

**NAIVE BAYES ALGORITHM BASED E-MAIL
SPAMMING FILTERING SYSTEM**

LEE KIM HAO

**THESIS SUBMITTED IN PARTIAL FULFILLMENT
FOR THE DEGREE OF BACHELOR OF COMPUTER
SCIENCE WITH HONOURS (NETWORK
ENGINEERING)**

**FACULTY OF COMPUTING AND INFORMATICS
UNIVERSITI MALAYSIA SABAH 2022**

i



UMS
UNIVERSITI MALAYSIA SABAH

NAME : LEE KIM HAO
MATRIC NUMBER : BI18110247
TITLE : PROJECT TITLE
DEGREE : BACHELOR OF COMPUTER SCIENCE WITH HONOURS
NETWORK ENGINEERING
VIVA'S DATE : 28 JANUARY 2022

CERTIFIED BY;

1. SUPERVISOR

DR LEAU YU BENG


Signature
DR LEAU YU BENG
Faculty of Computer Science
Universiti Malaysia Sabah
Tel : +6088 620000 Ext 3220
lybeng@fcs.ums.edu.my



UMS
UNIVERSITI MALAYSIA SABAH

DECLARATION

I hereby declare that the material in this thesis is my own except for quotations, equations,

summaries and references, which have been duly acknowledged.

28 JANUARY 2022

A rectangular box containing a handwritten signature in black ink. The signature appears to be 'Hao' with a stylized flourish.

LEE KIM HAO

BI18110247



UMS
UNIVERSITI MALAYSIA SABAH

ACKNOWLEDGEMENT

I would like to credit to all the tutors and lecturer that providing the guidance which help me in this project. Without forget my course mates that lead me to succeed the whole journey as I am considered as a weak learner in this course.

Thanks to my supervisor, Dr. Leau Yu Beng that tolerates and enlighten me up with many advisories on my inconvenience from public aspect of this project to my personal issues during the whole process of this project.



UMS
UNIVERSITI MALAYSIA SABAH

ABSTRACT

E-mail spam although not against the law of federation, this issue still annoying every user and clogging up the space of their mailbox. With the inspiration of previous happen spam issue in Universiti Malaysia Sabah official account and increasingly spam issue causing nuisance toward e-mail users. In this final year project, author will be looking for developing a spam filtering system that will scan and filter out spam message that might be sent from any other users with checking the keyword that record toward the system. According to the research found, there are various of spam filtering technology such as Content Based Filters, Bayesian Based Filters, Whitelist or Blacklist Filters, and Community Filters. Certain problem found by author on the common spamming content such as phishing scam content, irrelevant or fake advertising content and harassment content. The objective of this project is designing a spam filtering system using content-based Bayesian technique to classify and remove spam message to junk folder. This project final product is target toward user frequently using e-mail and the module containing login/logout authentication, home page and mailbox. Author conducted Agile model Scrum for One method toward this project in order to accomplish the project. A final version of product had been implemented in different directory without integrating due to limited skill possessed though putting away the integrating issue the project considered partially complete as it had fulfilled some of the objectives listed.



