VALLEY VIEW UNIVERSITY

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE BACHELOR OF SCIENCE (BSC.) IN INFORMATION TECHNOLOGY DEGREE

TOPIC:

ANALYSIS OF SECURITY VULNERABILITIES IN MOBILE APPLICATIONS

BY:

KWAKU TIEKU-DADEY
B203210032

SUPERVISOR:

DR. SETH ALORNYO

OCTOBER 2023

DECLARATION

This is to declare that, the research work underlying this senior research project has been carried out by the under-mentioned student under the supervisor. Both the student and the supervisor certify that the work documented in this thesis is the output of the research conducted by the student as part of his final year project work in partial fulfillment of the requirement of the Bachelor of Science in Information Technology degree.

STUDENT:	**SUPERVISOR:**
Kwaku Tieku-Dadey	Dr. Seth Alornyo
---------------------	---------------------
DATE: 7/11/2023	DATE: 29/11/2023

ACKNOWLEDGEMENT

My sincerest gratitude goes to God for granting me success in this project. I would also like to express my profound gratitude to my supervisor, Dr. Seth Alornyo for his relentless assistance given me in this project.

Also, I am most grateful for the support I received from my family and the Ghana Scholarship Fund Inc. for funding my education.

ABSTRACT

In light of a rapid digital evolution, Ghana has experienced an unprecedented digital device adoption. With an estimated market share of 75.82%, the Android OS dominates the country's digital landscape. This research investigates security and data privacy compliance in mobile applications in Ghana’s digital landscape. The study reveals that certain applications lack compliance with privacy policy regulations, while others are susceptible to security breaches due to coding practices. Furthermore, the study identifies from network communication protocol analysis that majority of the tested applications utilize modern version of Transport Layer Security (TLS) and TLS cipher suites for data transmission.

Keywords: Security, Vulnerability, Privacy Policy, Android.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

1.0 Introduction and Opportunity Statement

In recent years, Ghana has experienced a remarkable and transformative shift towards a digitally-driven society. This phenomenon is further supported by the concept that digitalization is the widespread adoption of connected digital technologies and applications by consumers, businesses, and governments [1].

Having established itself as one of the rapidly developing economies in West Africa, the country has harnessed the power of technology to enhance various sectors, leading to an unprecedented increase in digital infrastructure and the widespread adoption of web and mobile applications. This dynamic progression has brought about numerous opportunities for economic growth, improved service delivery, and increased connectivity among its citizens.

The embrace of digital technologies in Ghana has been largely driven by the government of Ghana’s initiative, including introducing a digital governance strategy in 2005 and the Information and Communication Technology for Accelerated Development (ICT4AD) Policy 2017 [2]. The initiative has led to a rapid expansion of internet connectivity and the ever-increasing accessibility of smartphones, computers, and other technologies. With the proliferation of affordable mobile devices and the deployment of fiber-optic cables, the country's internet penetration has soared, enabling more Ghanaians to access the digital realm. Consequently, this heightened connectivity has fostered the creation and use of web and mobile applications, catering to a myriad of needs, from e-commerce and online banking to social networking and government services.

The strive to achieve a modern and digitized country has increased partly through the involvement of private technology-based organizations and investors in the country as in [1] . These days businesses have widely adopted the use of mobile and web applications to foster transactions which have been massively influenced by the introduction of mobile money interoperability systems. Some of these common services include mobile money payment applications, e-commerce, banking, and finance.

As the nation strides confidently toward the digital frontier, it is essential to acknowledge the immense potential these advancements bring while being conscious of the challenges they introduce. As the use of these digital platforms to complete services significantly grows, there are data privacy concerns regarding personally identifiable information (PII).

One of the paramount concerns that arise in this digital evolution is the aspect of cybersecurity. With the exponential growth in the use of web and mobile applications and other digital services, there comes a corresponding increase in data privacy concerns, and security vulnerabilities that malicious actors could exploit. The implications of these vulnerabilities can be far-reaching, encompassing compromised personally identifiable information, financial fraud, and even threats to national security.

Hence, this thesis embarks on a comprehensive analysis of Ghana's digital infrastructure, with a specific focus on analyzing the security vulnerabilities prevalent in select widely used mobile applications developed for the Android operating system. By thoroughly examining the current landscape of digital technologies in Ghana, we seek to identify potential weaknesses that may undermine the integrity, confidentiality, and availability of these essential systems while also highlighting issues related to personally identifiable information. Moreover, our investigation aims to shed light on the practices and measures that can be implemented to bolster the security posture of these applications and safeguard the interests of individuals, businesses, and government entities alike.

Through a thorough analysis of case studies, industry best practices, and expert insights, this research endeavors to contribute valuable knowledge to Ghana's ongoing journey into the digital age. The findings and recommendations presented in this research will empower public and private sector stakeholders to make informed decisions, invest in robust cybersecurity measures, and foster a landscape that nurtures data privacy compliance, innovation, and sustainable growth in the digital realm.

1.1 Subject and Field of Study

The subject of this thesis is a comprehensive survey of digital infrastructure in Ghana, with a specific focus on analyzing security vulnerabilities and data privacy concerns in widely used Android-based mobile applications in Ghana.

The field of study encompasses the ever-expanding landscape of digital technologies and the challenges posed by potential cybersecurity threats. As Ghana experiences a shift towards digitization and an increased reliance on web and mobile applications, understanding the security risks associated with these technologies becomes crucial for ensuring a safe and sustainable digital environment.

1.2 Study Objectives

1.2.1 Global (General) Objectives

The primary objective of this research is to conduct a thorough analysis of the digital infrastructure in Ghana and identify prevalent security vulnerabilities in widely used mobile applications with a focus on Android-based applications only. By achieving this objective, we aim to contribute to the enhancement of cybersecurity measures, ensure data privacy compliance, and foster a resilient digital landscape in the country.

1.2.2 Specific Objectives

The specific objectives of this study are as follows:

i. Identify common security vulnerabilities in commonly used Android mobile applications in Ghana.

ii. Evaluate privacy policy in mobile applications to ensure adherence to data protection regulations.

iii. Propose actionable recommendations and best practices for enhancing the security posture of mobile applications used in Ghana, considering both technical and policy aspects.

1.3 Background to the Study

The digital transformation in Ghana has been propelled by the steady growth of internet connectivity and the widespread adoption of technology including computers and smartphones. This evolution has led to an upsurge in the development and usage of web and mobile applications, serving diverse purposes across sectors. However, as technology advances, so do cyber threats. The background of this study is rooted in the need to understand the opportunities and challenges presented by Ghana's digital infrastructure evolution, particularly in terms of cybersecurity, to safeguard the country's digital progress.

1.4 Scope of the Study

This research investigates the digital infrastructure in Ghana, with a focus on analyzing potential security vulnerabilities, and data privacy compliance in selected widely used mobile applications developed for the Android operating system

Although the broader digital ecosystem may involve other technologies such as web applications, this thesis will primarily concentrate on mobile applications developed for Android Operating System due to their ubiquitous nature and the patronage rate in Ghana.

1.5 Significance of Study

The significance of this study lies in its potential to contribute invaluable insights to the growing domain of cybersecurity in Ghana while bringing awareness to other countries. As the country embraces digitalization, the prevalence of mobile applications raises concerns about potential security vulnerabilities that can jeopardize personal privacy, economic stability, and national security. By thoroughly investigating these vulnerabilities and data privacy concerns, and proposing robust solutions, this research aims to:

i. Perform security analysis of widely used Android applications in Ghana.

ii. Highlight modern industry standards related to security in mobile application development and deployment.

iii. Enable businesses and software engineers to adopt best practices and implement secure coding techniques to safeguard their users' data.

iv. Raise cybersecurity awareness and assist policymakers and regulatory bodies in formulating effective strategies to mitigate security risks and protect citizens and businesses.

1.5.1 Limitations to the Study

i. **Time constraints:** The university's academic schedule will restrict this study. The time allocated for this project will not allow for thorough study and a large number of applications.

ii. **Legal Permit:** Legal consent from stakeholders will be necessary before conducting security testing for certain applications. Therefore, the testing will be restricted to a limited sample based on the inclusion criteria.

1.6 Methodology

In this research, a sample of mobile applications will be analyzed using mobile application security testing tools to assess their security and data privacy compliance. The analysis will focus on applications running on the Android operating system, which is known to have the largest user base in Ghana as seen in [3] . The sample will be analyzed using static and dynamic analysis methods, to provide comprehensive insights. The applications will be selected based on the criteria outlined in the following table.

Table 1.0 Application selection criteria

Criteria	Requirements
I	The application is free to download and use.
II	The application requires data input, and stores, and transmits personal data.
III	Application has at least 1,000 downloads on the Play Store

1.7 Expected Results of the Study

The following are the expected outcomes of this study:

1. Comprehensive evaluation report on widespread security vulnerabilities in mobile applications and data privacy compliance.
2. Recommendations and best practices for improving the security posture of Ghana's mobile application ecosystem.

The research deliverables are expected to be beneficial in various ways:

I. It will serve as a knowledge repository for academics, researchers, and policymakers interested in understanding Ghana’s cybersecurity ecosystem.

II. The findings may be used by policymakers and regulatory organizations to develop effective cybersecurity policies and laws.

