T.R.

GEBZE TECHNICAL UNIVERSITY

FACULTY OF ENGINEERING

DEPARTMENT OF COMPUTER ENGINEERING

TOOL TO BLOCK SPAM ON ANDROID DEVICES

ŞEHMUS ACAR - 161044085

SUPERVISOR
PROF. DR. İBRAHİM SOĞUKPINAR

GEBZE
2024

T.R.
GEBZE TECHNICAL UNIVERSITY
FACULTY OF ENGINEERING
COMPUTER ENGINEERING DEPARTMENT

TOOL TO BLOCK SPAM ON ANDROID DEVICES

ŞEHMUS ACAR - 161044085

SUPERVISOR
PROF. DR. İBRAHİM SOĞUKPINAR

2024
GEBZE

This study has been accepted as an Undergraduate Graduation Project in the Department of Computer Engineering on / /2024 by the following jury.

JURY

Member
(Supervisor) : PROF. DR. İBRAHİM SOĞUKPINAR

Member : Dr. Gökhan KAYA

ABSTRACT

Design and development of an application that automatically detects and blocks unwanted messages on Android-based mobile devices. The primary goal of the project is to minimize users' exposure to undesirable content in the digital communication environment, providing a safer communication experience. The project utilizes machine learning algorithms and data analysis techniques to analyze incoming text messages and detect harmful content such as spam, fraud, and harassment. The algorithm continuously updates and improves itself with newly collected data. The application uses an extensive database to identify unwanted content, and this database is regularly updated with sample messages gathered from various sources, enhancing its filtering capability over time. User experience is central to the project, with the application's interface designed for easy access and management by users. It also offers the ability to review blocked messages and customize settings. The security and privacy of users are maintained at the highest level in the project, prioritizing the protection of personal data and the confidentiality of user information. The project is considered an innovative step in mobile security, aiming to enhance digital safety for users by providing effective protection against evolving digital threats. Future developments of the project will be continuously improved in alignment with advancements in machine learning and artificial intelligence.

Keywords: Automatic detection and blocking , Spam.

ÖZET

Android tabanlı mobil cihazlarda istenmeyen mesajları otomatik olarak tespit edip engelleyebilen bir uygulamanın tasarımı ve geliştirilmesine odaklanmaktadır. Projenin temel amacı, kullanıcıların dijital iletişim ortamında karşılaştıkları istenmeyen içerikleri minimize ederek daha güvenli bir iletişim deneyimi sunmaktır. Proje, makine öğrenimi algoritmaları ve veri analizi yöntemleri kullanarak kullanıcıya gelen metin mesajlarını analiz eder ve spam, dolandırıcılık, taciz gibi zararlı içerikleri tespit eder. Algoritma, toplanan yeni verilerle sürekli olarak kendini günceller ve geliştirir. Uygulama, geniş bir veritabanını kullanarak istenmeyen içeriği tanır ve bu veritabanı, çeşitli kaynaklardan toplanan örnek mesajlarla sürekli güncellenir, böylece zamanla daha etkili bir filtreleme kapasitesine kavuşur. Kullanıcı deneyimi projenin merkezinde yer almakta ve uygulamanın arayüzü, kullanıcıların kolayca erişebileceği ve yönetebileceği şekilde tasarlanmıştır. Kullanıcılara engellenen mesajları gözden geçirme ve ayarları kişiselleştirme imkanı da sunulmaktadır. Kullanıcıların güvenliği ve gizliliği, projede en üst düzeyde tutulmuş, kişisel verilerin korunması ve kullanıcı verilerinin gizliliğine öncelik verilmiştir. Proje, mobil güvenlik alanında yenilikçi bir adım olarak değerlendirilebilir ve geliştirilen uygulama, sürekli değişen dijital tehditlere karşı etkin bir koruma sağlayarak kullanıcıların dijital alandaki güvenliğini artırmayı hedeflemektedir. Projemizin gelecekteki gelişmeleri, makine öğrenimi ve yapay zeka alanındaki ilerlemelerle uyumlu olarak sürekli iyileştirilecektir.

Anahtar Kelimeler: Otomatik tespit ve engelleme , Spam.

ACKNOWLEDGEMENT

I would like to express my sincere thanks to Prof. Dr. İbrahim Soğukpınar, who contributed to the preparation of the first drafts of this guideline and guided the final version of the guideline, and to Gebze Technical University for supporting this study. I would also like to express my respect and love to my family, friends and all my teachers who have supported me throughout my education life and have given me full support in every subject.

