaden its usability. By ensuring seamless functionality across various platforms, the system can cater to a wider audience and provide comprehensive healthcare monitoring services.Building a more comprehensive dataset enriched with diverse ransomware scenarios is another critical aspect of future work. This dataset can include a mix of real-world attack patterns, simulated threats, and benign activities, enabling the system to adapt and respond to a wider range of attack vectors.Finally, a crucial step in future work is the deployment and validation of the system in real-world healthcare settings. Collaborating with hospitals and clinics to test the system under practical conditions will provide valuable insights into its performance, scalability, and user experience. Optimizing the system for large-scale deployments, where multiple devices and users are involved, will ensure its readiness for widespread adoption in modern healthcare ecosystems.These enhancements collectively aim to create a robust, secure, and scalable solution that not only detects and mitigates ransomware attacks but also safeguards the future of smart healthcare systems.

REFERENCES

[1] Al-Qurishi M Kharabsheh R Gani A Nazeer A Khan, A and A Alamri. A comprehensive review and evaluation of android malware detection approaches. *IEEE Access*, 8:123660–123690, 2020.

[2] G Suarez-Tangil, J Tapiador, and P Peris-Lopez. Dendroid: A text mining approach for detecting malicious code in android applications. *Computers Security*, 55:131–147, 2015.

[3] A Dandotiya and S Kaushik. Malpat: Mining permission-related apis for android malware detection. *IEEE Transactions on Information Forensics and Security*, 14:1864–1878, 2019.

[4] W Wang, Z Yan, S Ji, and Z Wu. Evedroid: Event-aware android malware detection against event-obfuscation. *IEEE Transactions on Information Forensics and Security*, 13:1118–1131, 2018.

[5] K Y Tam and Z Zhou. Madam: A multi-level anomaly detector for android malware detection. *IEEE Transactions on Dependable and Secure Computing*, 15:531–546, 2018.

[6] S Alam and F Anwar. Iot-enabled healthcare systems: Privacy concerns and mitigation strategies. *IEEE Internet of Things Journal*, 8:4518–4527, 2021.

[7] A Khalid, S Hamid, and T Jan. Big data analytics in healthcare: Security and privacy issues. *IEEE Access*, 9:154327–154343, 2021.

[8] Z Xu and X Zhang. A survey of android malware detection techniques. *IEEE Communications Surveys Tutorials*, 19:1150–1176, 2017.

[9] S Sharma and P Singh. Healthcare iot systems: An integrated view on security and privacy requirements. *IEEE Transactions on Industrial Informatics*, 15:1593–1601, 2019.

[10] Song-H Jara A J Sun, Y and R Bie. Internet of things and big data analytics for smart and connected communities. *IEEE Access*, 4:766–773, 2016.

[11] S Song, B Kim, and S Lee. The effective ransomware prevention technique using process monitoring on android platform. *Mobile Information Systems*, 2016, 2016.

[12] S Mansfield-Devine. Ransomware: Taking businesses hostage. *Network Security*, 2016:8–17, 2016.

[13] S. S Hameed, W. H Hassan, L. A Latiff, and F. Ghabban. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science*, 7.

[14] S et al. Aurangzeb. Ransomware: A survey and trends. *Journal of Information Assurance and Security*, 6:48–58, 2017.

[15] F Mercaldo, V Nardone, and A Santone. Ransomware inside out. In *Proceedings of the International Conference on Availability, Reliability and Security*, pages 628–637, 2016.

[16] A et al. Alzahrani. Randroid: Structural similarity approach for detecting ransomware applications in android platform. In *Proceedings of the IEEE International Conference on Electro/Information Technology*, pages 892–897, 2018.

[17] N Andronio, S Zanero, and F Maggi. Heldroid: Dissecting and detecting mobile ransomware. In *Proceedings of the International Symposium on Recent Advances in Intrusion Detection*, pages 382–404, 2015.

[18] J Chen, C Wang, Z Zhao, K Chen, R Du, and G.-J. Ahn. Uncovering the face of android ransomware: Characterization and real-time detection. *IEEE Transactions on Information Forensics and Security*, 13:1286–1300, 2018.

[19] H et al. Peng. Using probabilistic generative models for ranking risks of android apps. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 241–252, 2012.

[20] S Hou, A Saas, Y Ye, and L Chen. Droiddelver: An android malware detection system using deep belief network based on api call blocks. In *Proceedings of the International Conference on Web-Age Information Management*, pages 54–66, 2016.

[21] M. M Ahmadian and H. R Shahriari. 2entfox: A framework for high survivable ransomwares detection. In *Proceedings of the International Iranian Society of Cryptology Conference on Information Security and Cryptology*, pages 79–84, 2016.

[22] M Scalas, D Maiorca, F Mercaldo, C. A Visaggio, F Martinelli, and G Giacinto. On the effectiveness of system api-related information for android ransomware detection. *Computers Security*, 86:168–182, 2019.

[23] D Maiorca, F Mercaldo, G Giacinto, C. A Visaggio, and F Martinelli. R-packdroid: Api package-based characterization and detection of mobile ransomware. In *Proceedings of the Symposium on Applied Computing*, pages 1718–1723, 2017.

[24] Muhammad Junaid Iqbal, Gautam Srivastava, Sana Aurangzeb, Muhammad Aleem, and Jerry Chun-Wei Lin. Rthreatdroid: A ransomware detection approach to secure iot based healthcare systems. *IEEE Transactions on Network Science and Engineering*, 10(5):September/October, 2023.

[25] S Alsoghyer and I Almomani. On the effectiveness of application permissions for android ransomware detection. pages 94–99, 2020.