OPTIMIZING SPAM FILTERING WITH MACHINE LEARNING

Bussiness Recurement

A business requirement for an SMS spam classification system would include the ability to accurately identify and flag spam messages, protect customs from unwanted or harmful messages, and comply with industry regulations and laws regarding spam messaging. Additionally, the system should be able to handle a high volume of messages, integrate with existing systems and databases, and provide reporting and analysis capabilities to track performance and improve the system over time. The system should also have an easy-to-use interface and be easy to maintain and update.

Hidalgo et al have analyzed that how Bayesian filtering technique can be used to detect SMS Spam. They have built two datasets one in English and another in Spanish. Their analysis shows that Bayesian filtering techniques that were earlier used in detecting email spam can also be used to block SMS Spam

How do spam filters protect your business?

Each filter category has a combination of controls that grant it the ability to distinguish and separate spam from legitimate emails, and also to block emails that contain known malware

Message content analysis

This checks the headers and body of a message for common telltale signs of spam, such as frequent misspellings and images with very poor quality. The message is thus given a score that determines the corresponding action a spam filter will take on it. Specifically, the spam filter can deliver, grey list, quarantine, or delete the message.

Malware scanning

A spam filter can use one or many antivirus programs to check if email attachments contain known malware

Grey listing

Grey listing is the process of rejecting suspicious emails and requesting email servers to send the rejected messages again. Since spammers' mail servers are often dedicated to sending countless spam emails, they take much longer to process the grey lister's requests than regular servers do. This delay helps to confirm suspected emails as spam.