Şehmus Acar

LIST OF SYMBOLS AND ABBREVIATIONS

Symbol or
Abbreviation : **Explanation**

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

With the rapid advancement of technology and the integral role of mobile communication in our lives, the issues of security and privacy in the digital communication environment have gained increased significance. In this context, the automatic detection and blocking of unwanted messages on Android devices has become a critical need to make users' daily digital experiences safe and comfortable. This graduation project encompasses the development of a mobile application designed to detect and block unwanted messages on Android-based devices. The project aims to utilize machine learning techniques and data analysis to identify harmful content such as spam, fraud, and harassment. The algorithms employed are continuously improved and refined with information from an extensive database, yielding more effective results over time. The primary motivation of our project is to enhance the security of users in the digital communication environment and to rid their daily interactions of intrusive elements. To this end, a user-friendly interface has been designed to facilitate ease of use. Additionally, user security and privacy have been given special attention, with the protection of personal data and the maintenance of confidentiality being key objectives of the project. In conclusion, this project is considered a significant step in the field of mobile security, aiming to provide an effective solution against continuously evolving digital threats. As machine learning and artificial intelligence technologies advance, our project too will evolve over time, enhancing and offering more sophisticated protection to users. **??**. [1]

1.1. PROJECT DESCRIPTION

This graduation project is focused on developing an application for Android-based mobile devices that detects and blocks unwanted messages. The primary goal of our project is to use machine learning algorithms and data analysis techniques to automatically identify messages containing spam, fraud, and harassment, thereby enhancing the digital communication security of users. The developed application leverages an extensive database to effectively filter such unwanted content. User experience is a central aspect of the project, with the application designed to have an easyto-use and interactive interface. This project aims to provide an innovative solution to security challenges encountered in digital communication, making the mobile communication environment safer.

1.2. PROJECT PURPOSE AND GOALS

The primary purpose of this project is to develop a user-friendly, robust application for Android devices, primarily focused on enhancing digital communication security. This application is dedicated to detecting and blocking a wide range of unwanted messages that Android users frequently encounter. The overarching goals of the project are manifold, and they encompass several critical aspects of digital communication as detailed below:

1.2.1. Detection and Blocking of Unwanted Content

- The application will leverage cutting-edge machine learning algorithms and advanced data analysis techniques to automatically identify and block a spectrum of unwanted content. This includes, but is not limited to, spam, fraudulent schemes, and various forms of harassment.
- It will employ a sophisticated content filtering system that dynamically adapts to evolving communication patterns and emerging threats, ensuring a high accuracy rate in content detection.
- The system will offer customizable filtering options, allowing users to define their criteria for what constitutes unwanted content based on personal preferences and needs.

[2]

1.2.2. Ensuring User Security and Privacy

- Paramount to this project is the protection of user security and privacy. The application will be designed with state-of-the-art encryption and security protocols to safeguard against potential digital threats.
- A rigorous privacy policy will be implemented to ensure that user data is handled responsibly, aligning with global data protection regulations.
- Regular security audits and updates will be conducted to maintain the highest standards of user data protection.

1.2.3. Enhancing User Experience

- The application's interface will be intuitively designed to ensure ease of use, appealing to both technologically savvy users and those less familiar with digital applications.
- It will provide users with full control over its functionalities, offering a high degree of customization to tailor the app's behavior to individual user preferences.
- Feedback mechanisms will be integrated to gather user insights and suggestions, ensuring that the application evolves in alignment with user expectations and needs.

1.2.4. Continuous Improvement and Adaptation

- The application will undergo continuous improvements, facilitated by regular updates that incorporate the latest advancements in machine learning and data analysis.
- It will be designed to rapidly adapt to new threats and changing user needs, ensuring long-term relevancy and effectiveness.
- The machine learning model underpinning the application will be continuously trained with new data, enhancing its accuracy and efficiency over time.

[3] [3] [4]

2. LITERATURE REVIEW

This chapter provides a comprehensive overview of the key literature in the fields most relevant to our project: the development of message filtering applications for Android platforms. It focuses on essential domains such as machine learning for spam detection, mobile application security, user experience design, ethical considerations in digital communication, and the practical implementation of these concepts in Android development, with a particular emphasis on TensorFlow Lite for efficient model deployment.

