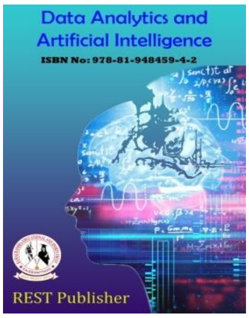
Data Analytics and Artificial Intelligence

Vol: 3(1), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/3/1/22


Data Analytics and Artificial Intelligence
ISBN No: 978-81-948459-4-2
REST Publisher

Classifying Message Application Using Kotlin

***Parthiban M A, AnandKumar.Y, Raghul.S, Saran Sanjay.R, SivaKumar.P**

Veltech high-tech Dr.Rangarajan Dr, Sakunthala Engineering College, Chennai, Tamil Nadu, India.

*Corresponding Author Email: parthiban.m@velhightech.com

Abstract: *Over the past few years, short message service (SMS) usage has significantly increased. This service is used to deliver text messages by billions of people. Service providers have launched a number of popular applications, including mobile banking, summons checkpoints, SMS chat, and others. This chapter explores the numerous SMS applications that are available to users and provides an outline of how this service isprovided. We examine the causes of its success and the problems that need to be solved. We also look at upcoming trends and the difficulties that to improve this service, certain obstacles must be overcome. This chapter should help you understand how SMS applications work and what to expect from them going forwards given the improvements to current SMS and technological advancement***.** *We propose a privacy-preserving Naive Bayes classifier and apply it to the problem of private text classification. In this setting, a party (Alice) holds a text message, while another party (Bob) holds a classifier. At the end of the protocol, Alice will only learn the result of the classifier applied to her text input and Bob learns nothing. Our solution is basedon Secure Multiparty Computation (SMC). Our Rust implementation provides a fast and secure solution for the classification of unstructured text. Applying our solution to the case of spam detection (the solution is generic, and can be used in any other scenario in which the Naive Bayes classifier can be employed), we can classify an SMS as spam or ham in less than 340 ms in the case where the dictionary size of Bob's model includes all words (n 5200) and Alice's SMS has at most m 160 unigrams. In the case with n 369 and m 8 (the average of a spam SMS in the database), our solution takes only 21ms.*

Keywords: *Android, Kotlin, Firebase, XML, Android App Studio.*

1. INTRODUCTION

The most common and popular form of communication is the short message service (SMS). In many regions of the world, the term "SMS" is used to refer to both user activity and all forms of short text messaging. It is being used as a platform for online offerings, banking updates, agricultural information, and product advertising and promotion. SMS marketing, often known as direct marketing, uses SMS technology. There are times when SMS marketing causes users to be disturbed. Spam SMS is the term used to describe these SMSs. One or more unwanted, unsolicited messages are referred to as spam. sent or posted to the users as part of a bigger group of messages with essentially the same content SMS spam serves commercial and marketing reasons. disseminating inappropriate pornographic content and internet offers, as well as the marketing of numerous items. Because of this, the global issue of spam SMS floods has gotten much worse. Because SMS communication is becoming more and more popular, SMS spamming has surpassed previous spamming strategies like email and twitter. Although email opens only 20 to 25 percent of the time within 24 hours of receipt, SMS opens more than 90% of the time and within 15 minutes of reception. Consequently, there is aclear need for an effective SMS spam detection method. Numerous studies have been done on spam detection methods for email, Twitter, the web, and social media. On the other hand, very few studies on SMS spamdetection have been carried out. Detecting spam SMS ismore difficult than detecting spam email. due to SMS's limited length, use of regional content and abbreviations, and lack of header information compared to email We consider the scenario in which there are two parties: one possesses the private data to be classifiedand the other party holds a private model used to classify such data. In such a scenario, the party holding the data (Alice) is interested in obtaining the classification result of such data against a model held by a second party (Bob) so that, at the end of the classification protocol, Alice knows solely the input data and the classification result, and Bob knows nothing beyond the model itself. This scenario is a very relevant one. There are many situations where a data owner is not comfortable sharing a piece of data that needs classification (think of psychological or health related data). Also,a machine learning model holder might not want to/cannot reveal the model in the clear for intellectual property issues or because the model reveals information about the data set used to train it. Thus, both parties have proper incentivesto participate in a protocol providing the joint functionality of private classification. Due to these concerns, mechanisms such as Secure Mul- tiparty Computation (MPC) [20], Differential Privacy (DP) and Homomorphic Encryption (HE) can be used to build privacy-preserving solutions. MPC allows two or more parties to jointly compute a function over their private inputs without revealing any information to the other party,whereas HE is an encryption scheme that allows per- forming computations on encrypted data without having to decrypt it. And, DP is a technique that adds ran- dom noise to queries, toprevent an adversary from learn- ing information about any particular individual in the data set.