III. Businesses and application developers can utilize the recommendations to safeguard their users and digital assets.

IV. General users can become more aware of potential security risks and adopt safer practices when using web and mobile applications.

1.8 Presentation of Project

The research will be structured into 8 chapters as follows:

Chapter 1: Introduction – Establishes the background, introducing the topic, highlighting Ghana's digital drift, and the rise in smartphone and computer usage. Chapter One outlines the objectives of the study, and its significance and provides an overview of the research methodology.
Chapter 2: Literature Review – Presents a comprehensive review of existing literature and research related to cybersecurity, digital infrastructure, mobile application security standards, and data privacy and protection compliance regulations relevant to the Ghanaian context.

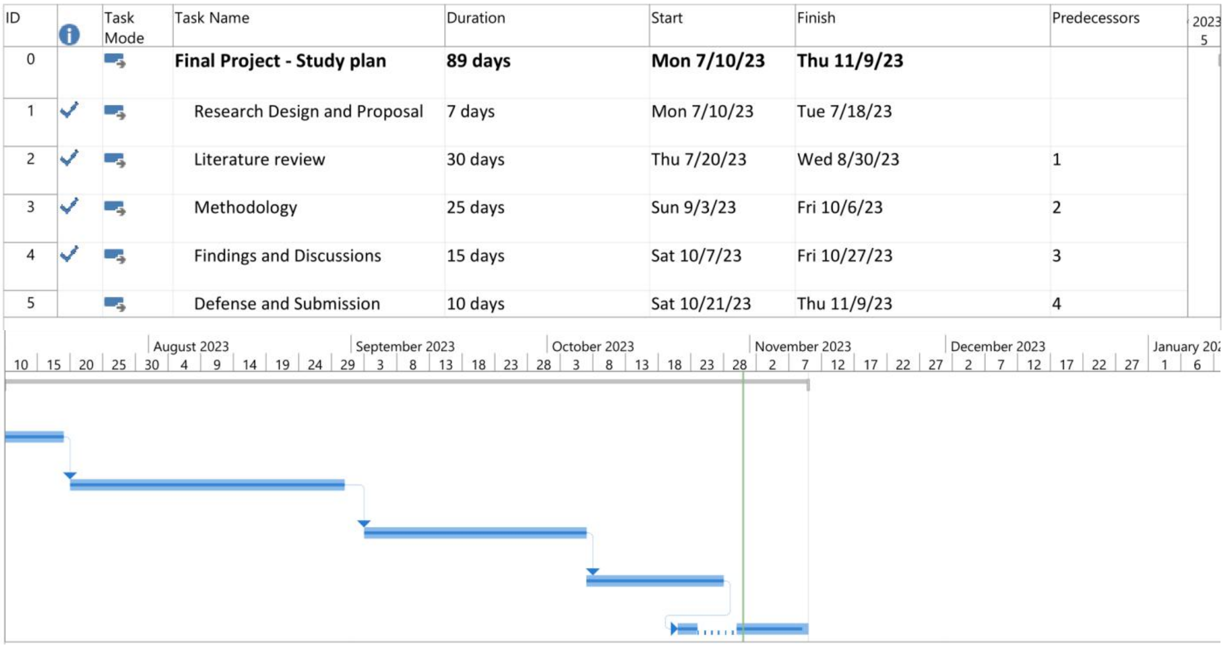
Chapter 3: Research Methodology – Expounds on the underlying process, methods, and tools used in carrying out the study. This chapter highlights the technical details of the research and how comprehensive insights will be drawn from the study sample.

Chapter 4: Findings and Discussions – Emphasizes the key findings resulting from the data analysis conducted in the research. This chapter offers a comprehensive analysis of the data collected and interprets the findings.

Chapter 5: Conclusion and Recommendations – Drawing from the preceding chapters, this section provides a concise summary of the study’s findings while also, proposing actionable recommendations and best practices. In addition, the chapter discusses the implications and potential future developments in Ghana's digital infrastructure landscape.

1.9 Study Work Plan (Timelines)

The following chart illustrates the work plan of the project expressed in days with the start date of each task.



ID	ℹ	Task Mode	Task Name	Duration	Start	Finish	Predecessors
0			**Final Project - Study plan**	**89 days**	**Mon 7/10/23**	**Thu 11/9/23**	
1	✓		Research Design and Proposal	7 days	Mon 7/10/23	Tue 7/18/23	
2	✓		Literature review	30 days	Thu 7/20/23	Wed 8/30/23	1
3	✓		Methodology	25 days	Sun 9/3/23	Fri 10/6/23	2
4	✓		Findings and Discussions	15 days	Sat 10/7/23	Fri 10/27/23	3
5			Defense and Submission	10 days	Sat 10/21/23	Thu 11/9/23	4

Figure 1.0 Study Work Plan

CHAPTER TWO

LITERATURE REVIEW

The digital evolution has catalyzed remarkable transformations across various societies worldwide, with Ghana being no exception. As one of the growing economies in West Africa, Ghana has witnessed a dynamic evolution in its digital landscape, experiencing an unprecedented surge in technological advancements and digital infrastructure. The extensive adoption and use of mobile applications by businesses in various sectors such as E-commerce, Banking and Finance, Health, and Entertainment has provided clients with convenient access to digital services. However, with this widespread use of mobile applications, there are growing concerns about how the respective providers have implemented data security and privacy in their mobile applications.

This chapter explores the literature, theories, and studies that are relevant to this study and sheds light on the interconnections between mobile application security, data privacy, and user protection in the Ghanaian context.

2.0 Digital Evolution in Ghana

Globally, economies thrive as they embrace digital technologies, revolutionizing communication and transactions. According to [4], Ghana has experienced significant technological advancements, particularly in internet access and usage, with 80% of the youth (ages 15-29), 49% of children (ages 6-14), and 64% of the elderly (ages 41 and above) benefiting from this trend. Financial Technology (FinTech), also sees robust adoption at approximately 67%. These improvements are attributed to the country's expansion of 3G and 4G networks.

Furthermore, [5] highlights in a report a remarkable 99.3% ownership rate of smartphones in Ghana, solidifying the country's position with the highest mobile penetration in West Africa, as confirmed by [6].

Regarding mobile operating systems, the Android OS holds a dominant market share of approximately 75.82% surpassing other vendors in the country [3].

Ghana's technology ecosystem has rapidly flourished, which is largely driven by government initiatives like digitizing citizen services and expanding communication and internet access. Additionally, the private sector, especially technology companies in both retail and service delivery, has played a significant role in this development.

While Ghana's digital ecosystem presents immense opportunities for businesses and individuals in service delivery and access, the rapid expansion also raises concerns about data security and privacy. Hence, it becomes imperative for businesses, especially those delivering services through digital means like mobile applications, to reevaluate data security implementations and ensure data privacy compliance to safeguard their clients' information and maintain trust in their digital services.

2.1 Mobile Applications

A mobile application, also commonly referred mobile app, is a software program designed to run on mobile devices. According to OWASP, a mobile application is a standalone computer program designed to execute on mobile devices.

Mobile applications have emerged as one of the most significant innovations in smartphone usage. [7] reports that there are around 3.55 million applications on the Google Play Store and 1.6 million applications on the Apple Store. These statistics represent growth in the mobile applications ecosystem. Mobile applications are platform-specific and hence require that vendors develop applications for all the platforms. The statistics show that the Android Operating system receives the largest share of the mobile application distribution and also has the largest user base.

In the subsequent sections of this chapter, we will explore the defining characteristics that categorize an app within the mobile application taxonomy. Additionally, we will delve into the distinctions between each variation, thoroughly examining security in mobile applications and the corresponding threats they may encounter.

2.1.1 Types of Mobile Applications

Mobile applications for various mobile operating systems are broadly categorized into native, web-based, hybrid, and progressive web applications:

2.1.1.1 Native Mobile Applications

Native mobile applications are specifically designed to operate on a particular mobile platform. Creating mobile apps for a specific operating system allows for optimal performance by utilizing the resources of that system. These apps are typically developed using platform-specific tools and languages and are distributed to users through application stores.

2.1.1.2 Web-based Mobile Applications

Web-based applications are built into a native mobile framework and leverage the cross-compatibility offered by standard web technologies such as HTML, CSS, and JavaScript. These applications require an internet connection to deliver their services. Web-based applications enjoy the ease of deployment unlike native apps that require distribution through digital marketplaces, web-based apps can be accessed directly through a web browser. Web-based apps are generally considered lightweight because they do not consume large space on the user’s device and also ensure faster loading times and reduce the need for frequent updates as changes made to the central application are instantly reflected across all platforms.

2.1.1.3 Hybrid Mobile Applications

Hybrid mobile applications seamlessly combine the features of native and web-based apps. They are built to support web and native technologies across multiple platforms, offering a flexible and versatile solution. Hybrid mobile applications have an underlying embedded web browser – WebView. This underlying component facilitates the incorporation of web technologies that provide web support for the entire application while also leveraging native features to enhance the user experience.

2.1.1.4 Progressive Web Applications

To achieve cross-platform compatibility of applications for both Android and iOS, Progressive Web Applications offers a revolutionary approach that blends the capabilities of web technologies with the functionality of native applications. Progressive web applications (PWA) are built using web platform technologies and provide a user experience like that of a platform-specific app [8].