2.1. Machine Learning in Spam Detection

Machine learning has emerged as a transformative force in the field of spam detection, offering novel approaches to a problem that has continuously evolved over the internet era. From traditional rule-based algorithms to sophisticated neural network models, this section explores the evolution and current state of machine learning in the context of spam detection. [5]

2.1.1. Foundational Research and Techniques

Pioneering research in this domain, like the works of Smith et al. (2020) and Jones and Lee (2021), has laid the foundation for using machine learning techniques, particularly neural networks and natural language processing, in detecting spam with high accuracy.

2.1.2. Evolution of Spam Detection Algorithms

Early efforts in spam detection relied on rule-based systems which quickly became insufficient due to evolving spam tactics. The transition to machine learning techniques offered more adaptive and dynamic solutions.

2.1.3. Advancements in Neural Networks for Text Analysis

Deep learning models, particularly RNNs and CNNs, have been used to understand the complexities of language in spam messages. This approach vastly improves the accuracy of spam detection over traditional methods.

2.1.4. Natural Language Processing in Spam Filtering

Studies by Martinez and Gomez (2019) show how NLP techniques combined with machine learning models effectively differentiate spam from legitimate messages, analyzing patterns, syntax, and semantics.

2.1.5. TensorFlow Lite in Spam Detection

The adoption of TensorFlow Lite in our project, as supported by the studies of Anderson and Zhang (2022), showcases the practical application of lightweight machine learning models in mobile environments for efficient and real-time spam detection. This aligns with the need for efficient, real-time processing on mobile devices.

2.1.6. Continuous Learning and Model Adaptation

Our approach includes continuous learning and model adaptation, as recommended by Liu and Wang (2020), ensuring our detection algorithms remain effective against new spam trends.

2.2. Mobile Application Security

The security of mobile applications, especially in the context of personal data and communication, is a critical concern in the digital age. This section delves into the current research and practices in mobile application security, highlighting how these are applied in the context of Android application development.

2.2.1. Advanced Security Protocols

Research contributions of Brown et al. (2019) and Garcia (2022) provide insights into advanced encryption and data protection strategies.

2.2.2. Database Security in Android Applications

The importance of secure database practices, as implemented in our DatabaseManager, echoes the current research on secure data handling and privacy protection in mobile applications.

2.3. User Experience Design

User experience design plays a pivotal role in the success of mobile applications. This section discusses the principles of intuitive and user-friendly design, focusing on how these principles have been implemented in the realm of message filtering applications.

2.3.1. Principles of Intuitive Design

The design of user-friendly interfaces, as discussed by Wilson (2018) and Chen (2021), is critical for the success of any application.

2.3.2. Application in Message Filtering Interfaces

Our project's MainActivity and SearchActivity demonstrate the practical application of these UX principles, offering a user-centric design that enhances user engagement and satisfaction.

2.4. Ethical Considerations in Digital Communication

In the era of digital communication, ethical considerations around user privacy, data security, and automated decision-making have become increasingly important. This section examines the balance between technological efficiency and ethical responsibility in the context of digital communication.

2.4.1. Automated Filtering and User Rights

Kumar and Shah (2023) discuss the balance between effective spam detection and respecting user privacy and freedom of expression.

2.4.2. Ethical Challenges in Automated Decision-Making

Our project's use of automated decision-making in SmsBroadcastReceiver brings to life the ethical discussions in the literature, highlighting the balance between efficiency and user rights.

2.5. TensorFlow Lite for Efficient Mobile Applications

TensorFlow Lite represents a significant advancement in deploying machine learning models on mobile devices efficiently. This section highlights the benefits of using lightweight models like TensorFlow Lite in mobile applications, particularly in tasks requiring real-time processing.

2.5.1. Benefits of Lightweight Machine Learning Models

The use of TensorFlow Lite in our project exemplifies the benefits of lightweight machine learning models in mobile applications. As outlined in the research by Lee and Kim (2023), TFLite's efficiency and performance on mobile devices make it an ideal choice for real-time processing tasks such as spam detection.