Our main goal is to propose protocols for privacy-preserving text classification. By carefully selecting cryptographic engineering optimizations, we improve upon previous results by Reich *et al.* [55] by over an order of magnitude achieving, to the best of our knowledge, the fastest text-classification results in the available literature (21ms for an average sample of our data set). More specifically, we propose a privacy- preserving Naive Bayes classification (PPNBC) based on MPCwhere given atrained model we classify/predict an example without revealing any additional information to the parties other than the classification result, which canbe revealed to one specified party or both parties. We then apply our solution to a text classification problem: classifying SMSes as spamor ham.

2. LITERATURE SURVEY

SMS spam detection for Indian messages: The growth of the mobile phone users has led to adramatic increase in SMS spam messages. Thoughin most parts of the world, mobile messaging channel is currently regarded as “clean” and trusted, on the contrast recent reports clearly indicate that the volume of mobile phone spam is dramatically increasing year by year. It is an evolving setback especially in the Middle East and Asia. SMS spam filtering is a comparatively recent errand to dealsuch a problem. It inherits many concerns and quickfixes from Email spam filtering. However, it fronts its own certain issues and problems. This paper inspires to work on the task of filtering mobile messages as Ham or Spam for the Indian Users by adding Indian messages to the worldwide available SMS dataset. The paper analyses different machine learning classifiers on large corpus of SMS messages for Indian people. Due to these concerns, mechanisms such as Secure Mul- tiparty Computation (MPC) [20], Differential Privacy (DP) and Homomorphic Encryption (HE) can beused to build privacy-preserving solutions. MPC allows two or more parties to jointly compute a function over their private inputs without revealing any information to the other party, whereas HE is an encryption scheme that allows per- forming computations on encrypted data without having to decrypt it. And, DP is a technique that adds ran- dom noise to queries, to prevent an adversary from learn- ing information about any particular individual in the data set. SMS is one of the most used telecommunication service in the world. It allows mobile phone users to send and receive a short text (which has 160 7-bit characters maximum). Due to advantages such as reliability (since the message reaches the mobile phone user), low cost to send an SMS (especially if bought in bulk), the possibility of personalizing, and immediate delivery, SMS is a widely used communication medium for commercial purposes, andmobile phone users are flooded with unsolicited advertising. SMSes are also used in scams, where someone triesto steal personal information, such as credit card details, bank account information, or social security numbers. Usually, the scammer sends an SMS with a link that invites a person to verify his/her accountdetails, make a payment, or that claims that he/she hasearned some amount of money and needs to use the link to confirm. In all cases, such SMSes can be classified as spam. Machine learning classifiers can be used to detect whether an SMS is a spam or not (ham). During the training phase, these algorithms learn a model from a data set of labeled exam- ples, and later on, are used during the classification/prediction phase to classify unseen SMS es. In a Naive Bayes classifier, the model is based on the frequency that each word occurs in the training data set. In the classification phase, based on these frequencies, the model predicts whether an unseen SMS is spam or not. A concern with this approach is related to Alice’s privacy since she needs to make her SMSes available to the spam filtering service provider, Bob, whichowns the model. SMSes may contain sensitive information that the user would not like to share with the service provider. Besides, the service provider also does not want to reveal what parametersthe model uses (in Naive Bayes, the words and their frequencies) to spammers and concurrent service providers. Our privacy-preserving Naive Bayes classification based on MPC, provides an extremely fast secure solution for both parties to classify SMSes as spam or ham without leaking any additional information while maintaining essentially the same accuracy as the original algorithm performed in the clear. While our experimental treatment is focused on SMS messages, the same approach can be naturally generalized to classify shortmessages received over Twitter or instant messengers such as WhatsApp or Signal.among the best models to be used for a multiclass SMSclassification.