Modern web technologies like HTML, CSS, and JavaScript are used by progressive web applications to produce responsive, immersive user interfaces that closely mirror those of native apps. To seamlessly adapt to different screen sizes and devices, they make use of technologies like the service worker API to provide offline access, push notifications for real-time updates, and responsive design. The ability of progressive web applications to avoid conventional digital marketplaces and be accessed directly through web browsers is a significant benefit. As a result, there is no longer a need for separate app installations and upgrades, streamlining the user experience and lowering the barrier to usage.

2.2 Security in Mobile Applications

Across all mobile operating systems, security in mobile applications is a complex issue that requires attention. Android OS and iOS, in particular, face increased security concerns as a result of their large user bases and approximately 99% market share, respectively [7].

The core of mobile application security is the use of security technology to defend applications against potential risks and threats. This involves the detection and removal of vulnerabilities both before and after the deployment of the application. The goal is to create an environment that is stable and secure for mobile applications, protecting user data and privacy while reducing the dangers brought on by cyber threats.

The importance of mobile application security, according to [9], is a result of the widespread adoption of these systems by businesses, which makes them appealing targets for possible data breaches. The usage patterns and communication methods used by mobile applications to interact with users are linked to several attacks. These applications communicate through various services, expanding their attack surface considerably. Some of the communication services utilized by these applications include Bluetooth, SMS, Microphone, Camera, and Near Field Communication (NFC). Moreover, [10] highlight that mobile applications face significant security challenges, including the use of untrusted or insecure networks including public Wi-Fi, mobile hotspots, and cellular connections. There are also risks associated with device loss or theft, and malware distribution through unofficial digital marketplaces. To protect user data and privacy from these vulnerabilities, thorough analysis and strong defense measures are required.

According to [11] , combining multiple security measures can enhance the overall protection offered by the mobile application. Mobile application security comprises a variety of crucial techniques. These methods consist of:

i. **Code hardening:** Utilizing obfuscation and encryption to safeguard the application’s source code and sensitive data from unauthorized access, providing a defense against static analysis.

ii. **Runtime application self-protection (RASP):** Implementing measures to detect and counter dynamic analysis in real-time, adding an extra layer of defense during the application's execution.

iii. **Mobile application security testing:** Conduct thorough assessments to identify and address potential security vulnerabilities, ensuring the application undergoes rigorous scrutiny before deployment.

iv. **Threat monitoring:** Monitoring and analyzing the mobile security landscape to swiftly identify and respond to emerging threats, enabling proactive measures to be taken to safeguard the application and its users.

Furthermore, as mentioned by [9] , mobile device security goes beyond just ensuring that programs are executed securely on the devices but also includes safeguarding residual data and data in transit. Data-related security challenges typically exist at multiple layers:

Network layer: Data traveling from mobile applications over Wi-Fi and data services are susceptible to potential security breaches

Hardware layer: Mobile devices are vulnerable to baseband attacks, broadband attacks, and RF range attacks that can impact their features.

Operating system layer: Mobile platforms may face vulnerabilities related to jailbreaking or rooting, posing security risks.

Application layer: The Application Program Interface of the device without administrative permissions may lack adequate security measures.

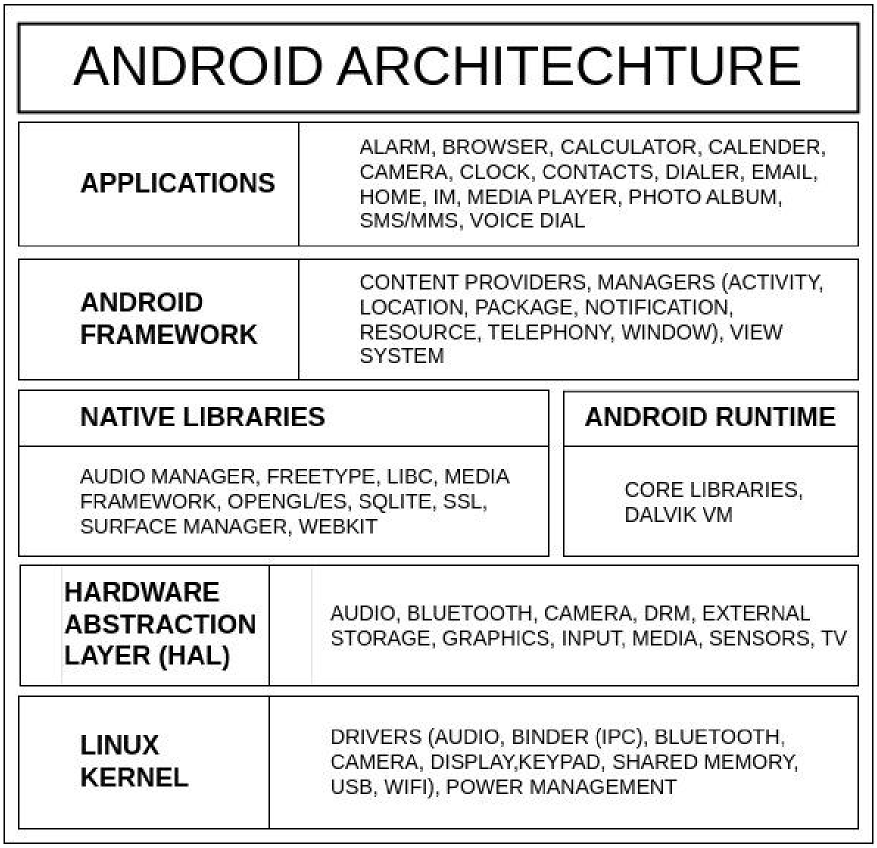
2.3 Security in Mobile Operating Systems

2.3.1 Security in Android OS

Android is a mobile operating system developed and managed by Google and the developer consortium, Open Handset Alliance. It is based on the Linux Kernel and is typically programmed in Java. The Android OS presents an open-source code without restrictive licenses or fees for developers to modify its code [12].

The Linux Kernel serves as a foundation for the security implementation methodology within the Android OS. Similar to the Unix UID, a unique user identity (UID) is assigned to each application upon installation. The kernel controls access to files, devices, and other resources using this UID. Applications are identified by their allocated UID, which is also used to share data with other applications. Additionally, an AndroidManifest.xml file defines the access permissions for system resources. Typically, applications need the owner's consent to perform certain functions.

To secure various components of the Android software stack, Android OS uses abstraction. Unless explicit access permissions are explicitly granted by the user during installation, applications only run in a sandbox, an isolated section of the system [13]. This layered security strategy in Android ensures a robust and controlled environment for mobile applications, safeguarding user data and system integrity.



ANDROID ARCHITECHTURE

APPLICATIONS: ALARM, BROWSER, CALCULATOR, CALENDER, CAMERA, CLOCK, CONTACTS, DIALER, EMAIL, HOME, IM, MEDIA PLAYER, PHOTO ALBUM, SMS/MMS, VOICE DIAL

ANDROID FRAMEWORK: CONTENT PROVIDERS, MANAGERS (ACTIVITY, LOCATION, PACKAGE, NOTIFICATION, RESOURCE, TELEPHONY, WINDOW), VIEW SYSTEM

NATIVE LIBRARIES: AUDIO MANAGER, FREETYPE, LIBC, MEDIA FRAMEWORK, OPENGL/ES, SQLITE, SSL, SURFACE MANAGER, WEBKIT

ANDROID RUNTIME: CORE LIBRARIES, DALVIK VM

HARDWARE ABSTRACTION LAYER (HAL): AUDIO, BLUETOOTH, CAMERA, DRM, EXTERNAL STORAGE, GRAPHICS, INPUT, MEDIA, SENSORS, TV

LINUX KERNEL: DRIVERS (AUDIO, BINDER (IPC), BLUETOOTH, CAMERA, DISPLAY,KEYPAD, SHARED MEMORY, USB, WIFI), POWER MANAGEMENT

Figure 2.0 Android software architecture (source: [14])

2.3.2 Security in iPhone OS

iOS is Apple’s mobile operating system for its range of mobile devices. With some of the operating system's components made available as open source, it is proprietary software created in Swift and was historically mostly created in Objective C based on the traditional C language. Given that it hosts a large number of mobile applications, the iOS platform offers a wide attack surface. To address security concerns, iOS employs a combination of multiple security technologies at different levels of the operating system, ensuring comprehensive protection. These measures include:

2.3.2.1 Secure boot chain

The secure boot chain is the process of initializing and loading firmware on iOS devices at boot time, serving as the first layer of defense for platform security. Before booting into iOS, a low-level code runs from the Boot ROM, verifying the bootloader's signature by the Apple Root Certificate Authority (CA) public key. This ensures no malicious or unauthorized software can run on the device. After completing its tasks, the low-level bootloader runs the higher-level bootloader, iBoot, which loads the iOS kernel and the operating system [10] and[15].

