

# Smart Spam Comment Detection Using Machine Learning

Nauman Zari<sup>1</sup>, Sanket Potghan<sup>2</sup>, Sweety Kale<sup>3</sup>, Prof. S. D. Babar<sup>4</sup>

Students, Department of Information Technology<sup>1,2,3</sup>

Professor, Department of Computer Engineering<sup>4</sup>

Sinhgad Institute of Technology, Lonavala, Maharashtra, India

**Abstract:** The profitability promoted by Google in its well-known video distribution platform YouTube has attracted an increasing number of users. However, such success has also attracted large number of malicious users, which aim to self-promote their videos or circulate viruses and malware. As we know that YouTube offers limited tools for comment moderation, so spam increases very rapidly and that's why comment section of the owners is disabled. It is very difficult to established classification methods for automatic spam filtering since the messages are very short and often widespread with slangs, symbols, and abbreviations. In this paper, we have evaluated several top-performance classification techniques for detecting and analysing spam comments. The statistical analysis of results indicates that, with 99.9% of confidence level, decision trees, logistic regression, Bernoulli Naive Bayes, random forests, linear and Gaussian SVMs are statistically equivalent in maximum rate. Therefore, it is very important to find a way to detect these comments on videos and report them before they are viewed by innocent users.

**Keywords:** Spam Comment Detection, Machine Learning, Naïve Bayes, Linear Regression, SVM

## I. INTRODUCTION

In the previous years, informal online communities like face book and youtube have become progressively common platform in an individual person's day to day life. People use social media as a virtual community platform to stay in touch with friends and family and to also share thoughts and ideas in blogs. Due to this developing pattern, these platforms pull in an enormous number of clients and are easy targets for spammers. Youtube has become the most well-known informal community among youngsters. For example, many makeup tutorials have been started by bloggers who are referred to as "beauty guru" or "beauty influencers" in which majority of the audiences are teenage girls. These days, 200 million clients produce 400 million new youtube content (videos) every day. This extensive environment provided by youtube also creates an opportunity for spammers to create irrelevant content directed to users. These irrelevant or unsolicited messages are aimed to attack users by luring them into clicking links to view malicious sites containing malware, phishing and scams. One of the most highlighted features of youtube is the comments section below every video posted by a user. This feature allows users to share opinions and ideas. In this project, the prediction of the spam comments present in the comments section of youtube videos using the concept called machine learning, it is also known as subset of artificial intelligence, is done. Supervised learning approach depends on a very large number of labelled datasets.

- Popularization boosted number of internet users on YouTube and other platforms
- Facing problems to manage undesired comments, malicious links etc.
- Social spam is increasing by 35%

In 2020 breadnbeyond blog reported efforts to deal with problems

## II. PROPOSED WORK

### 2.1 Naïve Bayes

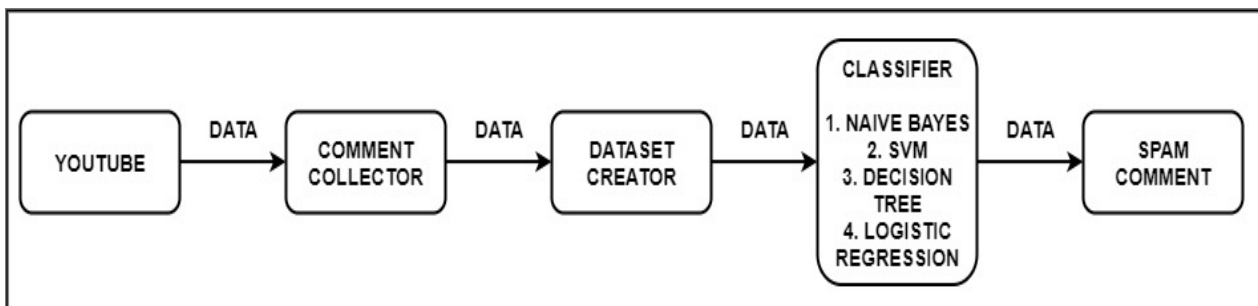
In the machine learning algorithm, Naive Bayes is the classification algorithm. Its primarily used for solving text classification problem, which having high dimensional training data sets. It is a probabilistic classifier. It calculates the conditional probability that is the probability of an event based on previous knowledge available. This algorithm is known for its simplicity but also for effectiveness.