UMS
UNIVERSITI MALAYSIA SABAH

ABSTRAK

SISTEM PENAPISIAN SPAMMING E-MEL BERASASKAN ALGORITMA NAIVE BAYES

Walaupun spam dalam emel tidak menyentuh undang-undang persekutuan, masalah ini masih menyinggung dan mengganggu pengguna-pengguna dengan memenuhkan emel yang tidak berkaitan dalam peti mel. Dengan kes yang berlaku pada sem lepas dalam Universiti Malaysia Sabah, bahawa pelajar-pelajar telah diganggu oleh emel yang tidak rasmi dan tidak diingini untuk terima. Dalam projek tahun akhir ini, pengarang akan mamajukan satu sistem yang menapiskeluarkan spam dalam emel selepas imbas emel menggunakan kata kunci yang terdapat dalam sistem. Mengikut penyelidikan yang dijalani, terdapat banyak teknologi untuk menapisikan emel seperti Content Based Filters, Bayesian Based Filters, Whitelist or Blacklist Filters, and Community Filters. Isu-isu utama dalam kandungan spam telah dijumpai iaitu penipuan 'phishing', iklan yang palsu dan tidak berkaitan, dan perkataan gangguan. Objektif dlam projek ini ialah untuk mereka bentuk satu sistem yang menapiskeluarkan spam dalam emel menggunakan teknik 'content-based Bayesian' untuk mengelaskan dan buangkan spam ke fail sampah. Produk projek ini menumpukan pengguna yang kerap mengguna e-mel dan dalam modul produk terdapat log masuk/keluar, laman utama, dan peti mel. Pengarang menggunakan cara model 'Agile Scrum for One' untuk menjalankan proses projek ini. Produk akhir telah berjaya dikeluarkan dengan direktori yang berlainan disebabkan kekurangan upaya pengarang. Projek mengirakan disiap separuh dengan memenuhi sesetengah objektif yang dicatatkan.



UMS
UNIVERSITI MALAYSIA SABAH

TABLE OF CONTENTS

TITLE.....	i
DECLARATION.....	iii
ACKNOWLEDGEMENT.....	iv
ABSTRACT.....	v
ABSTRAK.....	vi
TABLE OF CONTENTS.....	vii
LIST OF TABLES.....	xii
LIST OF FIGURES.....	xiii

CHAPTER 1 INTRODUCTION

1.1 Introduction.....	1
1.2 Problem background.....	2
1.3 Problem Statements	3
1.4 Project Goal.....	6
1.5 Objectives	6
1.6 Project Scope.....	6
1.7 Project Timeline	8
1.8 Organization of Report.....	10
1.9 Summary.....	10

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction.....	12
2.2 Concept of Spam Filtering	12
2.3 Spam Filtering Categories	14



2.3.1	Gateway Spam Filter	14
2.3.2	Hosted Spam Filter	14
2.3.3	Desktop Spam Filter.....	15
2.4	Spam Filtering Technique.....	15
2.4.1	Content Based Filters	16
2.4.2	Bayesian Based Filters.....	16
2.4.3	Whitelist or Blacklist Filters	16
2.4.4	Challenge/Response Filters.....	17
2.4.5	Previous Likeness Based Spam Filtering	17
2.4.6	Case Base Spam Filtering	18
2.4.7	Heuristic or Rule Based Spam Filtering.....	18
2.4.8	Community Filters.....	18
2.5	Concept of Machine Learning	19
2.6	Spam Filtering Method/Algorithm.....	20
2.6.1	Clustering technique	20
2.6.2	Naïve Bayes classifier	23
2.6.3	Neural networks	25
2.6.4	Firefly algorithm	28
2.6.5	Rough set classifiers	29
2.6.6	Support vector machine classifiers.....	31
2.6.7	Decision tree	33
2.6.8	NBTree classifier	33
2.6.9	C4.5/J48 decision tree algorithm	34
2.6.10	Logistic model tree induction (LMT).....	34



2.6.11	Ensemble classifiers	36
2.6.12	Random forests (RF).....	39
2.6.13	Deep learning algorithms.....	40
2.7	Related work	44
2.8	Study on Related Project.....	46
2.9	Review on Existing Related System.....	48
2.9.1	Gmail.....	48
2.9.2	Yahoo.....	50
2.9.3	Outlook.....	51
2.10	Comparison between the Algorithm Majorly Used.....	52
2.11	Summary.....	53

CHAPTER 3 METHODOLOGY

3.1	Introduction.....	55
3.2	System Development Life Cycle Model	55
3.3	Methodology used in System Development.....	57
3.4	Software/Hardware Requirement.....	60
3.5	Summary.....	61