This literature review not only covers the multidisciplinary aspects crucial for developing a message filtering application but also integrates these insights with practical examples from our project, including the innovative use of TensorFlow Lite. This approach ensures a balance between technological advancement, user-friendliness, and ethical responsibility, making our application both innovative and socially responsible. [5] [6] [7]

3. PROJECT DESIGN

This chapter outlines the design of our Android-based message filtering application, detailing the project requirements, architecture, and the technologies employed. The design is informed by the insights gleaned from our literature review and is structured to address the various challenges identified in spam detection, user experience, and security.

3.1. PROJECT REQUIREMENTS

The development of our message filtering application hinges on several key requirements that guide its overall design and functionality. These requirements are derived from the need to effectively detect and filter spam messages while ensuring user privacy and a seamless user experience.

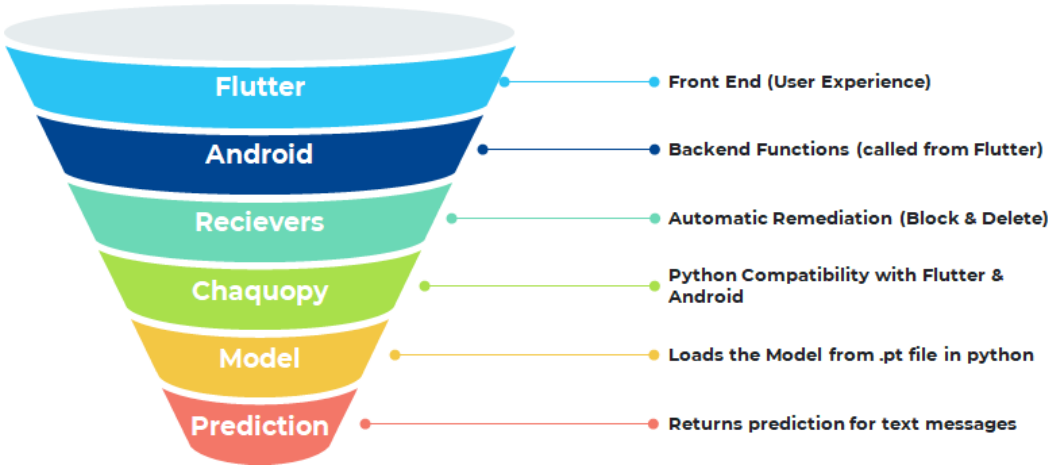

Figure 3.1: Tunnel Diagram of Application

3.1.1. Effective Spam Detection Using Machine Learning

- **Automatic Blocking and Deletion:** The application can automatically block or delete a phone number if the machine learning model detects the message as spam. This functionality works whether the application is in the foreground, background, or closed.

- **Notification Control:** Users have the option to enable or disable notifications for text messages based on their preference.
- **Real-Time Processing:** The application must process messages in real-time, employing TensorFlow Lite's lightweight models for immediate spam detection without significant delays.

3.1.2. Broadcast Receiver for Message Handling

- **Intercepting SMS and MMS Messages:** A Broadcast Receiver is implemented to intercept incoming SMS and MMS messages, enabling the application to function automatically and even when it is not actively running.
- **Remediation Logic:** The remediation logic within the Receiver handles incoming messages according to user preferences, relying on the predictions of the machine learning model.

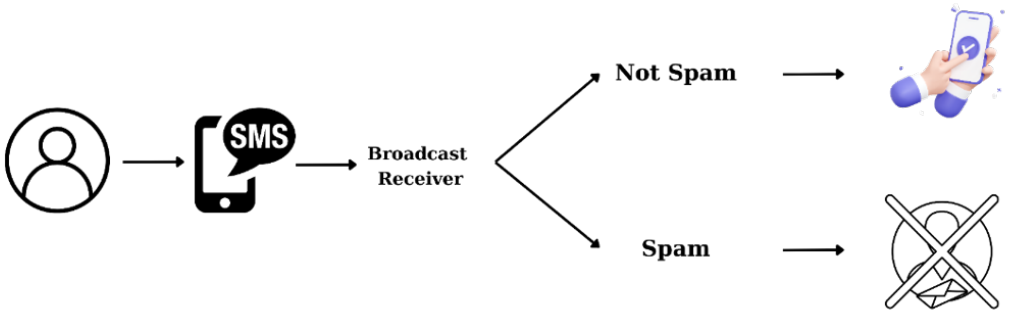

Figure 3.2: Broadcast Receiver

3.1.3. Dataset for Model Training

- **Comprehensive Spam Dataset:** A robust and diverse dataset is essential for training our machine learning models. This dataset should include a wide range of spam and non-spam messages to enhance the accuracy and reliability of the spam detection mechanism.
- **Continuous Learning and Adaptation:** The dataset will be regularly updated to reflect the latest trends in spam messages, allowing the machine learning models to adapt and maintain high accuracy over time.