## 2.2 SVM

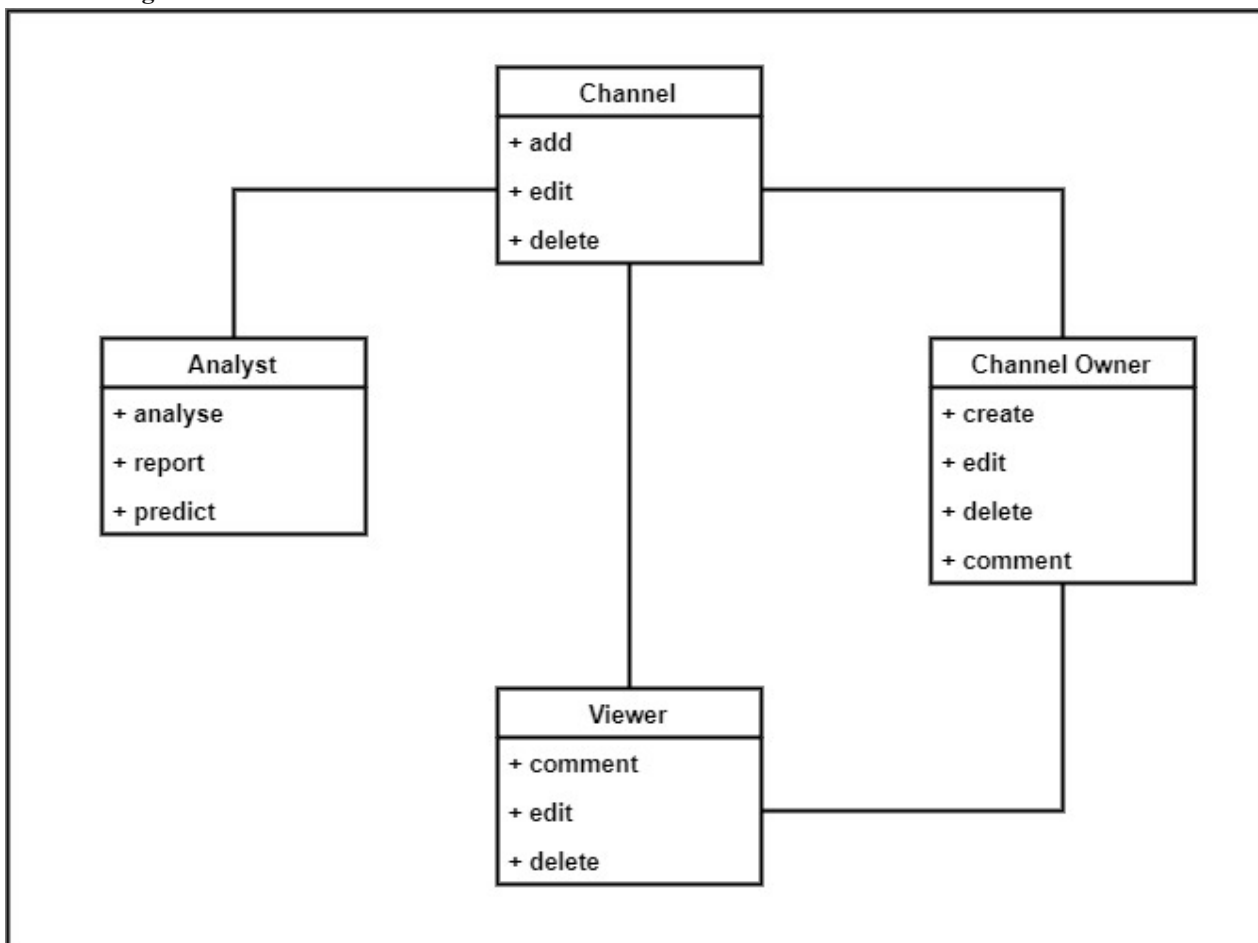
Support Vector Machine used for the regression but primarily used for the classification. SVM Supervised learning algorithm that looks of data & sorts it into one of the two categories. It is a discriminative classifier that is formally designed by a separate hyper plane. SVM represents the examples as points and mapped in a space so that examples are divided by a clear gap as wide as possible. This is helpful in text and hypertext categorization. SVM is more effective in high dimensional space.