2.3.2.2 Code signing

Code signing is a runtime security feature that verifies the application signature each time it is executed, improving platform security. It ensures only legitimate programs can operate on a device, and any attempt to execute unsigned code in memory is rejected by the kernel. Apple provides a provisioning profile for developers to install these certificates, which include a developer certificate and application rights. During the production phase, all code must be signed by Apple through the App Store submission procedure, granting control over software, developer APIs, and other features. This process prevents unwanted updates and establishes a chain of trust from Secure Boot to the user-installed application on the device, further strengthening the overall security of the iOS platform [15].

2.3.2.3 Process-level sandboxing

In iOS, third-party programs run in a process-level sandbox, which limits the data they can change to their home directories unless specific permission is given for extra actions. This sandbox establishes a self-contained environment that isolates applications from the operating system and from one another, significantly enhancing platform security and reducing the potential harm brought on by malware [10].

Additionally, iOS provides a wide range of privacy controls that let users decide which permissions programs have access to, including the camera, contacts, background application refresh, and cellular data, among others. To keep essential system files and other iOS resources hidden and inaccessible to user-installed programs, applications typically operate with permissions for mobile operating system users without root administrative privileges [15].

2.3.2.4 Data-at-rest encryption

iOS uses data-at-rest encryption to protect data using the Advanced Encryption Standard (AES) block-based encryption. This is achieved through a file system key generated during system boot and stored in flash storage. The file system is encrypted at rest, and the hardware-based cryptographic accelerator unlocks the file system upon device activation.

Also, iOS uses Data Protection API to enhance data security by enabling encryption of specific files and key-chain items. Because of this, files are encrypted with the API and are unavailable when the device is locked. This API allows third-party applications to encrypt data, providing a comprehensive approach to data protection on iOS devices.

2.3.2.5 Generic native language exploit mitigations

The iOS platform employs advanced exploit mitigation techniques to make device attacks more difficult. One such technique is the write but not execute memory policy, which prevents writable and executable memory pages from being changed back to executable status. It ensures that memory pages cannot be both writable and executable at the same time. This policy is similar to other systems' Data Execution Protection (DEP) features. The complexity of exploitation is further heightened by mandatory code signing, Address Space Layout Randomization (ASLR), and non-executable memory protections. ASLR randomizes the mapping of data and code in a process's address space, limiting the ability to exploit memory corruption issues by randomizing code locations. This makes it challenging for techniques like return-oriented programming (ROP) to evade non-executable memory safeguards.

2.4 Mobile Application Vulnerabilities

Digital stores like the Apple App Store and Google Play Store distribute mobile applications to users. While platform suppliers inspect these applications for security compliance, some can evade inspection and pose threats to users. Unauthorized distribution channels can spread dangerous apps, and users may receive modified versions to avoid subscription fees or custom-improved app features. Applications distributed via digital marketplaces may not be identified as malicious during vetting, but they may have underlying security weaknesses beyond malicious code. Mobile application development patterns often create vulnerabilities that adversaries can exploit for various attacks. Risks to mobile applications more often involve rogue code or malfunctioning applications, rather than viruses, which are often missed by antivirus software.

2.4.1 OWASP Mobile Application Vulnerabilities

The Open Worldwide Application Security Project (OWASP), a nonprofit organization dedicated to improving software security, finds that specific vulnerabilities are frequent in mobile applications. According to OWASP security surveys, these vulnerabilities compromise both the hardware of the device and user data.

Annual security surveys are released by OWASP to highlight the top 10 security flaws in both web and mobile applications. To ensure security implementation, the report informs software developers and businesses about the many types of vulnerabilities.

The top 10 vulnerabilities that are frequently found in mobile applications are listed in the OWASP 2023 report and are briefly described below:

Table 2.0 Summary of OWASP's 2023 top 10 mobile security risks.

OWASP Top 10 Mobile Risks		
SERIAL	VULNERABILITY	DESCRIPTION
M1	Improper Credential Usage.	**Threat agent:** **Application specific;** Threat agents might identify and exploit hardcoded

		credentials or exploit weaknesses due to improper credential usage. **Attack Vector:** • Acquire and employ hardcoded credentials to attain unauthorized access to sensitive information
M2	**Inadequate Supply Chain Security.**	**Threat Agent:** **Application specific;** Attackers modify the application codebase to insert backdoors. **Attack Vectors:** • Malicious code injection during app development • Using compromised app signing keys • Exploitation of vulnerabilities in third-party libraries utilized by the app.
M3	**Insecure Authentication/Authorization.**	**Threat Agents:** **Application Specific** – Threat agents exploiting vulnerabilities in authentication and authorization typically tend to utilize automated attacks employing specialized tools available. **Attack Vectors:** • They might employ fake or bypass authentication by submitting service requests to the app's backend server, bypassing direct interaction with the mobile app.

		• Alternatively, they could log into the app as a legitimate user after authentication, and then navigate to a vulnerable endpoint to execute administrative functionalities.
M4	**Insufficient Input/Output Validation**	**Threat agents:** **Application specific;** Attackers target exploiting vulnerabilities within mobile applications including SQL injection, Command Injection, and cross-site scripting (XSS) **Attack Vector:** • SQL Injection • Cross-site scripting (XSS) • Command injection • Path traversal
M5	**Insecure Communication.**	**Threat Agents:** • Malware on a mobile device • Rogue carrier or network devices • Adversary shares local network (compromised or monitored Wi-Fi) **Attack Vectors:** • Deprecated protocols or improper configurations • Acceptance of invalid or bad Secure Sockets Layer (SSL) certificates. • Inconsistent deployment of SSL/TLS protocols
M6	**Inadequate Privacy Controls**	**Threat Agents:** **Application specific;** Attackers have the potential to mimic the victim's identity

		to engage in fraudulent activities, exploit the victim's data for improper purposes, or use sensitive information for extortion **Attack Vectors:** • Eavesdrop on the network communication. • Employ trojans to gain access to the file system, clipboard, or logs. • Retrieve the device and create a backup for further analysis.
M7	Insufficient Binary Protections	**Threat agents:** **Application specific;** Attackers target commercial API keys or cryptographic secrets embedded within the code. **Attack Vectors:** • Reverse engineering • Code tampering
M8	Security Misconfiguration	**Threat agents:** **Application specific;** Attackers with physical device access or leveraging malicious applications on the device. **Attack Vectors:** • Insecure default settings • Weak encryption or hashing • Lack of secure communication • Unprotected storage
M9	Insecure Data Storage	**Threat agents:** **Application specific;** Encompasses individuals or entities targeting

		vulnerabilities related to data storage. This includes skilled adversaries, malicious insiders, state-sponsored actors, cybercriminals, data brokers, competitors, cybercriminals, and activists or hacktivists. **Attack Vectors:** • Social engineering • Rooted or jailbroken devices • Malware or Malicious Applications • Data transmission interception • Weak encryption or no encryption • Unauthorized access to the file system
M10	**Insufficient Cryptography**	**Threat agents:** **Application specific;** Includes malicious insiders, state-sponsored actors, cybercriminals, attackers focusing on cryptographic algorithms or implementation, and attackers exploiting vulnerabilities in cryptographic protocol or libraries. **Attack Vectors:** • Cryptographic attacks • Brute force attacks • Side-channel attacks

2.5 Data Privacy and Data Protection

2.5.1 Data Privacy

Users' personal information is utilized in a variety of ways when using digital devices and services, and often the nature of the service defines the data that users share and the security measures employed to protect users' personal information. Concern for data privacy and protection is increased by the idea of personally identifiable information (PII).

According to [16] , privacy is primarily the individual's right to control who has access to their information, the scope of personal data disclosure or sharing, and the protection of this data from unauthorized parties that should not have access to it. The collecting, use, and related legal, ethical, and political issues related to data are all defined by data privacy. Even while there is some awareness of data privacy in Africa, [17] claim that it is noticeably lower than in other parts of the world. The discovery that some 23 African states have adopted data privacy laws lends credence to this statement.

Generally, data privacy has gained significant attention due to several countries establishing regulations and policies aimed at safeguarding the personal information of their citizens. These regulations ensure that companies provide transparent explanations within their policies regarding the nature of collected personal data, its purpose, distribution, and associated security measures. Furthermore, users retain the right to grant consent for the collection of their personal information and must be given the avenues to exercise such rights. For instance, the use of cookies in applications requires informed consent.

2.5.2 Data Protection

Data Protection constitutes another relevant concept in the collection, utilization, and distribution of information. This concept enforces regulations to ensure the confidentiality and security of personal information. Data protection encompasses all the procedures used to preserve important data from loss, tampering, or corruption while also permitting the restoration of the data to a usable state in the event of unforeseen circumstances [18]

In essence, data protection ensures the accuracy of the information, limits access to approved uses, and complies with any applicable legal or regulatory requirements.

Examples of legal frameworks for data protection and privacy include:

- Data Protection Act (Act No. 843) 2012 - DPA.
- The Nigerian Data Protection Regulation (NDPR).
- The General Data Protection Regulation - Regulation (EU) 2016/679 (GDPR).
- Privacy Act of 1974.
- Federal Trade Commission Act of 1914.

2.6 Related Works

The subject of security in mobile applications has been thoroughly researched, and much effort has been made to analyze the landscape of mobile application security. The emphasis has been on identifying and mitigating a wide range of security issues associated with mobile devices and the applications.