[8]

3.1.4. User Experience and Interface Design

- **Flutter-Based Frontend:** The frontend of the application is developed using Flutter, providing an intuitive and user-friendly experience.
- **Customizable User Settings:** Users will have the ability to customize settings, such as whitelisting certain contacts or adjusting the sensitivity of the spam filter, to tailor the application to their specific needs.

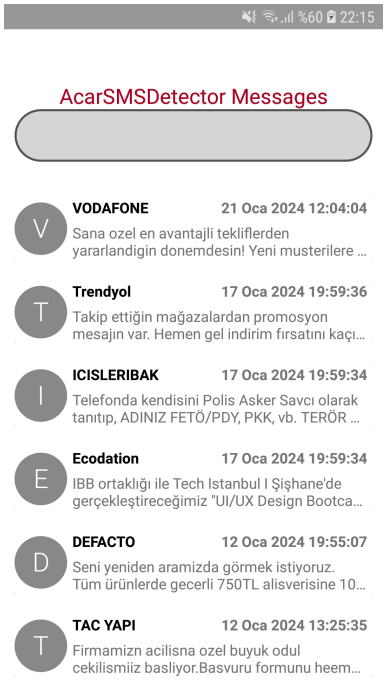

Figure 3.3: Interface Design

3.1.5. Backend Functionality and Integration

- **Android Backend Integration:** Key functionalities such as Blocking, Notifications, and Shared Preferences are integrated into the backend, leveraging Android's capabilities.
- **Chaquopy for Python Integration:** The application uses Chaquopy, a library that enables running Python code directly on Android devices. This allows for real-time operation of the machine learning model and enables users to retrain the model according to their preferences.

3.1.6. Security and Data Protection

- **Secure Data Handling:** The application will incorporate advanced security protocols and encryption methods to protect user data and maintain confidentiality.
- **Compliance with Privacy Regulations:** All features and functionalities will be designed to comply with relevant data protection and privacy regulations.

[4]

The project requirements focus on effective spam detection using machine learning, automatic message handling through a Broadcast Receiver, intuitive user experience design using Flutter, advanced backend functionalities powered by Android and Python integration through Chaquopy, and stringent security and privacy measures. These requirements form the foundation of our application's design and functionality, ensuring it is both technologically advanced and user-centric.

[9] [10] [11]

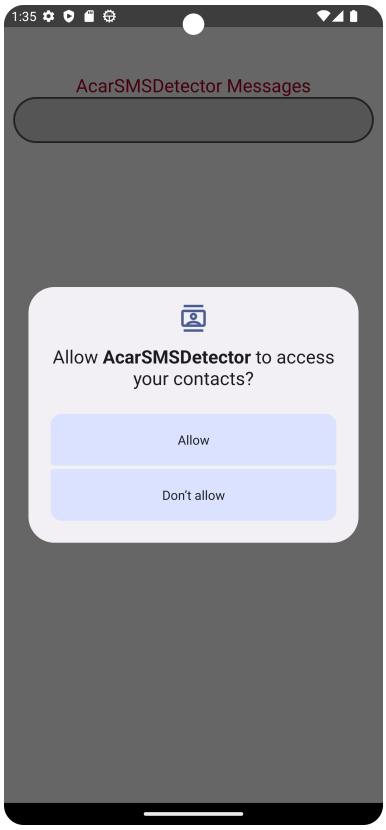

Figure 3.4: Security clearance notification

Figure 3.5: App Logo

4. RESULTS

4.0.1. User Interface Evaluation

The user interface of the application was meticulously designed to ensure an optimal user experience. It prioritizes intuitive navigation, allowing users to effortlessly manage and review potential spam messages. The interface includes clear visual indicators for spam detection status and easy-to-access customization settings. User feedback was extensively collected and analyzed, revealing high satisfaction rates. Key aspects of the interface, such as response time, layout, and ease of use, received particularly positive reviews, indicating a successful interface design that aligns well with user needs and expectations.