SMS Spam Detection using Machine Learning and Deep Learning Techniques

The number of people using mobile devices increasingday by day. SMS (short message service) is a text message service available in smartphones as well as basic phones. So, the traffic of SMS increaseddrastically. The spam messages also increased. The spammers try to send spam messages for theirfinancial or business benefits like market growth, lottery ticket information, credit card information, etc. So, spam classification has special attention. In this paper, we applied various machine learning and deep learning techniques for SMS spam detection. we useda dataset from UCI and build a spam detection model. Our experimental results have shown that our LSTM model outperforms previous models in spam detection with an accuracy of 98.5%. We used python for all implementations

SMS: The Short Message Service

Although it is a widely used communication mechanism for cell phone users, SMS is far more than just a technology for teenage chat. SMS technology evolved out of the global system for mobile communications standard, an internationally accepted cell phone network specification the European Telecommunications Standards Institute created. The 3rd Generation Partnership Project maintains the SMS standard. SMS messages are handled via a short message service center that the cellular provider maintains for the end devices. The SMSC can send SMS messages to the end device using a maximum payload of 140 octets. This defines the upper bound of an SMS message to be 160 characters using 7-bit encoding. It is possible to specify other schemes such as 8-bit or 16-bit encoding, which decreases the maximum message length to 140 and 70 characters, respectively.

Short Message Service (SMS) Spam Filtering using Machine Learning in Bahasa Indonesia

Short Message Service (SMS) is an essential communication tool in Indonesian society. Companies use SMS as a promotion tool but unfortunately some individuals use SMS to send spam messages. A smartphone user in Indonesia has had an experience with these spam and promotional messages. This studypresents a model to classify spam, promotion and ham messages based on Indonesian text messages. The model was trained with 4,125 text messages, tested with 1,260 text messages. A 10-fold cross validation method was used to evaluate the classifiers and the results show that Random Forest (94.62%), Multinomial Logistic Regression (94.57%), SupportVector Machine (94.38%), and XGBoost (94.52%) are

Comparative Study of Machine LearningAlgorithms for SMS Spam Detection

The short message service (SMS) became popular after it was initially provided as a service in the second- generation (2G) terrestrial mobile network architecture (Global System for Mobile Communication - GSM). Itspopularity has been exploited by some advertising companies and others to spread unwanted advertising, communicate advertising offers, and send unwanted material to the end users. These undesirable messages, known as spam, make it difficult for the users to receivethe desirable messages and make them frustration and irritation. Consequently, there are measures that various experts have implemented in filtering out these spam messages and blocking them from reaching the end users. Most of the solutions have followed the success of email spam filtering and utilized machine learning techniques to filter spam messages. The popular machine learning techniques that have successfully been used include logistical regression, Naïve Bayes algorithms, Support Vector Machine (SVM), and neuralnetworks. The present study adopts these techniques in filtering spam messages and measures their accuracy to determine the most effective method of filtering spam messages. Based on the findings, the neural network performs best as the trained classifier model used to classify incoming messages as ham or spam

SMS spam detection and comparison ofvarious machine learning algorithm

Past few years have seen increase in the number of spam emails and messages. Legal, economic and technical measures can be used to tackle spam sms's nowadays. A key role is being played by Bayesian filters in stopping this problem. In this paper, we analyzed and studied the relative strengths of various machine learning algorithms in order to detect spam messages which are sent on mobile devices. We have acquired the data from on open public dataset and prepared two datasets for our testing and validation purposes. Accuracy in detecting spam messages was the first priority in ranking these algorithms. Our resultsclearly demonstrate that different machine learning algorithms under different features tend to perform differently in classifying spam messages.