- [19] conducted a study on security implementations in mobile money applications, also known as branchless banking, using a dual approach of manual and automatic analysis. They analyzed 47 mobile money applications using an automated analysis approach and static analysis tools to detect Secure Sockets Layer and Transport Layer Security (SSL/TLS) vulnerabilities. Only 24 applications exhibited security flaws, but it was identified that the automatic static analyses were not conclusive.

  The study then proceeded to a manual analysis phase, focusing on the implementation of SSL/TLS on remote servers and the underlying source code. Key conclusions found were inadequate or poor SSL/TLS certificate validation, deficient access control mechanisms, and exposure of sensitive personally identifiable information (PII) through logging and preference storage practices. The report highlights the tendency of application developers to prioritize user-centric features over effective security controls, leading to a significant number of applications failing to meet service provider guidelines for protection.
- Another study conducted by [20] on the security and privacy exposure of freeware mobile health applications, focused on

the Android Operating System. The researchers identified security privacy issues within these applications and informed app vendors. A follow-up evaluation was conducted using dynamic analysis to validate the previous findings. The study collected 20 widely used m-Health applications from the Android marketplace from the "Medical" and "Health and Fitness" categories.

The findings align with [19] observations, with approximately 20% of the analyzed applications failing to provide privacy policy information. The issues include broken links to privacy policies or policies available in foreign language. Additionally, the study found instances where certain applications had permissions that exceeded their intended usage scope, falling under the classification of "dangerous." The study also found that 20% of the applications stored users' health-related data locally, while 80% transmitted this data. Half of the transmitting apps employed Hypertext Transfer Protocol Secure (HTTPS) to transmit users' health data. Additionally, these apps shared user-submitted multimedia files closely tied to their health condition but often lacked adequate transmission security.

The findings can be compared to the insecure communication identified by [19], but they present deeper insights into m-

Health applications that apply to other applications that collect personally identifiable information.

- Moreover, [21] made a significant contribution to mobile application security and privacy by examining the privacy vulnerability in 25 Android m-Heath applications, emulating methods by [19] and [20]. Their study focused on applications that establish connections to medical devices via network connections, distinguishing it from other researchers. The researchers found that only 4 (16%) of the 25 applications used proper Transport Layer Security (TLS) configuration, and only 1 application communicated with remote servers supporting the latest TLS version, TLS 1.3. The remaining 24 application servers employed deprecated TLS 1.2. Only 3 application servers supported HTTP Strict Transport Security (HSTS), leaving 22 applications susceptible to potential HTTP downgrade attacks. Additionally, 4 applications effectively transmitted encrypted user information, while 21 applications transmitted unencrypted data. 12 of the applications fall under the purview of the Health Insurance Portability and Accountability Act (HIPAA) because they collect protected health information (PHI). In that category, only 1 application demonstrated transparent HIPAA compliance measures, with two apps discussing HIPAA compliance in their respective policies. Despite the importance of cryptographic mechanisms for health information privacy and protection, this study reveals that several applications lack sufficient implementation to ensure confidentiality, integrity, and authenticity [22].

- Despite the existing research efforts, a study by [23] analyzed privacy and security in cryptocurrency mobile applications, specifically wallets used for cryptocurrency transactions. The researchers used static and manual code analysis to assess prevalent mobile app vulnerabilities, including improper cryptographic algorithms. They used download counts to group cryptocurrency applications from the Google Play Store and used a two-phase approach for evaluation. The first phase involved static code analysis to identify known security threats from the OWASP Top 10 and network data analysis to monitor potential transmission of sensitive data in plaintext. The second phase involved manual code testing to address the drawbacks of static analysis, focusing on authentication and cryptography threats. The results showed that 98% of the tested applications used the camera for scanning QR codes, but some issues raised concerns due to their outside-the-application workflow and potential unauthorized disclosure of user data. The study also found that over half of the issues identified in Phase 1 were not detrimental to end-users, mirroring the approach used by [20]. The investigation highlights potential security pitfalls within less-regulated digital platforms, with a comprehensive analysis combining static code assessment, network traffic examination, and manual examination.

- Finally, [24] contributed to the field of security and privacy issues related to mobile applications by analyzing the unapproved gathering and distribution of user data. The study reveals that many apps secretly gather and transfer additional data without the user's knowledge, even after describing permissions and privacy policies during installation.

  Users are vulnerable to social engineering threats due to insufficient safeguarding of data collected. The researchers focused on widely used mobile applications catering to both individual users and employees, revealing how these applications collect extensive user data beyond consent, resulting in compromised privacy for individuals and heightened organizational risks. This phenomenon is linked to potential social engineering attacks and malware distribution.

  The researchers used a combination of static, dynamic, and privacy policy statement analyses to derive their findings on threats to individual privacy and organizational security. They selected six Android mobile apps popular in the USA based on participant feedback from a survey. The investigation revealed instances where certain applications use deep-linking techniques to share user data without clear disclosure in their privacy policies. The study highlights contrasting approaches to data protection, with some apps implementing encryption to safeguard user data stored within the app, while others neglect encryption for data stored on users' mobile devices. This study provides valuable evidence that application developers often exceed their claims about data collection practices and emphasizes the IT risks associated with popular mobile applications that share and store user data without proper encryption.

2.7 Research Gap

Despite the substantial body of research focusing on the security and privacy aspects of mobile applications, there remains a notable gap in the current literature. While previous studies have diligently explored various vulnerabilities, threats, and privacy concerns associated with mobile applications, there is a distinct lack of comprehensive investigations that are specific to the mobile application security and privacy landscape in Ghana and guided by the country’s data protection regulations.

This gap is evident in the previous works where some studies were confined to specific regions outside of Ghana and also conformed to international data protection laws.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Type of Research

This project employs exploration to answer the research questions. It aims to uncover insights about security vulnerabilities and privacy compliance of Android mobile applications in Ghana. The research provides a comprehensive understanding of security challenges and privacy considerations in the digital landscape.

3.2 Population

The study examines Android mobile applications in Ghana, given the country's growing digital infrastructure and mobile technology adoption.

3.2.1 Identification of Mobile Applications

A collection of Android mobile applications will be selected based on usage or download statistics. The following inclusion criteria are used to select the mobile applications.

Table 3.0 Mobile Application Selection Criteria

Criteria	Requirements
I	The application is free to download and use.
II	The application requires data input, and stores, and transmits personal data.
III	Application has at least 1,000 downloads on

	the Play Store

A sample of 10 Android applications specific to Ghana's mobile application landscape were selected according to the inclusion criteria.

Table 3.1 Selected Mobile Applications

Category	Application
Finance	● PalmPay ● Fido
Health & Fitness	● DrugNet ● MyNHIS
E-Commerce (Shopping)	● Jumia Online Shopping ● Jiji Ghana ● Hubtel ● Franko Trading ● KiKuu
Maps & Navigation	● Ghana PostGPS

3.3 Data Collection Method

Mobile application security assessment tools will be used to scan the sample applications through automated and manual analysis.

Also, each application's privacy policy and terms of service will be reviewed to check for compliance with data privacy legislation and data management practices.

3.4 Types of data to be collected

Through the application analysis, different types of data on security and privacy will be collected.

1. **Vulnerability report:** This will include specifics on any identified security vulnerabilities in the applications, categorized by type and severity.
2. **Privacy compliance metrics:** This will involve data on each application's adherence to data protection regulations, focusing on the handling and storage of sensitive user information.
3. **Permissions analysis:** Information on the permissions requested and utilized by each application, especially those pertaining to sensitive data access.
4. **Network Traffic Analysis:** Data regarding the nature of information transmitted over networks, including any instances of unencrypted or potentially insecure transmissions.
5. **Source Code Evaluation:** This will involve details on any identified code-level security issues, such as improper handling of cryptographic algorithms.

3.4.1 Application Assessment Model

Applications subjected to analysis must meet specific selection criteria. The chosen applications undergo a comprehensive evaluation involving source code analysis, privacy policy assessment, and data communication testing. The model employed for app analysis is depicted in the following figure.

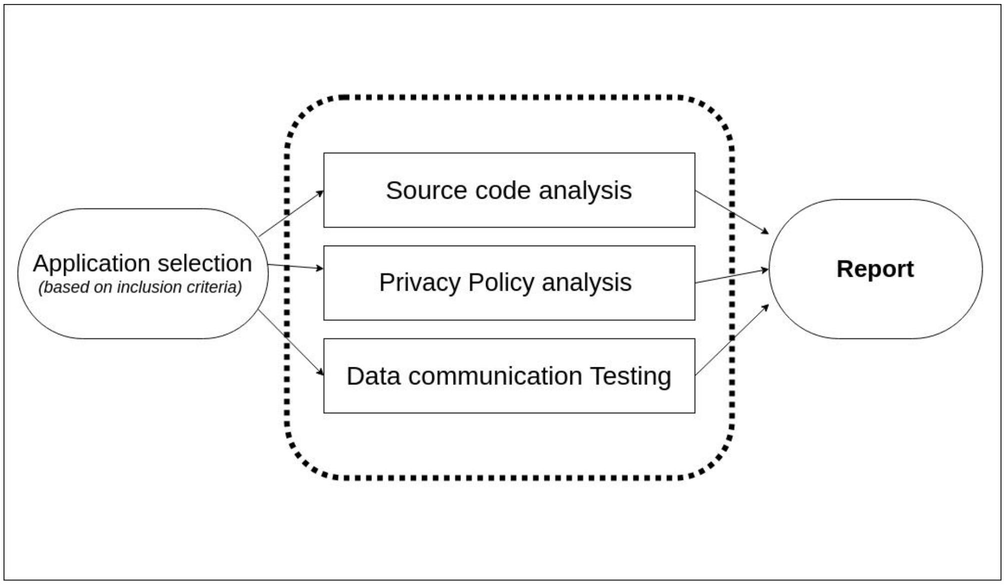


Figure 3.0 Applications Analysis Model

3.7 Instrument for Data Collection

3.7.1 Automated Testing (Static Analysis) Tools:

Industry-standard static analysis tools are used to conduct systematic evaluations of the sample mobile applications.