CHAPTER 4 SYSTEM ANALYSIS AND DESIGN

4.1	Introduction.....	62
4.2	System Analysis	62
4.2.1	Questionnaire Analyse.....	63
4.2.1.1	Spam e-mail experience review	63
4.2.1.2	Application scope review	70
4.2.1.3	Application User Interface Review.....	73



4.3	System Design	75
4.3.1	Entity Relationship Diagram	76
4.3.2	Data Dictionary.....	77
4.3.3	Data Flow Diagram	79
4.4	User Interface Design	85
4.5	Summary.....	87
CHAPTER 5 IMPLEMENTATION		
5.1	Introduction.....	89
5.2	User Interface Implementation	89
5.3	System Implementation	98
5.4	Summary.....	99
CHAPTER 6 TESTING		
6.1	Introduction.....	101
6.2	Unit Testing	101
6.3	Algorithm Testing	104
6.4	Integrating Testing.....	108
6.5	Summary.....	109
CHAPTER 7 CONCLUSION		
7.1	Introduction.....	110
7.2	Project Summary.....	110
7.3	Future Work	111
7.4	Summary.....	111
REFERENCE.....		111
APPENDIX.....		114





UMS
UNIVERSITI MALAYSIA SABAH

LIST OF TABLES

Table 1.1 User Role Modules of The Projects.....	7
Table 1.2 Admin Role Modules of The Projects.....	7
Table 1.3: Gantt Chart of The Project Timeline Semester 2 - 2020/2021(FYP 1).....	8
Table 1.4: Gantt Chart of The Project Timeline Semester 1 - 2021/2022(FYP 2).....	9
Table 2.1: Comparison Result Between Algorithm.....	52
Table 4.1: User Data Dictionary.....	77
Table 4.2: Adminlogin Data Dictionary.....	77
Table 4.3: Userlogin Data Dictionary.....	78
Table 4.4: Usermailbox Data Dictionary.....	78
Table 4.5: Junk Data Dictionary.....	78
Table 6.1 Register/Login/Logout Module (Admin And User Site) Testing List.....	101
Table 6.2 Fetching/Filtering/Display E-Mail Message Module Testing List.....	103



LIST OF FIGURES

Figure 2.1: Google Spam Filter Graph.....	50
Figure 2.2: Graph of Comparison Result Between Algorithm.....	53
Figure 3.1: Agile Scrum for One Model cycle illustration.....	57
Figure 4.1: Statistics pie chart of "How often did you get a spam e-mail?".....	64
Figure 4.2: Statistics horizontal bar chart of "What type of spam you often received?"...65	
Figure 4.3: Statistics pie chart of "Did you think the spam e-mail annoyed you?".....	66
Figure 4.4: Statistics pie chart of "Did the spam e-mail bringing harm on you?".....	67
Figure 4.5: Statistics pie chart of "Did you ever missed important e-mail accidentally?...68	
Figure 4.6: Statistics pie chart of "How you react after received spam?".....	69
Figure 4.7: Statistics pie chart of "Which e-mail you are mainly using?".....	70
Figure 4.8: Statistics pie chart of "Do you think spam filtering service is necessary for you?	71
Figure 4.9: Statistics pie chart of "Do you concern about confidentiality of your e-mail content?"	71
Figure 4.10: Statistics pie chart of "If application require to grant access on your mailbox, will you accept it?"	72
Figure 4.11: Statistics pie chart of "Which filtering process do you prefer?".....	73
Figure 4.12: Statistics pie chart of "Which type of logo do you prefer?".....	74
Figure 4.13: Statistics pie chart of "Which type of background do you prefer?".....	75
Figure 4.14: ERD of Spam Filtering System.....	76
Figure 4.15: Context Diagram of Spam Filtering System.....	79