3. EXISTING AND PROPOSED SYSTEM

India has one of the densest and prospective markets forcellular phones, and mobile service providers have a strict policy about providing access to their customer bases. Many consumers activate “Do Not Disturb” services that disallow mass publicity calls and messages. However, Bulk SMS service provider in Mumbai maintain databases of people who are open to mass messages. This means that a company engaging in this kind of marketing can actually reach out to a target audience more efficiently. Not all bulk SMSreseller providers have extensive resources however, and it is up to you to select the right vendor. Bulk SMSs reach the target audience with greater efficiencythan television or print advertising because they reach the client directly. A message on your phone is something that you can always refer to later; and it doesn’t go ignored as marketing calls often do. On the other side of the playing field, a bulk SMS reseller provider can reach out to thousands of people within a limited cost. While conventional advertising cannotguarantee the attention of your intended target audience, bulk SMSs will allow you a deeper reach into the market without spending as much as you would when be engaging in conventional marketing! Moreover, in this digital world, smartphones are the best partner. Without it, nobody survives. Even the oldaged or illiterate people used to have smartphones and they try to read all messages. These people never read email as they don’t have an email account. Hence, there may be no doubt that Bulk SMS service will assist you to connect with your audiences better. Get your Bulk SMS service through us thousands of your audience at the same time. It is believed that an SMS isopened within five minutes of its receipt, making it an effective mediumto attain out on your target market.ies

4. PROPOSED SYSTEM

The proposed system used advanced methodologies to facilitate ease of use and makes the messages more filtered and cleaner to view. The transactions from various apps (like gpay , phonepe , paytm etc) are arranged dynamically based on the content they possess . Otp's(One Time Passwords) are automatically from the device after a specified amount of time which makes it more secure and helps the comtribute to the free space on the device . Thesemessages are automatically converted into modules based on a timed basis as all messages from a certain timeline are clubbed together enabling to view it easier. Spam messages are automatically seperated from the other essential messages which makes it easier to identify messages we dont actually need. These spam messages are also converted into seperated folders to make them to be deleted easier.

5. TOOL DESCRIPTION

Android: Android is a mobile operating system based on a modified version of the Linux kernel and otheropen- source software, designed primarily for touch screen mobile devices. Android is developed by a consortium of developers known as the Open Handset Alliance and commercially sponsored by Google.

About android app:Android App is software designed to run on anAndroid device or emulator. The term also refers to an APK file which stands for Android package. This file is a Zip archive containing app code, resources, and meta information. Android apps can be written in Kotlin, Java, and C++ and are run inside Virtual Machine.

Kotlin the programming language: Kotlin is a cross-platform, statically typed, general- purpose programming language with type inference. Kotlin is designed to interoperate fully with Java, and the JVM version of Kotlin's standard library depends on the Java Class Library but type inference allows its syntax to be more concise. Kotlin mainly targets the JVM, but also compiles to Java Script or native code via LLVM Language development costs are borne by JetBrains, while the Kotlin Foundation protects the Kotlin trademark.

Google fire base: Firebase is a set of hosting services for any type of application (Android, iOS, Java script, Node.js, Java, Unity, PHP, C++ ...). It offers NoSQL and real-time hosting of databases, content, social authentication (Google, Face book, Twitter and Github), and notifications, or services, such as a real-time communication server. Firebase is a Backend-as-a-Service (BaaS) app development platform that provides hosted backend services such as a realtime database, cloud storage, authentication, crash reporting, .

Secure socket layer: SSL stands for secure sockets layer. Protocol for web browsers and servers that allows for the authentication, encryption & decryption of data sent over the internet.\

Real time database: Fire Base is a Real time Data Base. Having a real- time database is the standout feature of the Firebase framework. Firebase caters to a cloud-hosted database in which the data is stored as JSON and further synchronized constantly to each associated client. Having a real-time database instance

Android: Android is a mobile operating system based on a modified version of the Linux kernel and other open- source software, designed primarily fortouch screen mobile devices. Android is developed by a consortium of developers known as the Open Handset Alliance and commercially sponsored by Google.

About android app: Android App is software designed to run on an Android device or emulator. The term also refers to an APK file which stands for Android package. This file is a Zip archive containing app code, resources, and meta information. Android apps canbe written in Kotlin, Java, and C++ and are run inside Virtual Machine.

Kotlin the programming language: Kotlin is a cross-platform, statically typed, general- purpose programming language with type inference. Kotlin is designed to interoperate fully with Java, and the JVM version of Kotlin's standard library depends on the Java Class Library but type inference allows its syntax to be more concise. Kotlin mainly targets the JVM, but also compiles to Java Script or native code via LLVM Language development costs are borne by JetBrains, while the Kotlin Foundation protects the Kotlin trademark.

