

CATHOLIC UNIVERSITY OF BUKAVU



B.P.285 BUKAVU

FACULTY OF SCIENCES

Department of Computer Science

Development of a messaging application for communication and detection of spam on a mobile network, case study of Airtel, Vodacom and Orange.

Presented by : **MURHULA BYABUSHI Christian**
*Dissertation presented and defended in order to obtain the
degree of Bachelor in Computer Science.*

Option: Network and Telecommunications
Degree: Final year of Bachelor

Supervised by: ***Hw.* MUGISHO MUSHEGERHA Youen**
Directed by : ***Ph.D.* Elie ZIHINDULA**

Academic year: 2022-2023

Contents

Introduction	4
0.1 Context and generalities	4
0.2 Problematic	4
0.3 Hypotheses	5
0.4 Delimitation and objectives	5

List of Figures

List of Tables

Introduction

0.1 Context and generalities

With the increasing of use of mobile devices and the rise of mobile communication, the number of text messages sent every day has grown exponentially. According to *Statista*, a company that provides market and consumer data on a wide range of topics, including digital media and technology; the number of mobile messages sent worldwide in 2020 was 3.5 trillion [6]. Along with this growth, there has been an increase in the number of spam messages that aim to deceive people into providing personal information, sending money, menacing to death or taking other actions that benefit the scammer.

To address this problem, the development of a messaging application with advanced spam detection capabilities is essential. This dissertation focuses on the development of such an application for mobile networks, with a specific case study of Airtel, Vodacom and Orange.

Indeed, Airtel, Vodacom, and Orange are major telecommunications operators which mostly function in Democratic Republic of Congo, with a significant market share and importance in online services, including messaging.

0.2 Problematic

In communication domain, we use mobile devices or phones for sharing *SMS*, Email, chats by using some specific apps. Among all these we use specifically *SMS* for personal and professional information sharing [4]. The SMS stands for Short Message Service, which is a text messaging service for mobile phones and other mobile devices. It allows users to send and receive short messages of up to 160 characters [5]. It also possible to send or receive automatic SMS which are not sent by human, whereas by using web interface or API [3].

Due to all these means, we are facing against malicious attacks inside of messages which are commonly responsible of annoyance of users, wasting mobile network resources and potentially introducing security risks like *Simjacker* vulnerability which was discovered in 2019, which allows attackers to exploit a weakness in the SMS messaging system to remotely install spyware on mobile devices [2]. Besides, the spam messages are increasing likelihood of users by leading them to ignore important messages or being more hesitant to engage with *SMS* marketing campaigns [1].

Considering all above issues caused by spam, what are key technical challenges that could be addressed in messaging apps which can effectively facilitate the communication as well as detecting and filtering spam messages ?

0.3 Hypotheses

Using the content-based filtering techniques, which involves analyzing the content of messages and determining it is spam or not. This would be done by utilizing the Machine learning algorithms which are : **Naive Bayes, Logistic Regression, and Supper vector Machines**. All these would be combined by the ensemble methods for making a more predictive model [7].

Besides, we would integrate the model inside of the system able of adding technically in a blacklist or whitelist suspect users based on the specific probability of being a potential attack.

0.4 Delimitation and objectives

Bibliography

- [1] Guangquan Chen, Weijun Wang, and Xuan Zhou. A survey on sms spam filtering techniques. *Journal of Network and Computer Applications*, 80:149–159, 2017.
- [2] Catalin Cimpanu. Simjacker vulnerability exploited for surveillance by at least one nation-state. *ZDNet*, 2019.
- [3] Sunil Kumar Jangir, Manoj Kumar Sharma, and Pawan Kumar Gupta. Design and implementation of sms gateway api for mobile communication networks. *International Journal of Computer Applications*, 151(9):1–5, 2016.
- [4] M Lavanya and KR Aruna. Sms spam detection using deep learning. *Journal homepage: www.ijrpr.com ISSN*, 2582:7421.
- [5] Gwenaél Le Bodic. *Mobile messaging technologies and services: SMS, EMS and MMS*. John Wiley & Sons, 2005.
- [6] Statista’s own team of researchers and analysts. *Number of mobile messages worldwide from 2019 to 2023 (in trillions)*. <https://fr.statista.com/>, 2020.
- [7] Sebastian Raschka and Vahid Mirjalili. Python machine learning: Machine learning and deep learning with python. *Scikit-Learn, and TensorFlow. Second edition ed*, 3, 2017.