Table 3.2 Static analysis tools

Tool	Description
Mobile Security Framework	MobSF is an all-in-one mobile

(MobSF)	application utility for Android, iOS, and Windows pen-testing, malware analysis, and security assessment framework capable of performing static and dynamic analysis.
SSL Server Test	Performs deep analysis of the configuration of any SSL web server on the public Internet.

3.7.2 Manual Analysis Techniques (Dynamic Analysis):

Manual analysis techniques are applied to scrutinize the application's code and data handling processes.

Table 3.3 Dynamic analysis tool

Tool	Description
Mobile Security Framework (MobSF)	MobSF is an all-in-one mobile application utility for Android, iOS, and Windows pen-testing, malware analysis, and security assessment framework capable of performing static and dynamic analysis.

3.5 Instrument validity and reliability

The OWASP Mobile Application (MAS) framework and the Mobile Security Framework (MobSF) are used in this study to evaluate the mobile applications sample.

The OWASP Mobile Application Security (MAS) project offers the Mobile Application Security Verification Standard (MASVS) for mobile applications and the Mobile Application Security Testing Guide (MASTG). These resources cover the processes, techniques, and tools used in mobile app security testing, along with a comprehensive set of test cases for consistent and thorough results [25].

Mobile Security Framework (MobSF) is a mobile application security assessment framework. It offers automated pen-testing, malware analysis, and both static and dynamic analysis capabilities. It supports mobile application binaries including APK, XAPK, IPA, and APPX, and zipped source code [26] The framework has been proven to yield up to 97% true positive results as indicated by [27] , with a proven higher precision accuracy compared to similar tools demonstrated in [28] and [20].

3.6 Instrument structure to meet research objectives

The security testing tools used in this study have components that align with reaching the research goals.

Table 3.4 Summary of Instruments structure

COMPONENT OF INSTRUMENT	DESCRIPTION
Security assessment modules	The OWASP MASTG consists of modules dedicated to specific security

	assessments. These modules are designed to comprehensively evaluate aspects of application security, including but not limited to, data storage (MASVS-STORAGE), cryptography (MASVS-CRYPTO), secure coding practices (MASVS-CODE), and protection against common attack vectors such as network connections (MASVS-NETWORK).
Scoring mechanism	To measure the level of security implementation, the instruments use a structured scoring methodology. This allows for a comparative review of the app's security strengths and limitations.

3.7 Method of Data Analysis

The data collected from the evaluation of the application will be compared to the OWASP security recommendations to extract meaningful insights regarding vulnerabilities and privacy compliance.

3.7.1 Quantitative Analysis

The quantitative analysis of the collected data involves computing various metrics related to security vulnerabilities and privacy compliance. These metrics include the number of identified vulnerabilities, severity levels, and compliance scores with data protection regulations.

3.7.2 Qualitative Analysis

In addition to the quantitative measure, a qualitative analysis is conducted to gain deeper insights into security and privacy aspects. This involves examining individual vulnerabilities, assessing their potential impact, and considering the context in which they occur. The analysis will also cover categorizing vulnerabilities based on their nature and potential exploitability.

3.8 Instrument

Automated and manual testing tools are employed in this study for the evaluation of Android Applications.

3.8.1 Automated Testing Tools

- OWASP Mobile Application Security (MAS) Framework.

OWASP MAS contains a suite of tests covering various security aspects, including code analysis, network traffic interception, and dynamic application testing.

- **Mobile Security Framework (MobSF)**

Mobile Security Framework (MobSF) is a comprehensive mobile application security assessment framework. It offers automated pen-testing, malware analysis, and both static and dynamic analysis capabilities. MobSF supports various mobile app binaries, including APK, XAPK, IPA, and APPX, as well as zipped source code (Ajin, n.d.).

3.9 Computer Simulation of Instrument

In this study, computer simulation tools are not employed as the research primarily involves practical assessments of actual mobile applications.

The following table presents all the tools and their purposes used in this study

Table 3.5 List of Security Testing Tools

Tool	Description
MobSF	Utilized for static and dynamic analysis.
SSL Server Test	Performs deep analysis of the configuration of any SSL web server on the public Internet.
MITMProxy	mitmproxy is a suite of tools that provides an interactive, SSL/TLS-capable HTTP/1, HTTP/2, and WebSocket intercepting proxy.

CHAPTER FOUR

FINDINGS AND DISCUSSIONS

This study defines its goal to evaluate the security and data privacy compliance of Android mobile applications in Ghana. The OWASP MAS underpins the security testing and evaluations.

4.1 Presentation of Findings

4.1.1 Data Privacy Policy Review

The data privacy policy review examines how developers prioritize functionality over ethical considerations in selected applications.

Out of ten reviewed applications, seven (7) provided detailed privacy policies outlining data collection processes and security measures.

Two (2) applications presented generic privacy policies with little to no useful information for users. These policies are typically used for testing purposes and meet hosting requirements on the Google Play Store. Developers should make the policy available to users, but some provide an email for users to contact them for a copy.

Additionally, one (1) application directs users to an unavailable privacy policy link, which was identified to be hosted at a different URL than the one provided on the Android Play Store

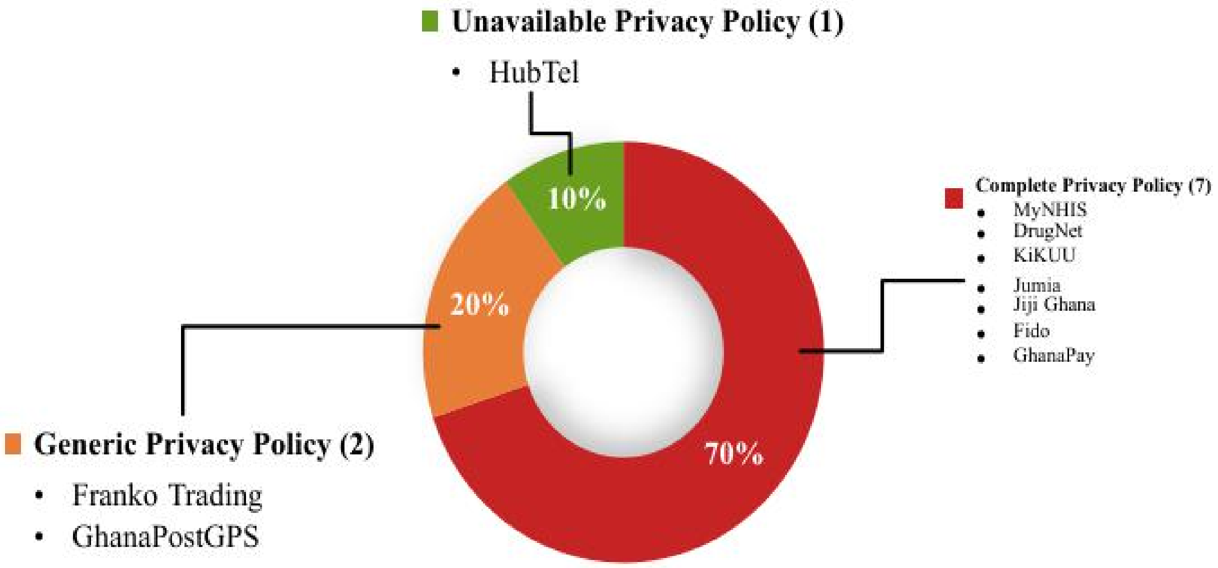


Figure 4.0 Summary of Data Privacy Compliance Review

4.1.2 Application Permissions Review

The application permissions review involved comparing the generated MobSF static analysis report to the actual AndroidManifest file existing in each application. This process was carried out to ensure that mobile applications were only using the least permissions they require of the mobile device to function as declared in the Google PlayStore permissions section. The MobSF report identified applications accessing sensitive permissions from the mobile device. These permissions are flagged as 'dangerous' because they expose the user's information and risk the device to malicious attack should the application be compromised.