Google fire base: Firebase is a set of hosting services for any type of application (Android, iOS, Java script, Node.js, Java, Unity, PHP, C++ ...). It offers NoSQL and real-time hosting of databases, content, social authentication (Google, Face book, Twitter and Github), and notifications, or services, such as a real-time communication server. Firebase is a Backend-as-a-Service (BaaS) appdevelopment platform that provides hosted backend services such as a realtime database, cloud storage, authentication, crash report

Secure socket layer: SSL stands for secure sockets layer. Protocol for webbrowsers and servers that allows for the authentication, encryption & decryption of data sent over the internet.\

Real time database*:* Fire Base is a Real time Data Base. Having a real- time database is the standout feature of the Firebase framework. Firebase caters to a cloud-hosted databasein which the data is stored as JSON and further synchronized constantly to each associated client. Having a real-time database instance that updates thecurrent data is essential for modern applications.

XML: XML stands for *eXtensible Mark-up Language*, which is away of describing data using a text-baseddocument. Because XML is extensible and very flexible, it's used for many different things, including defining the UI layout of Android apps. Other resources like strings for your app arealso defined in an XML file called strings.xml. You describe the view hierarchy of UI elements on the screen. For example, a Constraint Layout can contain Buttons, Text Views, Image Views, or other views. Remember, Constraint Layout is a subclass of View Group. It allows you to position or size child views in a flexible manner.

We can see there are three sections at top right corner

- Code
- Split
- Design

Code option allows us to view the entire code the working slide. Split is useful when we want to checkboth the code and design side by side. Design is usedto view the design of the screen generated and allows us to make changes According to that it will modify the code.

6. SYSTEM ARCHITECTURE

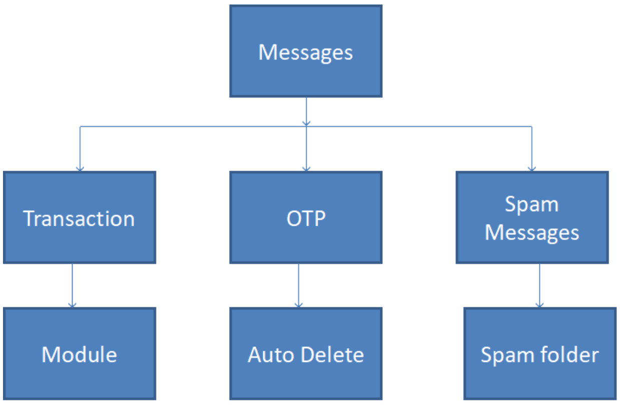


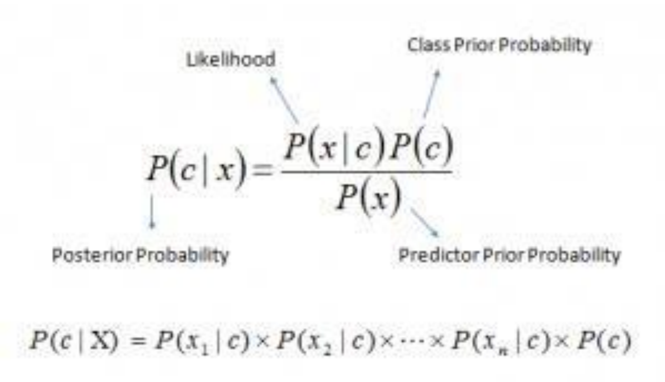
FIGURE 1.

Modules: The system is an App-based approach. We are goingto use Android App Studio which is a platform to make Android Apps.
Android App Studio: Android Studio provides a unified environment whereyou can build apps for Android phones, tablets, ndroid Wear, Android TV, and Android Auto. Structured code modules allow you to divide yourproject into units of functionality that you can independently build, test, and debug. It provides Gradle-based build support. Android- specific refactoring and quick fixes. Lint tools to catchperformance, usability, version compatibility and otherproblems. It contains Templates to create Android designs and components. A rich layout editor that allows users to drag-and-drop components even has Option to preview layouts on multiple screen configurations. It has Built-in support for Google Cloud Platform, enabling integration with Firebase Cloud Messaging and Google App Engine. It even contains a Virtual Device (Emulator) to run and debugapps in the Android studio.
Spam Filtering Process: A manually classified spam and ham messages are input or training set for a spam filtering algorithm. Thealgorithm consists of the following steps Pre-processing: Removing irrelevant contents like stop words are thepart of data preprocessing.
Tokenization: Segmenting the message according to words, characters or symbols called tokens. There are different tokenization approaches such as word tokenization, sentence tokenization, word or character Ngrams and orthogonal sparse bigrams.