## III. DATA FLOW DIAGRAM

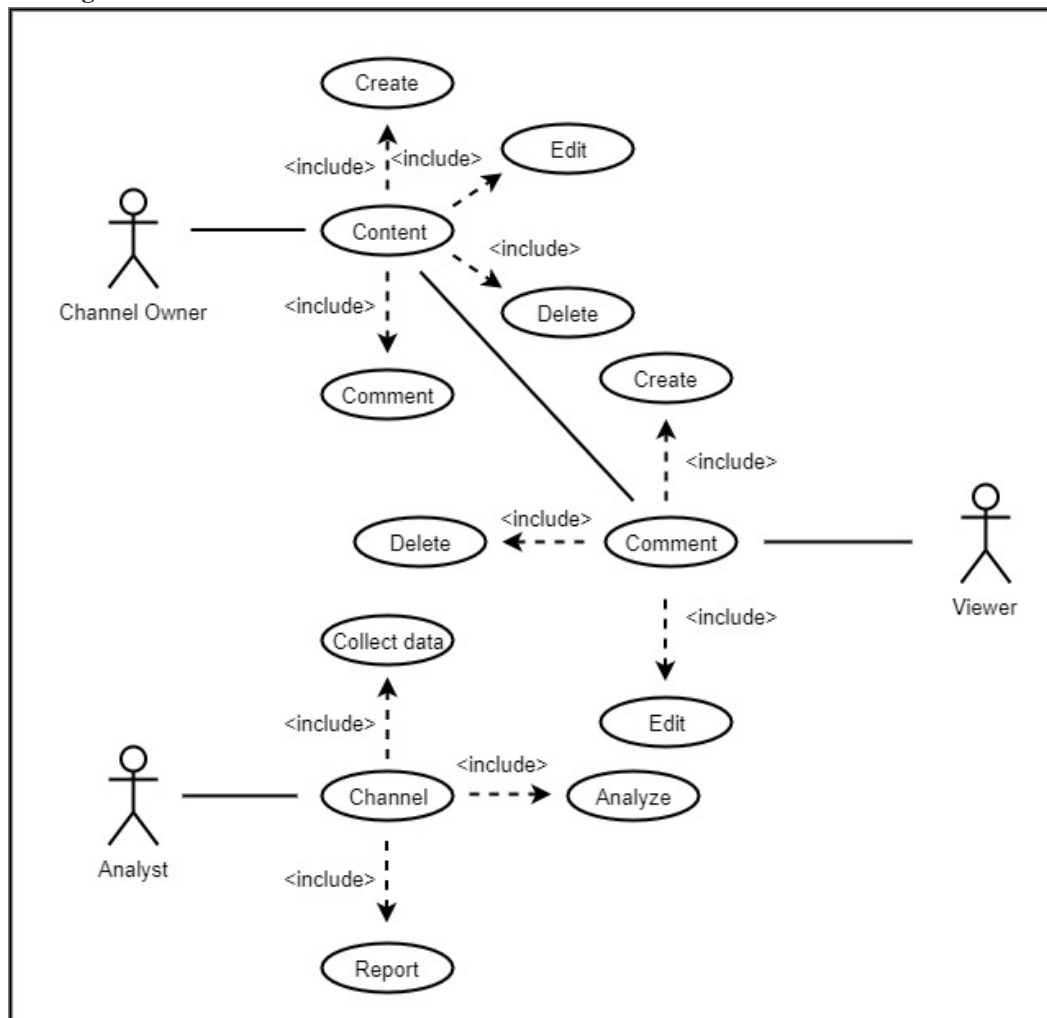
### 3.1 Flow Chart



### 3.2 Class Diagram



### 3.3 Use Case Diagram



## IV. HARDWARE AND SOFTWARE REQUIREMENTS

### 4.1 Software Requirements

- IDE: Spyder
- Coding Language: PythonVersion3.8
- Operating System: Windows10(64Bit)

### 4.2 Hardware Requirements

- RAM: 8GB
- Hard Disk: 500GB
- Processor: Intel i5Processor
- Speed: 2.5GHz

## V. APPLICATIONS

- Youtube Comments
- Tweets posted on Twitter
- Instagram

## **VI. CONCLUSION**

To Conclude, Social media networks have become popular and this creates the opportunity for the spammers to publish unwanted comments.

Previously, some machine learning algorithms were used for this detection. In the proposed system we also use the advanced machine learning algorithms with advanced features also compares the efficiency of various algorithms by applying them. We construct features based on the features obtained from the user profile and the content that they shared. Based on the experiments conducted, it can be expected that existing classifiers widely used in the data mining community can utilize these functions to detect spammers.

## **VII. ACKNOWLEDGMENT**

The authors would like to thank professor of the Department of Information Technology in Sinhgad institute of Technology, Lonavala Prof. S.D. Babar for their time and efforts she provided throughout the project and her advice and suggestions were really helpful to us.

## **REFERENCES**

- [1]. N. M. Samsudin, C. F. B. MohdFoozy, N. Alias, P. Shamala, N. F. Othaman and W. I. S. Wan Din, "Youtube spam detection framework using Naïve Bayes and logistic regression", Indonesian J. Electr. Eng. Comput. Sci., vol. 14, no. 3, pp. 1508, Jun. 2019.