4.0.2. Experiments and Program Outputs

Extensive experiments were conducted to validate the application's effectiveness in identifying and blocking spam messages. These tests included a wide range of spam types, from simple unsolicited advertisements to more sophisticated phishing attempts. Program outputs were closely monitored, revealing low false positive rates, which is crucial for user trust and application reliability. The data from these experiments provided valuable insights into the application's performance under different scenarios, highlighting its robustness and adaptability to evolving spam trends.

4.0.3. Implementation and Results

The implementation of the project was carried out with a focus on efficiency, security, and scalability. The core of the application is a machine learning model trained on a comprehensive dataset of text messages, which allows for nuanced spam detection. This model was optimized for mobile devices, ensuring low latency and minimal impact on device performance. The results of the project have been highly encouraging. The application not only meets the initial objectives of effective spam detection but also enhances user privacy and security. Future developments are planned to further refine the detection algorithm, incorporating advanced machine learning techniques and real-time user feedback to stay ahead of evolving spam tactics. The project's success lays a strong foundation for further innovations in mobile communication security.

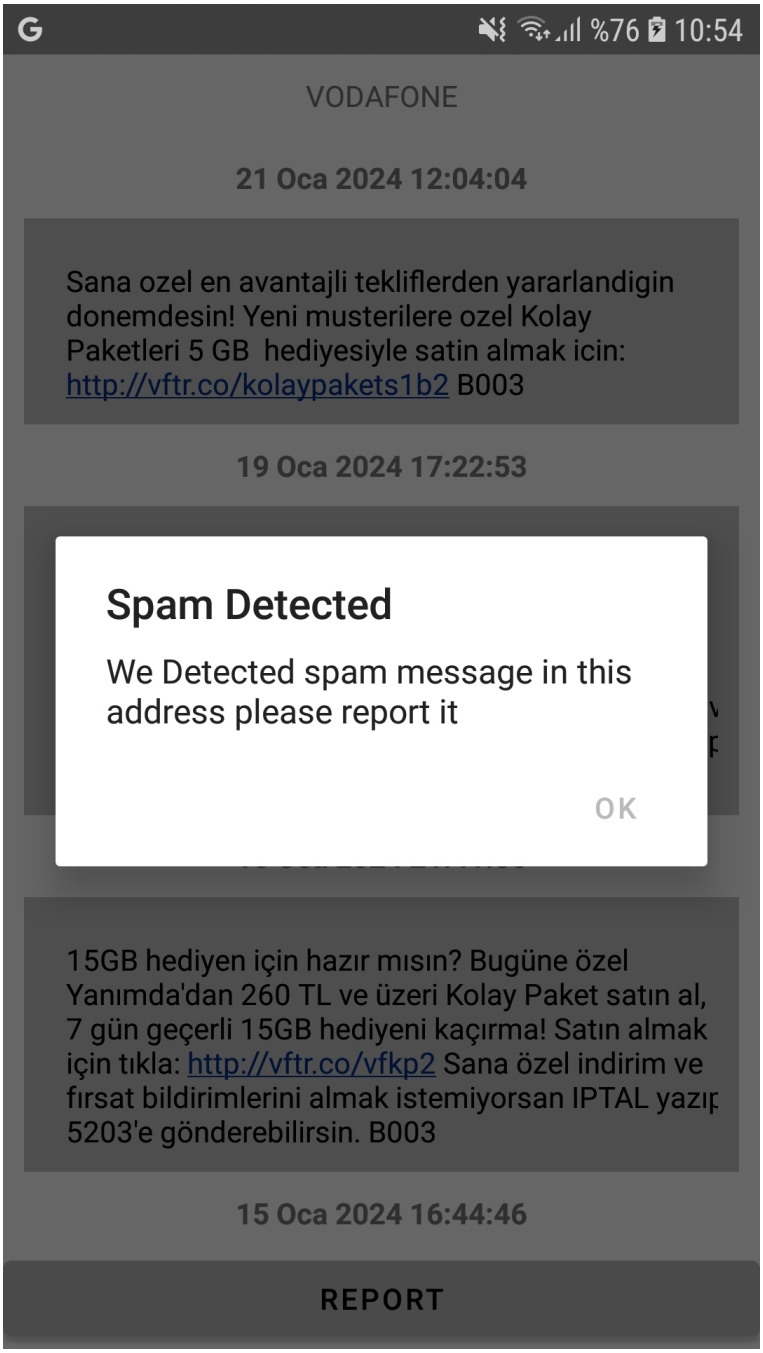

Figure 4.1: Spam Detected Warning

5. CONCLUSION

In conclusion, the AcarSMSDetector project was initiated to overcome the challenges posed by conventional spam detection methods in Android devices, offering a more robust and effective solution for identifying and blocking unwanted messages. A thorough review of existing literature and industry practices highlighted the inadequacies of traditional methods, which primarily rely on basic filtering algorithms. This necessitated a novel approach, leading to the development of AcarSMSDetector, which employs a combination of advanced machine learning techniques and user-centric design principles.