Representation: Conversion to attribute value pairs. Selection: Selecting important attribute values which have impacton classification rather than choosing all pairs of attribute value. Using the conditional probability, we can calculate the probability of an event using its prior knowledge.

Training: Train the algorithm with the selected attribute values.Testing: Test the newly arrived data with the trainingmodel.

SMS Spam/Ham classifier using Naive Bayesalgorithm: Using the conditional probability, we can calculate the probability of an event using its prior knowledge



$$P(c\mid x)=\frac{P(x\mid c)P(c)}{P(x)}$$

$$P(c\mid X)=P(x_1\mid c)\times P(x_2\mid c)\times\cdots\times P(x_n\mid c)\times P(c)$$

OTP Detection: Privacy concerns have always been an issue for Android users. Before Android 6 Marshmallow devices, accessing almost anything was possible fromuser's devices which makes users privacy violated andvulnerable. But since Android released request application permission before actually using it made itsecure in some manners. Two of the major dangerous level permissions i.e., SMS and Location permissions are most of the privacy concerning permissions. And now it's almost impossible for new and old apps having these permissions to be published without having a verystrong use-case. SMS / OTP detection requires SMS permissions from user. And its a common use case for apps to auto-detectOTP while logging in through mobile verification. But since READ_SMS and RCEIVE_SMS are not so mucheasier to get published on the play store, Google launched SMS Verification APIs which does the task in-place. Transaction Detection Transactional Monitoring in today's world is necessary to implement variable plans and tiers of services to our customer base. With intelligent systems being put into place at every junction of the transactional process frompayment till the evaluation of end numbers of purchases, we sought to find an intelligent source of digital data that can drive insight generation like no other in the market. The transactional SMS's from a whole lot of messagesare filtered out. Virtual passbook is created by applying ML algorithmsto the messages. SMS transaction extractor solution applies its intelligence to categorize the messages into various expense types across products & services, purchase patterns, and credit & insurance risks. Duplications are removed and filtered out. If there are any incomplete values in the data, thenthey are filled.

7. RESULT

This project is widely use full in any organizations, colleges, banking, companies,E-Commerce, Market News, Government & Public Utilities, Logistics, Media& Entertainment, Travel & Tourism Industry etc. Alert your customer/user about the new updates of organization/colleges. In Logistics it use to send the shipping updates, invoices, bills, tracking detail web URLs and much more via an SMS. Media & Entertainment it use to invite the audience to an FM/TVshow or ask the audience to vote for their favorite contestants in your reality show. and it also used in Travel & Tourism Industry Become a travel buddy of your customer by sending all the itineraries and travel routes via an SMS to make their journey more hassle-free.

REFERENCES

[1]. S. Adams et al., "Privacy-preserving trainingof tree ensembles over continuous data," Proc. Privacy Enhancing Technol., no. 2, 2022.

[2]. A. Agarwal et al., "Protecting privacy of users inbrain-computer interface applications," IEEE Trans. Neural Syst. Rehabil. Eng., vol. 27, no. 8,pp. 1546–1555, Aug. 2019.

[3]. N. Agrawal, A. S. Shamsabadi, M. J. Kusner, and A. Gascón, "QUO- TIENT: Two-party secure

[4]. neural network training and prediction," in Proc.26th ACM SIGSAC Conf. Comput. Commun. Secur., L. Cavallaro,

[5]. K. Yadav, S. K. Saha, P. Kumaraguru, and R.Kumra,"Take control of your smses:

[6]. Designing an usable spam sms filtering system,"in 2012 IEEE 13th InternationalConference on Mobile Data Management. IEEE, 2012, pp. 352–355.

[7]. J. Kinder, X. Wang, and J. Katz, Eds. New York,NY, USA: ACM Press, Nov. 2019, pp.

[8]. K. M. M. Aung, "PrivFT: Private and fast text classification with homomorphic encryption," IEEE Access, vol. 8, pp. 226544–226556, 2020.

[9]. S. J. Warade, P. A. Tijare, and S. N. Sawalkar,"An approach for sms spam detection."