Figure 4.16: Level 0 Data Flow Diagram of Spam Filtering System.....	81
Figure 4.17: Level 1 Data Flow Diagram of Login.....	82
Figure 4.18 Level 1 Data Flow Diagram of Gmail Authorization.....	83
Figure 4.19 Level 1 Data Flow Diagram of Mailbox Display.....	84
Figure 4.20 Level 1 Data Flow Diagram of User Management.....	85
Figure 4.21: Login module.....	86
Figure 4.22: Homepage module.....	87
Figure 5.1: Admin Login module.....	90
Figure 5.2: Admin Panel module.....	90
Figure 5.3: User Lists module	91
Figure 5.4: Add User module.....	91
Figure 5.5: Change User module.....	92
Figure 5.6: Change User Password module.....	92
Figure 5.7: Change Password module.....	93
Figure 5.8: Visitor module.....	93
Figure 5.9: Sign In via Google module.....	94
Figure 5.10: Register module	94
Figure 5.11: Login module.....	95
Figure 5.12: Home Page module.....	95
Figure 5.13: Profile module.....	96
Figure 5.14: Intro module.....	96
Figure 5.15: Mailbox module.....	98



Figure 5.16 Implemented URI from the Google API credentials for fetching e-mail messages..... 99

Figure 5.17 Implemented Naïve Bayes classifier with delete function.....99

Figure 6.1 Naïve Bayes filtering algorithm source code(i)105

Figure 6.2 Naïve Bayes filtering algorithm source code(ii)106

Figure 6.3 Spam dataset.....107

Figure 6.4 System result.....108

Figure 6.5 Mailbox showing the result of classification of Ham and Spam.....109



CHAPTER 1

INTRODUCTION

1.1 Introduction

Spam, or unnecessary commercial mass communications, has been a major concern on the internet in recent years. The spammer is the one who sends out the spam messages. This person collects email addresses from a variety of sources, including blogs, chat rooms, and viruses. Spam prohibits users from getting the most out of their time, computing space, and network bandwidth. The massive amount of spam mails streaming through computer networks has a negative impact on email servers' memory capacity, communication speed, CPU resources, and usage time. Spam email is becoming a bigger problem last year, accounting for more than 77 percent of all global email traffic. It irritates users who get spam emails that they did not order. Many consumers have suffered untold financial losses as a result of internet scams and other malicious activities by spammers who deliver emails posing as from legitimate firms in order to force people to share confidential personal details such as passwords, Bank Verification Numbers (BVN), and credit card numbers.

In this chapter, the author will share the problem found in relevant field which related to email spamming and the project that aimed to undergoing. Author will also share the timeline of project in this topic.



1.2 Problem background

Few years ago, official Universiti Malaysia Sabah (UMS) student email account came out a lot of spam message which some of the users exploiting the bugs occur from the server side and they are using it to make spam message and causing a short nuisance toward other users which under using the official UMS email account.

The problem soon had been recovered by Jabatan Teknologi Maklumat dan Komunikasi (JTMK) from UMS but in consider of the flaws might be occurred in upcoming day since there will have a chance to happen some of the users might take this advantage again to spam other users' email account cause nuisance and mailbox clogged which in advance may occur problem such as phishing scam, malicious act as other users or sending malicious link for hacking, inappropriate advertising attempt and sending sensitive topic causing others to feel uncomfortable. This all action will be an unwanted criminal issue which will bring out to happen involving law execution and crime charging from Polis Diraja Malaysia (PDRM).

Besides from UMS official account spam incident, nowadays peoples met spam problem more frequent as the internet is now a convenient or compulsory part of their life which bring up the opportunity for some people intended to make spam to cause nuisance and harassment toward other for their own benefit. Spam email already became a common problem which the case increases during pandemic season because of everyone or mostly have to work from home with their gadget and some people take this advantage to make the spam. A cold email is an email that's sent without prior permission from or contact with the recipient. (Sujan Patel, 2020) Although spam itself, people usually mentioned the spam as a cold emailing which it just a marketing purpose to promote their product or service if there is no harmful intention found, it still an annoying due to sometime the irrelevant content that fill up the space in mailbox.

