




SpamShield

Detect, Block and Protect your mobile life



Proof of concept : What is it and why we need it

Spam messages are a growing problem that affects millions of people worldwide. They not only cause frustration and lost productivity, but can also lead to financial loss and even pose a threat and jeopardize personal safety. The spam detection app project aims to address this problem by providing an innovative solution that can detect spam messages in two ways - by detecting incoming messages and by reading messages from the notification space of the user's phone. The app will use a graph database at the backend to analyze patterns in malicious messages using collaborative filtering and alert the police. This project is important because it has the potential to reduce the negative impact of spam messages on people's lives and improve their overall well-being.



Ideas for implementation

- 01 We will be creating an app that will allow the user to read all the text messages they receive and automatically classify it as spam and not spam
- 02 Alternatively, if the users do not wish to set our app as the default one, then we will provide an option for our app to read the text and emails directly from the notification centre and alert the users accordingly
- 03 We will create a model to identify patterns in the messages sent using graph databases and identify any malicious players and report them to the authorities (COLLABORATIVE FILTERING)



Proposed methodology

First, create an NLP based Deep learning model with feed forward architecture to classify messages as spam and not spam (aka, ham). We also create a secondary graph database in the backend that will help us to draw connections between malicious actors.

Once trained, we can store the state of the model into the application.

We can then build our Android application using kotlin and Android studio. We should be able to connect and read people's messages directly from the Google messages API. Else, we provide a method for the application to read the messages from the notifications bar directly.

Design the UI and backend of the system. We make sure to store the sender and the message in the cloud database for further processing of messages. We can follow the MVC and Observer Pattern for designing the main application.

Once completed, we can unit test the app and deploy it as an APK.



Techstack used

1. Kotlin: To create the UI/UX and the functionality of the application
2. React Native / Flutter : Development Framework to design the application
3. NLTK or Spacy : To develop the NLP models
4. OpenSSL : Encryption library to protect user data
5. Firebase or AWS : Speed and Scalable backend development
6. Firebase realtime database : Serverless database applications
7. Neo4j : Secondary database application to map and discover patterns in messages
8. Travis CI or Jenkins: To create CI/CD pipeline
9. Google Safe Browsing APIs : An API provided by Google with a list of malicious web pages



Innovations Incorporated

Two major innovations have been incorporated into this application :

1. The ability to use the application as a primary messaging app or as a secondary messaging app gives users the option and flexibility to choose whether they want to use our app or a different application while also ensuring that they will be protected against spam messages
2. By using a graph backend database and finding out connections between senders, it is possible for the police to track down and nab the criminals in a much more easier and efficient pattern



Feasibility of Solution

The spam detection app solution is a feasible and innovative approach to detecting spam messages. The use of a graph database at the backend to analyze patterns in malicious messages using collaborative filtering is an efficient way to detect spam messages quickly and accurately. In fact, many websites with heavy traffic like Twitter also use graph databases in the Backend. By using a service like Firebase or AWS, we can ensure the scalability of our application and also ensure that we get the data at a low latency. We can also use the same model and approach for different scenarios, making it an ideal starting point for new innovations. Also, since we are using common design practices, It will make it easier for others to understand and develop their features on top of our application.

The app's alert system can provide useful information to the police, such as the sender's phone number, the content of the message, and the time it was sent. This information can be used to track down the source of spam messages and help the police to nab criminals who use spam messages to commit crimes, such as fraud or phishing. The app's ability to analyze patterns in spam messages can also be used by law enforcement agencies to identify and track organized crime networks that use spam messages as a means of communication. Overall, the spam detection app solution has the potential to be a powerful tool in the fight against spam messages and cybercrime.



Future scope

- Advanced geolocation: Use location data of the sender to track the precise location of the sender
- Sentiment analysis: used to identify threatening messages
- Real Time Translation: A language translation tool can be built into the application for the police to translate any text in different languages
- Encryption Detection: Develop a technique that can detect and flag messages that are encrypted