[10].A. Narayan and P. Saxena, "The curse of 140 characters: evaluating the efficacy of sms spam detection on android," in Proceedings of the ThirdACM workshop on Security and privacy in smartphones & mobile devices. ACM, 2013, pp. 33–42.

[11].A. S. Onashoga, O. O. Abayomi-Alli, A. S. Sodiya, and D. A. Ojo, "An adaptive and collaborative server side sms spam filtering scheme using artificial immune system," Information Security Journal: A Global Perspective, vol. 24, no. 4-6, pp. 133–145, 2015

[12].3.A. A. Badawi, L. Hoang, C. F. Mun, K. Laine, L. Leung, "Unwillingness-to-communicate and college

student's motives in SMS mobile messaging," Telematics and Informatics, vol. 24,pp. 115-129, 2007.

[13]. Almeida, Tiago, José María Gómez Hidalgo, andTiago Pasqualini Silva. "Towards sms spam filtering: Results under a new dataset." (2013): 1-18.

[14]. Mujtaba, G., and M. Yasin. "SMS spam detectionusing simple message content features." J. Basic Appl. Sci. Res 4 (2014): 275-279

[15]. Q. Sun, H. Qiao, and Z. Luo, "The feature updating algorithm for short message content filtering," Information Technology Journal, vol. 7,no. 5, pp. 790– 795, 2008.

[16]. I. Ahmed, D. Guan, and T. C. Chung, "Sms classification based on naïve bayes classifier andapriori algorithm frequent itemset," InternationalJournal of machine Learning and computing, vol.4, no. 2, p. 183, 2014.

[17]. T. M. Mahmoud and A. M. Mahfouz, "Sms spamfiltering technique based on artificial immune system," IJCSI International Journal of ComputerScience Issues, vol. 9, no. 1, pp. 589–597, 2012.

[18]. K. Yadav, P. Kumaraguru, A. Goyal, A. Gupta, and V. Naik, "Smsassassin: crowdsourcing driven mobile-based system for sms spam filtering," in Proceedings of the 12th Workshop on Mobile Computing Systems and Applications. ACM, 2011,pp. 1–6.

[19]. T. A. Almeida, J. M. G. Hidalgo, and A. Yamakami, "Contributions to the study of sms spam filtering: new collection and results," in Proceedings of the 11th ACM symposium on Document engineering. ACM, 2011, pp. 259–262.

[20]. M. Poorshahsavari and O. Pourgalehdari, "Enhancing the rate of accuracy and precision inspam filtering in farsi sms."

[21]. Hidalgo JMG, Bringas GC, Sánz EP, García FC (2006) Content based SMS spam filtering. In: ACMsymposium on document engineering, pp 107–114. ACM. https://doi.org/10.1145/116 6160.1166191

[22]. (2015). Wechat-free messaging& calling app[Online]. Available: http://www.wechat.com/

[23]. (2015). Whatsapp web [Online]. Available:http://web.whatsapp. com/

[24]. P. Haffner, S. Sen, O. Spatscheck, and D. Wang, "Acas: Automated construction of application signatures," in Proc. ACM SIGCOMM WorkshopMining Netw. Data, 2005, pp. 197–202.

[25]. T. Karagiannis, A. Broido, M. Faloutsos et al., "Transport layer identification of p2p traffic," in Proc. 4th ACM SIGCOMM Conf. Internet Meas.,2004, pp. 121–134.

[26]. S. Sen, O. Spatscheck, and D. Wang, "Accurate,scalable in- network identification of p2p trafficusing application signatures," in nProc. 13th Int.Conf. World Wide Webn, 2004, pp. 512–521.

[27]. K. P. Dyer, S. E. Coull, T. Ristenpart, and T. Shrimpton, "Peek- a-boo, i still see you: Why efficient traffic analysis counter-measures fail," inProc. IEEE Symp. Security Privacy, 2012, pp. 332–346.

[28]. T. Sto€ber, M. Frank, J. Schmitt, and I.Martinovic, "Who do you sync you are?: Smartphone fingerprinting via application behav- iour," in Proc. 6th ACM Conf. Security Privacy Wireless Mobile Netw., 2013, pp.7–12.

[29]. M. Conti, L. V. Mancini, R. Spolaor, and . V. Verde, "Can't you hear me knocking: Identification of user actions on android apps via traffic analysis," in Proc. Data Appl. Security Pri-vacy, 2015, pp. 297–304.