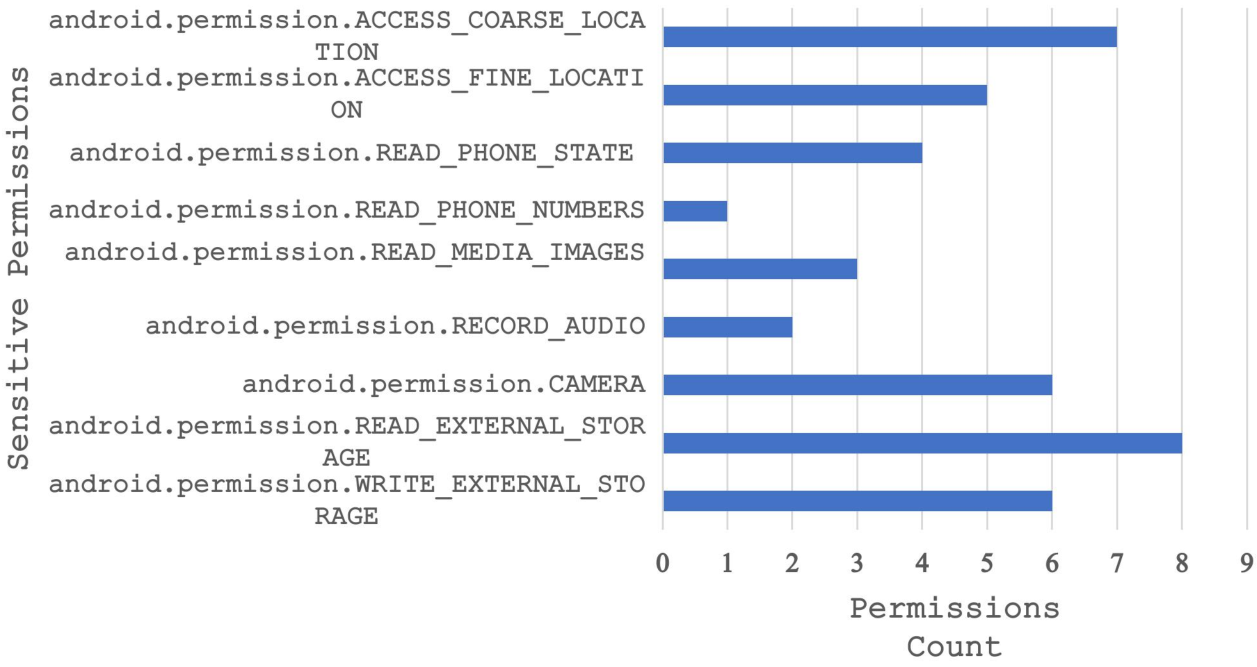


Figure 4.1 Summary of Sensitive Permissions accessed by applications

4.1.3 Source Code Analysis Report

MobSF static code analysis also identified possible weaknesses within the application's source code. Although the report highlighted coding techniques that could expose the application to common security risks, further examination revealed that some of the reported issues are false positives.

The table below summarizes identified issues in some applications from the source code analysis.

Table 4.0 Summary of Source Code Analysis

ISSUE/STANDARDS	APPLICATIONS
• **The App logs information.** CWE: CWE-532: Insertion of Sensitive Information into Log File. OWASP MASVS: MSTG-STORAGE-3	DrugNet MyNHIS Fido Franko Trading
• **Files may contain hardcoded sensitive information like usernames, passwords, and keys.** CWE: CWE-312: Cleartext Storage of Sensitive Information. OWASP Top 10: M9: Reverse Engineering (OWASP MASVS: MSTG-STORAGE-14)	DrugNet MyNHIS Fido Franko Trading
• **The app can read/write to External Storage. Any App can read data written to External Storage.** CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	DrugNet Franko Trading
• **The App uses an insecure Random Number Generator.** CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	DrugNet MyNHIS Fido Franko Trading
App uses SQLite Database and executes raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	DrugNet MyNHIS Fido Franko Trading
• **The App uses the encryption mode CBC with**	MyNHIS

PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks. CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	
• **App creates temp file. Sensitive information should never be written into a temp file.** CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	Fido
• **SHA-1 is a weak hash known to have hash collisions.** CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	Franko Trading
• **MD5 is a weak hash known to have hash collisions.** CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	Franko Trading

4.1.4 Network Communication Analysis

Table 4.1 Summary of Applications Communication Protocols

Application	Protocol (TLS version and Cipher Suite)
KiKuu	TLSv1.2

	TLS_ECDHE_RSA_WITH_AES_28_GCM_SHA256
Franko Trading Enterprise	TLSv1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
DrugNet	TLSv1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
Jumia	TLSv1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
HubTel	TLSv1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Jiji	TLSv1.3 TLS_AES_128_GCM_SHA256 TLSv1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
MyNHIS	TLSv1.2 TLS_RSA_WITH_RC4_128_SHA
GhanaPostGPS	TLSv1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Fido	TLSv1.3 TLS_AES_256_GCM_SHA384 TLSv1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
PalmPay	TLSv1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.0 Summary of Findings

The comprehensive evaluation undertaken in this study encompassed a review of privacy policies, an examination of source code, and a detailed analysis of network communication protocols. Through these assessments, valuable insights into prevalent trends in the development and deployment of widely used Android mobile applications were obtained.

5.0.1 Privacy Policy Review:

Out of the ten applications reviewed, seven provided detailed and transparent privacy policies. Two applications presented generic policies, offering limited information, and one application directed users to an unavailable privacy policy link, indicating a potential gap in transparency.

5.0.2 Source Code Analysis:

The analysis uncovered instances of substandard coding practices, which could pose security risks. Notably, certain applications exhibited areas of vulnerability due to inadequate security controls in the source code.

5.0.3 Network Communication Protocol:

A majority of the applications transmitted user data securely using TLS on HTTP, highlighting a positive trend in ensuring security between the client and the remote server. However, a few applications use TLS version and cipher suites which may be vulnerable to attacks.

5.1 Discussion of Findings

5.1.1 Privacy Policy Transparency:

The study discovered that a majority of the applications provided clear and comprehensive privacy policies. This is a positive indication of a growing awareness among developers regarding the importance of transparent data handling practices and compliance with the Ghana Data Protection Act 2012. However, the presence of generic policies in some applications raises concerns about the level of detail provided to users.

5.1.2 Source Code Vulnerabilities:

Source code analysis revealed several instances of suboptimal coding practices. These vulnerabilities, while not universally present, suggest that there is room for improvement in secure coding techniques. Mobile application developers should be encouraged to adopt best practices laid out by the Google Developer Documentation and the OWASP mobile top 10 security risks to fortify the applications against potential security breaches.

5.1.3 Mobile Application Network Communication:

The examination of network communication protocols revealed a prevalent usage of secure transport layer protocols among the selected applications, specifically TLS versions 1.2 and 1.3, to ensure encrypted data transmission. This demonstrates developers' commitment to data security.

However, some applications use older versions of TLS cipher suites, such as TLS_RSA_WITH_RC4_128_SHA in MyNHIS, which may pose security risks. Also, Jiji, adopts the latest TLS 1.3 protocol, offering enhanced security features, setting a positive precedent for the industry. This proactive approach to security measures is commendable.

5.2 Conclusion

In conclusion, this study conducted a comprehensive evaluation of widely used Android mobile applications in Ghana, focusing on security vulnerabilities and data privacy standards compliance. The results present a mixed landscape, with commendable efforts in privacy policy transparency, although other areas require attention. It is evident that developers are increasingly recognizing the significance of transparent data-handling practices.

However, the presence of generic policies in some applications underscores the need for more detailed and context-specific privacy disclosures. This study emphasizes the critical role of adherence to privacy regulations and secure coding techniques in the development and deployment of mobile applications.

Moving forward, both developers and regulatory bodies must work collaboratively towards enhancing privacy practices in the digital landscape. This research serves as a foundational step towards a more secure and privacy-aware mobile application ecosystem in Ghana.

5.3 Recommendations

Drawing from the findings of this study, several key recommendations emerge to fortify the security and data privacy landscape of mobile applications in Ghana. By embracing these recommendations, stakeholders in the mobile application ecosystem can significantly strengthen security and privacy protocols, fostering a more resilient digital environment for users in Ghana.

1. **Adherence to Data Protection Regulations:**

Mobile application developers should align their practices with established data protection regulations, such as the Ghana Data Protection Act 2012. This does not only ensure legal compliance but also upholds ethical standards in data handling. Moreover, developers should diligently update and maintain accessible privacy policy information.

2. Integration of OWASP Top 10 Mobile Security Practices:

Companies and mobile application developers need to incorporate the OWASP top 10 mobile security risks and leverage their recommended testing tools for comprehensive security assessments. This proactive approach mitigates common errors that may persist in deployed mobile applications.

3. Secure TLS Configuration:

Mobile application developers and IT infrastructure engineers should adopt the technique of configuring back-end services to exclusively accept secure TLS cipher suites. This measure will prevent servers from reverting to potentially vulnerable cipher suites, thereby safeguarding user data against potential breaches.

5.4 Limitations of the Study

While this project endeavors to provide insights into the security and privacy landscape of mobile applications in Ghana, the following limitations are acknowledged:

1. Sample Size:

The study focused on only 10 Android mobile applications labeled as “widely-used” applications. While this approach allowed for in-depth analysis, it may not encompass the entirety of the mobile application landscape in Ghana.

2. Dynamic Nature of Mobile Application Landscape:

The mobile application landscape is constantly evolving with updates, new releases, and emerging technologies. This study captures a snapshot within a specific timeframe, and therefore, findings might evolve.

3. Single Platform Emphasis:

The research primarily centered on the Android platform. Different operating systems may exhibit distinct security and privacy characteristics, which were not extensively explored in this study.