Email has been considered as one of the most efficient and convenient ways of communication since the users of the Internet has increased rapidly. E-mail spam, known as junk e-mail, UBE (unsolicited bulk e-mail) or UCE (unsolicited commercial e-mail), is the act of sending unwanted e-mail messages to e-mail users. Spam is becoming a huge problem to most users since it clutters their mailboxes and waste their time to delete all



the spam before reading the legitimate ones. They also cost the user money with dial up connections, waste network bandwidth and disk space and make available harmful and offensive materials.

1.3 Problem Statements

A spam filtering system is important in nowadays especially in this pandemic season the online working and studying became somehow necessity for everyone and emailing the important message became one of the least ways to transmit to their working partner, student, teacher and so on for the idea, working plan etc. A secure email account is one of the most valuable parts of running a successful business. (Global Harvest Network, 2018). This is also considered a component of university development to improve the official mailbox environment from latest version. Also, besides from official mailbox spam, user can also solve their private mailbox if the permission accessed. The problem should be identified by author to be solved with the system.

The following list is the problem that had been target in common unsolicited email junk filtration:

- Phishing scam content

Phishing is a form of social engineering attack, including login credentials and credit card numbers, mostly used to steal user data. This happens when an intruder, posing as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then fooled into clicking a malicious connection, which can lead to malware installation, system freezing as part of a ransomware attack, or confidential information being exposed.

In addition, phishing is also used as a part of a larger attack, such as an advanced persistent threat (APT) case, to gain a foothold in corporate or governmental networks. Employees are compromised in this latter scenario in order to circumvent safety perimeters, spread malware inside a closed environment, or obtain privileged access to protected data.



UMS
UNIVERSITI MALAYSIA SABAH

A company that falls victim to such an attack normally experiences substantial financial losses as well as a loss of market share, prestige, and customer confidence. A phishing attempt may, depending on the scope, escalate into a security incident from which an organization would have a hard time recovering.

The following illustrates a common phishing scam attempt:

- A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.
- The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.

Scammers launch thousands of phishing attacks like these every day and they are often successful. The FBI's Internet Crime Complaint Center reported that people lost \$57 million to phishing schemes in one year.

- Irrelevant or fake advertising content

Email is both an excellent communication tool and also a way that companies can inform you about their latest products and services. However, email is frequently used to deliver unwanted material, which is at best, annoying and at worst, malicious – causing considerable harm to your computer and yourself.

Bunch of criminal start taking advantages of this convenience to make fake advertisement to trick victim from falling into the trading trap and getting scam of their money. They usually fishing for people who intended to buy something they advertising which does not exist.

The vast majority of email sent every day is unsolicited junk mail. Examples include:

- Advertising, for example online pharmacies, pornography, dating, gambling.
- Get rich quick and work from home schemes.
- Hoax virus warnings.
- Hoax charity appeals.



UMS
UNIVERSITI MALAYSIA SABAH

- Chain emails which encourage you to forward them to multiple contacts (often to bring 'good luck').
- Harassment content

Internet harassment, also referred to as "cyberbullying", is the term used to describe the use of the Internet to bully, harass, threaten, or maliciously embarrass.

- Cyberbullying, especially among teenagers, has become increasingly popular as the digital sphere has grown, and technology has progressed. Cyberbullying victims may experience lower self-esteem, increased suicidal ideation, and a range of adverse emotional responses, including fear, rage, anger, or depression.
- Cyberstalking, meanwhile, is also a form of online bullying or harassment that uses electronic communications to stalk a victim. This may pose a legitimate threat to the victim.

People starting to use the advantages of internet to judge and punish their victim with their own way and email is one of the ways they are using. They will keep sending harassing content toward their victim until they are satisfied. Same as cyberbullying, cyberstalking criminal also taking this advantage to send harassing email to their victim and letting their victim to suffer in fear.