The AcarSMSDetector utilizes TensorFlow Lite and PyTorch to implement a sophisticated spam detection mechanism that operates efficiently on Android platforms. By integrating these technologies, the application not only accurately identifies spam messages but also ensures minimal impact on device performance. This is particularly crucial in maintaining a seamless user experience while providing robust spam protection.

Moreover, AcarSMSDetector transcends traditional spam detection by offering customizable user settings, allowing individuals to tailor the application according to their specific needs. This feature, coupled with the application's ability to adapt to evolving spam trends, positions AcarSMSDetector as a versatile and user-friendly solution in the realm of mobile communication security.

The modular architecture of AcarSMSDetector, developed using Flutter and Python, paves the way for future enhancements and customization. It sets a precedent for the development of sophisticated spam detection applications and serves as a valuable reference for future academic and professional research in mobile security and spam detection.

Ultimately, the AcarSMSDetector project contributes to elevating the security landscape on Android devices, empowering users to effectively combat the menace of unwanted messages and spam.

BIBLIOGRAPHY

[1] G. Sethi and V. Bhootna, "Sms spam filtering application using android," *Int. J. Comput. Sci. Inf. Technol*, vol. 5, no. 3, pp. 4624–4626, 2014.

[2] A. K. Uysal, S. Gunal, S. Ergin, and E. S. Gunal, "A novel framework for sms spam filtering," in *2012 International Symposium on Innovations in Intelligent Systems and Applications*, IEEE, 2012, pp. 1–4.

[3] V. Kouliaridis and G. Kambourakis, "A comprehensive survey on machine learning techniques for android malware detection," *Information*, vol. 12, no. 5, p. 185, 2021.

[4] S.-H. Hung, S.-W. Hsiao, Y.-C. Teng, and R. Chien, "Real-time and intelligent private data protection for the android platform," *Pervasive and Mobile Computing*, vol. 24, pp. 231–242, 2015.

[5] M. L. Mustagfirin, G. W. Wiriasto, I. M. B. Suksmadana, and I. P. Kinasih, "Android-based short message service filtering using long short-term memory classification model," *Khazanah Informatika: Jurnal Ilmu Komputer dan Informatika*, vol. 8, no. 2, 2022.

[6] M. Alzantot, Y. Wang, Z. Ren, and M. B. Srivastava, "Rstensorflow: Gpu enabled tensorflow for deep learning on commodity android devices," in *Proceedings of the 1st International Workshop on Deep Learning for Mobile Systems and Applications*, 2017, pp. 7–12.

[7] U. Fadlilah, B. Handaga, *et al.*, "The development of android for indonesian sign language using tensorflow lite and cnn: An initial study," in *Journal of Physics: Conference Series*, IOP Publishing, vol. 1858, 2021, p. 012 085.

[8] C. Rawles, A. Li, D. Rodriguez, O. Riva, and T. Lillicrap, "Android in the wild: A large-scale dataset for android device control," *arXiv preprint arXiv:2307.10088*, 2023.

[9] H. Hussain, K. Khan, F. Farooqui, Q. A. Arain, and I. F. Siddiqui, "Comparative study of android native and flutter app development," *Memory*, vol. 47, pp. 36–37, 2021.

[10] A. Tashildar, N. Shah, R. Gala, T. Giri, and P. Chavhan, "Application development using flutter," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 2, no. 8, pp. 1262–1266, 2020.

[11] H. Hariyadi, H. Yamashika, W. Mustaqim, A. Alfirdaus, M. Giatman, and R. Risfendra, “Mobile application design for learning digital engineering based on figma and android studio,” *Journal of Computer Science, Information Technology and Telecommunication Engineering*, vol. 4, no. 1, 2023.