

FRAUDSHIELD

Real time Scam detection

¹Afifa Mahat, ²Manasi Pawar, ³Ajinkya Gadekar, ⁴Ms. Neha Mane

¹Student, ²Student, ³Student, ⁴Guide

¹Department of Computer Science,

¹Dr. D. Y. Patil Polytechnic, Kolhapur, India

Abstract : Due to the rapid development of smartphones and internet-based communication, online scams/phishing attacks are becoming a major threat for mobile users. Cybercriminals are sending fraudulent information and malicious links via social media, messaging apps, and emails. Many users are unknowingly copying the scam information, which may lead to financial losses. Existing security tools like antivirus software are mainly focused on detecting malware or network attacks. They may not be effective in detecting scam information embedded in copied text.

In this research, the researcher proposes a mobile application named “FraudShield Lite - Real-Time Scam Detector” for detecting scam-related text and URLs. This system monitors the clipboard for copied text or URLs. It uses Artificial Intelligence (AI) and Natural Language Processing (NLP) for analysing the copied text. This mobile application is built using the Android environment, where the application is developed using Android Studio with Java. In addition, the scam detection is done using the Python environment, where the Chaquopy library is integrated for the development of the mobile application.

When the user copies the text or URL, the system will automatically analyse the copied information for detecting scam patterns. If the copied information is malicious, the application will immediately alert the user. This application is offline-based, which is more efficient for protecting the user’s privacy.

The proposed system is a simple application for enhancing mobile security.

IndexTerms - Scam Detection, Cybersecurity, Fraud Detection, Python, Artificial Intelligence, Phishing Protection.

I. INTRODUCTION

The use of smartphones, along with the widespread use of internet-based communication, has altered the dynamics of interaction among users. However, this has also led to an increase in the probability of cyber fraud. Scam messages, fake advertisements, and scam links are commonly used by fraudsters to trick users into divulging sensitive information or carrying out financial transactions.

Scam messages are commonly circulated via messaging apps, where users may unintentionally copy scam links or messages. Conventional security software, such as antivirus programs, is only capable of detecting malicious files or suspicious sites but cannot monitor the clipboard, where scam links may be temporarily copied.

In this context, there is a need for a smart mobile application that is capable of detecting scam-related text. FraudShield Lite is an application that monitors the clipboard and uses AI-based detection to scan the copied text.

II. NEED OF THE STUDY

With an increase in online scams and phishing attacks, the situation has become a major concern among internet users across the globe. According to cybersecurity reports, millions of people become victims of online scams every year due to a lack of awareness or inappropriate security tools.

However, the existing security tools have some major drawbacks:

- They only protect against online threats at the network level, such as downloading viruses or accessing unsafe websites.
- They do not protect against clipboard attacks, where online scam messages or websites are temporarily stored.
- Many security tools require an Internet connection at all times, which is not always available.
- Antivirus programs can consume a lot of system resources, affecting device performance.

Therefore, users are still at a greater risk of text-based online scams using messaging applications or copied online scam websites.

FraudShield Lite is designed to solve these problems with a lightweight and intelligent security tool that can function directly on the device and protect users from online scams even before they interact with the scam content.

III. RESEARCH METHODOLOGY

The research methodology provides a detailed explanation of the research approach that was adopted to design, develop, and evaluate the FraudShield Lite – Real-Time Scam Detector system. The research methodology adopted for this research includes the study population, data sources, system framework, and the system implementation process to identify the text and link-based scam content on mobile devices.

3.1 Population and Sample

The population of this research includes smartphone users who regularly use internet-based communication platforms such as messaging applications, social media networks, and email services. The population of this research will be exposed to various links, promotional messages, or notifications that may contain scam-related content.

For this research, a sample of the most commonly used scam messages, phishing links, and text patterns were collected from various publicly available cybersecurity resources. These include various publicly available cybersecurity resources containing information about the most commonly used scam messages, phishing links, and text patterns.

The sample collected for this research includes the following types of scam messages that are commonly used to trick the end-user:

- Fake lottery or prize-winning messages
- Phishing links that mimic banking or payment-related services
- Fake job offers or advertisements
- Suspicious URLs containing misleading domain names

3.2 Data and Sources of Data

The system will be designed to identify the scam content based on the dataset containing the keywords, patterns, and URLs of the scam content. The data used in this research was collected from the following sources:

- Publicly available phishing databases and cybersecurity resources
- Various online security awareness resources
- Examples of various scam messages available on messaging platforms or emails
- Research articles related to the detection of phishing and scam content

This gathered information includes commonly used keywords or phrases such as “Congratulations, you have won,” “urgent payment required,” “verify your account immediately,” etc.

In addition to the keyword pattern, the system also analysed the pattern of suspicious URL structures. These include the use of shortened URLs or fake website domains.

This gathered information was then used to develop a set of detection rules that enable the system to identify suspicious content by detecting the copied content on the device’s clipboard.

3.3 System Framework

The FraudShield Lite system follows a system framework that includes various components that work together to detect scam content.

Clipboard Monitoring Module

This module monitors the clipboard of the mobile device for any newly copied content or URLs. Once the user copies any content from the internet or sends a message to another user, the module captures the content or URL copied by the user.

Detection Engine

This module is written in Python. Once the module captures the content or URL copied by the user, the detection engine analyses the content to determine whether it is a scam message or not. To do this, the detection engine performs the following actions:

- It checks for keyword matches for commonly used scam messages or phrases.
- It checks for pattern matches for suspicious content or URL structures.
- It performs a simple Natural Language Processing (NLP) analysis to check the context of the message.
- URL pattern analysis to check for phishing URLs.
- Once the detection engine analyses the content copied by the user, it checks the content with the gathered dataset of scam content to determine whether the content or URL copied by the user is a scam message or not.