4. Assumed Compliance with Privacy Policies:

The study assessed privacy policy transparency based on provided information. It is possible that actual adherence to these policies may vary, and further investigations could be required.

5. Resource and Time Constraints:

The depth of analysis was constrained by available resources and time. A more extensive study might uncover additional nuances.

5.5 Future work

This project sets a foundational understanding of the security and privacy landscape of mobile applications in Ghana, there are several avenues for future research and development.

i. Expanded Application Portfolio:

To attain a comprehensive view, future studies would encompass a broader range of applications, including emerging ones from various mobile application categories to gauge their adherence to privacy policies and security standards.

ii. Dynamic Testing Methods:

Integrating dynamic analysis techniques, like penetration testing and runtime security checks, can provide real-time insights into application behavior and vulnerabilities.

REFERENCES

[1] M. Kpessa-Whyte and J. S. Dzisah, “Digitalisation of Basic Services in Ghana: State of Policies in Action and Lesson for Progress,” 2022.

[2] J. Demuyakor, “Ghana’s Digitization Initiatives: A Survey of Citizens Perceptions on the Benefits and Challenges to the Utilization of Digital Governance Services,” *International Journal of Publication and Social Studies*, vol. 6, no. 1, pp. 42–55, 2021, doi: 10.18488/journal.135.2021.61.42.55.

[3] Doris Dokua Sasu, “Market share of mobile operating systems in Ghana 2022.” Accessed: Jul. 21, 2023. [Online]. Available: https://www.statista.com/statistics/1330502/market-share-of-mobile-operating-systems-in-ghana/

[4] A. Dabalen and J. Tei Mensah, “Ten Facts about digital technology adoption in Ghana.” Oct. 2023. [Online]. Available: https://blogs.worldbank.org/africacan/ten-facts-about-digital-technology-adoption-ghana

[5] F. Laricchia, “Smartphones - Statistics and Facts .” Oct. 2023. [Online]. Available: https://www.statista.com/topics/840/smartphones/

[6] G. Omondi, “The state of mobile in Ghana’s tech ecosystem | Mobile for Development.” Oct. 2020. [Online]. Available: https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-in-ghanas-tech-ecosystem/

[7] Statista Research Department, “Market share of mobile operating systems worldwide 2009-2023.” Oct. 2023. [Online]. Available: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

[8] T. A. Majchrzak, A. Biørn-Hansen, and G. Tor-Morten, “Progressive Web Apps: the Definite Approach to Cross-Platform Development?,” Oct. 2018, doi: http://hdl.handle.net/10125/50607.

[9] V. K. Velu, *Mobile application penetration testing: Explore real-world threat scenarios, attacks on mobile applications, and ways to counter them*. Packt Publishing, 2016.

[10] D. Chell, T. Erasmus, S. Colley, and O. Whitehouse, *The mobile application Hacker’s handbook*. 2015. doi: 10.1002/9781119183655.

[11] GuardSquare, "What is Mobile App Security?" [Online]. Available: https://www.guardsquare.com/what-is-mobile-app-security

[12] H. Dwivedi, C. Clark, and D. Thiel, *Mobile Application Security*. McGraw Hill Professional, 2010.

[13] G. Sims, "How secure is Android?," *Android Authority*, Oct. 2012, [Online]. Available: http://www.androidauthority.com/secure-android-90523/

[14] Google Android Developers, "Platform architecture." [Online]. Available: https://developer.android.com/guide/platform

[15] Apple Inc., "Apple Platform Security." Oct. 2022. [Online]. Available: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[16] A. P. Uche-Awaji, "Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World," *Social Science Research Network*, Oct. 2022, doi: 10.2139/ssrn.4005750.

[17] P. Prinsloo and R. Kaliisa, "Data privacy on the African continent: Opportunities, challenges and implications for learning analytics," *British Journal of Educational Technology*, vol. 53, no. 4, pp. 894–913, Oct. 2022, doi: 10.1111/bjet.13226.

[18] SNIA, "What is Data Protection?" [Online]. Available: https://www.snia.org/education/what-is-data-protection

[19] B. Reaves, N. Scaife, A. Bates, P. Traynor, and K. R. B. Butler, "Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World," 2017. doi: https://doi.org/10.1145/3092368.

[20] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice," *IEEE Access*, vol. 6, pp. 9390–9403, Jan. 2018, doi: 10.1109/ACCESS.2018.2799522.

[21] M. Aliasgari, M. Black, and N. Yadav, "Security Vulnerabilities in Mobile Health Applications," 2018.

[22] B. M. C. Silva, J. J. P. C. Rodrigues, F. Canelo, I. M. Lopes, and J. Lloret, "Towards a cooperative security system for mobile-health applications," *Electronic Commerce Research*, Oct. 2014, doi: 10.1007/s10660-014-9154-3.

[23] A. R. Sai, J. Buckley, and A. Le Gear, “Privacy and security analysis of cryptocurrency mobile applications,” in *2019 fifth conference on mobile and secure services (MobiSecServ)*, 2019, pp. 1–6.

[24] D. Hayes, F. Cappa, and N. A. Le-Khac, “An effective approach to mobile device management: Security and privacy issues associated with mobile applications,” *Digital Business*, vol. 1, no. 1, Sep. 2020, doi: 10.1016/j.digbus.2020.100001.

[25] OWASP, “OWASP Mobile Application Security.” [Online]. Available: https://mas.owasp.org/#our-mission

[26] A. Ajin, “About mobile security framework.” [Online]. Available: https://mobsf.live/about

[27] C. Anwar, C. Herli Sumerli A., S. Hady, N. Rahayu, and K. Kraugusteeliana, “The Application of Mobile Security Framework (MOBSF) and Mobile Application Security Testing Guide to Ensure the Security in Mobile Commerce Applications,” *Jurnal Sistim Informasi dan Teknologi (JSISFOTEK)* , vol. 5, no. 2, Oct. 2023, doi: 10.37034/jsisfotek.v5i1.231.

[28] C. Hanifurohman and D. D. Hutagalung, “Static Analysis Using the Mobile Security Framework for Testing the Security of Android-Based E-Commerce Mobile Applications,” *Sebatik*, vol. 24, no. 1, pp. 22–28, Oct. 2020, doi: 10.46984/sebatik.v24i1.920.

turnitin

Digital Receipt

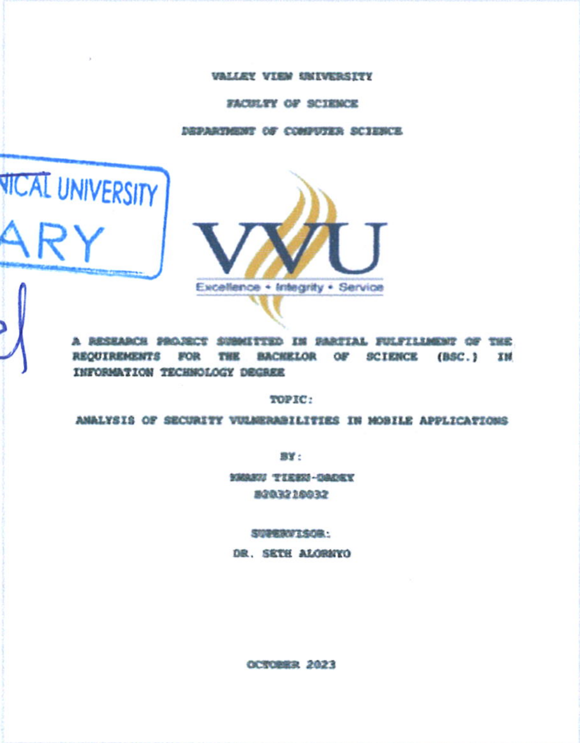
This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	FARUQ YEVU
Assignment title:	Plagiarism check @UNIVERSITY_LIBRARY_KTU
Submission title:	KWAKU_TIEKU-DADEY
File name:	KWAKU_TIEKU-DADEY_B203210032_COMPUTER_SCIENCE_DE...
File size:	630.02K
Page count:	72
Word count:	10,588
Character count:	65,725
Submission date:	14-Nov-2023 11:55AM (UTC+0000)
Submission ID:	2216249561

27/11/2023

Patrick Baayel



VALLEY VIEW UNIVERSITY

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

VVU
Excellence • Integrity • Service

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE BACHELOR OF SCIENCE (BSC.) IN INFORMATION TECHNOLOGY DEGREE

TOPIC:

ANALYSIS OF SECURITY VULNERABILITIES IN MOBILE APPLICATIONS

BY:

KWAKU TIEKU-DADEY
B203210032

SUPERVISOR:

DR. SETH ALORNYO

OCTOBER 2023

KWAKU_TIEKU-DADEY

ORIGINALITY REPORT

16%	13%	6%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	2%
2	Submitted to Royal Holloway and Bedford New College Student Paper	1%
3	Submitted to Hogeschool NOVI Student Paper	1%
4	mobsf.github.io Internet Source	1%
5	lalitkala.gov.in Internet Source	1%
6	Submitted to Universiti Teknologi MARA Student Paper	<1%
7	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1%
8	www.pulsesecure.net Internet Source	<1%
9	docs.oracle.com	