This problem is the most need to be concerned that this might bring suicidal thought toward victim and even they brave enough to support the damage, a traumatic shade will also trap them for their whole life. Victim usually avoid using the template again to prevent from getting harass which made them lost confidence on trusting the upcoming message or email they received, and this affected their normal living routine. In the past decade, there have been multiple cyberbullying cases that ended with the victims taking their own lives.

There are certain related cases happened in Malaysia. A 20-year-old who was found dead at her family home in Bukit Tengah left a heart-breaking note to her loved ones. She allegedly fell victim to cyberbullying after a Tik Tok video of her and a Nepali colleague drew criticism on Facebook and went viral. Datin Paduka Marina Mahathir, prominent blogger, and daughter of the former Prime Minister has had a run in with a cyberstalker. According to a 2008 article in *The Star*, the stalker sent her weird and



nonsensical e-mail messages. When she refused to respond to his e-mail messages, because that would be engaging the cyberstalker, he got hold of her office phone and fax numbers.

1.4 Project Goal

The author goal is to create an interface containing the login and logout function for user connecting their relevant mailbox to the system. Furthermore, author wants the system which to filter the spam from the mailbox help user to clarify, classify, and arrange the mailbox automatically after they authorize their email.

1.5 Objectives

In order to solve the problem and achieve the set goal, the following objectives are needed to fulfill.

To design a web-based system for users which can allow them to clear spam email.

To develop an e-mail spam filtering system using content-based Bayesian technique.

To test the performance of prototype related to proposed project through configuring the final prototype.

1.6 Project Scope

The proposed spam filtering system basically targeting users who frequently using e-mail as their part of work and study. A registration using their e-mail will be compulsory to take action on the functionality of the system. As the registration done, the system will require user for access permission to make change on their e-mailing system. User can set keyword in order for the system to block the e-mail containing the keyword. System will also learn to predict the upcoming spam by using heuristics machine learning through Bayesian approach using the keyword to prevent spammer modify message using unique character.



UMS
UNIVERSITI MALAYSIA SABAH

The following table shows the module with description to explain how the system will work.

Table 1.1 User Role Modules of The Projects

Module	Description
Sign up and Login authentication	Users sign up and log in with the username and password created/ sign in via Google (recommended)
Home page	Shows users brief introduction and explanation for users
Mail Box	Present users' mailbox

Table 1.2 Admin Role Modules of The Projects

Module	Description
User Authentication/ Authorization	Admins can add/modify/delete user
Notification	Notify users action log



1.7 Project Timeline

Table 1.3: Gantt Chart of the Project Timeline Semester 2 - 2020/2021(FYP 1)

Milestone		Semester 2 - 2020/2021(FYP 1)													
		W	W	W	W	W	W	W	W	W	W	W	W	W	W
		E	E	E	E	E	E	E	E	E	E	E	E	E	E
		E	E	E	E	E	E	E	E	E	E	E	E	E	E
		K	K	K	K	K	K	K	K	K	K	K	K	K	K
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Project Activities	Stating the problem														
	Identify the objective of project														
	Conduct preliminary study														
	Gather project requirements														
	Establish milestone														



Table 1.4: Gantt Chart of the Project Timeline Semester 1 - 2021/2022(FYP 2)

Milestone		Semester 1 - 2021/2022(FYP 2)													
		W	W	W	W	W	W	W	W	W	W	W	W	W	W
		E	E	E	E	E	E	E	E	E	E	E	E	E	E
		E	E	E	E	E	E	E	E	E	E	E	E	E	E
		K	K	K	K	K	K	K	K	K	K	K	K	K	K
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Project Activities	Construct the system														
	Design user interface														
	Implementing prototype														
	Release alpha beta version for user testing														
	Release final product														