Alert Module

Once the detection engine determines that the content or URL copied by the user is a scam message or content, the alert module sends a notification to the user that the content or URL copied by the user is a fraudulent message or content.

User Interface

The user interface enables the user to view the alerts and interact with the application. It has a simple and user-friendly interface to enable the user to understand the alerts generated by the application.

3.4 Implementation Method

The implementation of the FraudShield Lite application involved the following phases.

Phase 1: Requirement Analysis

In the first phase, the requirements of the application were determined. This involved identifying the key features of the application, including the clipboard monitoring feature, the scam detection feature, and the notification alerts.

Phase 2: System Design

During this phase, the design of the application was determined. This involved the creation of flowcharts and system diagrams to illustrate the interaction between the different components of the application.

Phase 3: Application Development

During this phase, the interface of the application was developed using Java and the Android Studio platform. It involved the development of the application interface and the implementation of the scam detection engine using Python.

The Python language offers powerful tools for the detection of scams and phishing attacks.

Integration of Java and Python

ChaQuopy integrates Python with Java to enable the execution of Python scripts within the Java application.

Phase 4: Testing

During this phase, the application was tested with different examples of phishing and scam messages. During the testing, the following were determined:

- Accuracy of the scam detection
- Speed of the scam detection
- Performance of the application

Phase 5: Deployment

Once the application was tested, it was deployed on the Android platform and installed on the devices to enable the testing of the application.

IV. RESULTS AND DISCUSSION

This section presents the results obtained from testing the FraudShield Lite system and discusses its performance in detecting scam-related messages and suspicious links in real time.

4.1 System Testing Results

The FraudShield Lite system's application was tested using various copied text messages and URLs containing legitimate and scam-related messages. The test aimed to determine how accurately the system could detect fraudulent messages.

Several test cases were developed using common patterns of scams such as messages related to winning prizes, fake banking messages, and phishing links. When these messages were copied into the device's clipboard, the system's application correctly analysed the messages and generated a warning when suspicious patterns were detected.

From the test results, it was clear that the system could correctly identify most of the scam-related messages containing phishing keywords and suspicious URL patterns. When normal messages were copied into the device's clipboard, the system did not generate any warning, indicating that it could differentiate between normal and suspicious messages.

4.2 Detection Performance

The performance of the system in detecting messages was evaluated using various factors such as accuracy, response time, and usability.

Accuracy: The system's detection engine could correctly identify most of the scam messages containing predefined phishing keywords and suspicious URL patterns.

Response Time: The analysis process took almost no time after the user copied the information into the clipboard. Thus, the response time is considered real-time.

Usability: The alert notification was simple, enabling the user to understand the potential threat without affecting the normal use of the device.

The keyword matching method, along with the pattern analysis, has been successful in detecting the most common types of scams, which are usually present in social media messages or emails.

4.3 Discussion

The results obtained from the experiment prove that the FraudShield Lite application is successful in detecting scam messages and suspicious links, thereby protecting users from potential fraud.

The first advantage of the system is that it is lightweight, enabling the application to function on mobile devices. Unlike other security-related apps, the FraudShield Lite application does not require the internet to function. Moreover, it uses simple analysis techniques, which are effective.

Another important advantage of the system is that it warns the user before a potential threat occurs, helping protect the user from phishing attacks or financial fraud.

However, the application currently relies mainly on keyword matching and pattern recognition, which may fail to identify new types of scam attacks. Future improvements could include the use of machine learning algorithms and larger phishing datasets to improve detection accuracy and adapt to evolving cyber threats.

Overall, the experimental results demonstrate that the FraudShield Lite application can help improve user awareness and provide an additional layer of protection against online scams.

V. ACKNOWLEDGMENT

I wish to express my sincere thanks to my project guide and faculty members for their valuable guidance, support, and encouragement in the development of this research work titled “FraudShield Lite – Real-Time Scam Detector.”

I also wish to express my sincere thanks to my institution for providing me with the suitable academic environment, resources, and facilities required to complete this research work successfully.

Finally, I wish to express my sincere thanks to all the researchers and cybersecurity resources whose published work and data were useful in the development of this research work related to scam detection techniques.

REFERENCES

- [1] Garera, S., Provos, N., Chew, M. and Rubin, A.D. 2007. A framework for detection and measurement of phishing attacks. Proceedings of the ACM Workshop on Recurring Malcode (WORM), pp. 1–8.
- [2] Fawcett, T. 2006. An introduction to ROC analysis. Pattern Recognition Letters, 27(8): 861–874.
- [3] Axelsson, S. 2000. The base-rate fallacy and its implications for the difficulty of intrusion detection. ACM Transactions on Information and System Security, 3(3): 186–205.
- [4] Sahingoz, O.K., Buber, E., Demir, O. and Diri, B. 2019. Machine learning based phishing detection from URLs. Expert Systems with Applications, 117: 345–357.
- [5] Aburrous, M., Hossain, M.A., Dahal, K. and Thabtah, F. 2010. Intelligent phishing detection system for e-banking using fuzzy data mining. Expert Systems with Applications, 37(12): 7913–7921.
- [6] Sahoo, D., Liu, C. and Hoi, S.C.H. 2017. Malicious URL detection using machine learning: A survey. ACM Computing Surveys, 50(6): 1–36.