- [2]. K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan and S. A. Razak, "Malicious accounts: Dark of the social networks", Elsevier, 2017, pp. 41-67.
- [3]. R. K. Das, S. S. Dash, K. Das and M. Panda, "Detection of spam in Youtube comments using different classifiers", Advanced Computing and Intelligent Engineering, pp. 201-214, 2020.
- [4]. S. Garg Makkar, N. Kumar, M. S. Hossain, A. Ghoneim and M. Alrashoud, "An Efficient Spam Detection Technique Using Machine Learning", IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 903-912, Feb. 2021.
- [5]. C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou and G. Min, "Statistical Features- Based Real- Time Detection of Drifted Twitter Spam", IEEE Transactions, April 2017, pp. 914-925.
- [6]. M. Verma, Divya, S. Sofat, "Techniques to Detect Spammers in Twitter – A Survey", International Journal of Computer Applications, January 2014, Vol. 85, No. 10, pp. 27-32.
- [7]. A. Gupta and R. Kaushal, "Improving Spam Detection in Online Social Networks", IEEE, 2015

## **BIOGRAPHY**

- Nauman Zari-An Undergraduate Scholar pursuing Bachelors of Engineering in Computer from Sinhgad Institute of Technology. He is working under the guidance of Prof. S.D. Babar.
- Sanket Potghan - An Undergraduate Scholar pursuing Bachelors of Engineering in Computer from Sinhgad Institute of Technology. He is working under the guidance of Prof. S.D. Babar.
- Sweety Kale- An Undergraduate Scholar pursuing Bachelors of Engineering in Computer from Sinhgad Institute of Technology. He is working under the guidance of Prof. S.D. Babar.