5-2022

Evaluation of Email Spam Detection Techniques

Seshi Reddy Guda

Evaluation of Email Spam Detection Techniques

By

Seshi Reddy Guda

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Information Assurance

May, 2022

Starred Paper Committee:
Abdullah Abu Hussein, Chairperson
Lynn Collen
Sneh Kalia

Abstract

Email has become a vital form of communication among individuals and organizations in today’s world. However, simultaneously it became a threat to many users in the form of spam emails which are also referred to as junk/unsolicited emails. Most of the spam emails received by the users are in the form of commercial advertising, which usually carry computer viruses without any notifications. Today, 95% of the email messages across the world are believed to be spam; therefore, it is essential to develop spam detection techniques. There are different techniques to detect and filter spam emails, but recently a handful of developed techniques have been implemented to successfully minimize the threats. This paper describes how the current spam email detection approaches are determining and evaluating the problems. There are different types of techniques developed based on Reputation, Origin, Words, Multimedia, Textual, Community, Rules, Hybrid, Machine learning, Fingerprint, Social networks, Protocols, Traffic analysis, OCR techniques, Low-level features, and many other techniques. All these filtering techniques are developed to detect and evaluate spam emails. Along with the classification of the email messages into spam or ham, this paper also demonstrates the effectiveness and accuracy of the spam detection techniques.

Acknowledgments

I am thankful and would like to convey my gratitude to every individual who has helped me with their input in the accomplishment of my Starred Paper. Primarily, I am thankful to Professor Abdullah Abu Hussein, who is the chairperson and advisor of my Starred Paper Committee. He provided valuable guidance wherever required and assisted me throughout the completion of my study. I am also thankful to Dr. Sneh Kalia and Dr. Lynn Collen for their support and guidance in my research study, who are also members of my Starred Paper Committee. I am grateful to Professor Abdullah Abu Hussein, who assisted me with his insightful suggestions and comments throughout my study.

Lastly, I am grateful to the library staff of St. Cloud State University for providing their resources which helped me during my study.

Table of Contents

Page

Chapter

Chapter Page

List of Figures

Figure Page

List of Tables

Table Page

Chapter I: Introduction

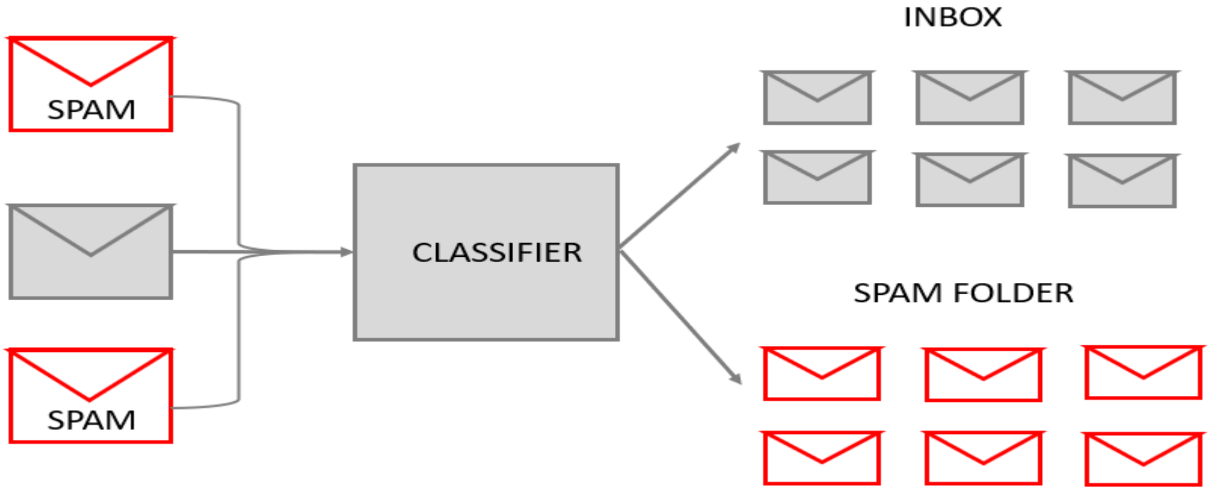
The Internet is an essential source in today's world. Email users have been increasing day by day. The increased use of email has been causing many problems through unsolicited (unwanted) email messages, which are referred to as Spam. Spam emails are being sent to receivers in the form of advertisements, which most of them do not wish to receive and have also been causing severe problems to many industries/organizations, individuals, and Internet Service Providers (ISP). Spam is an improper way of the electronic messaging system which sends messages in bulk to several recipients (Vijayasekaran & Rosi, 2018).

With the availability of internet access, spam can occur anywhere in the world. So, it has become difficult to trace a spammer and is a tedious task. To minimize these issues, there is a necessity for spam filtering and detection techniques (separating email messages between legitimate and spam). Spam detection can categorize email messages into legitimate and illegitimate (spam) messages using some techniques.

There are different approaches to detect/filter spam emails. Machine learning algorithms are widely used to detect these emails. One of the machine learning algorithms is the Naive Bayesian classifier detection technique, which classifies the spam email messages into spam or ham. The logistic regression approach filters the spam emails using certain types of characteristics, such as the identification of recurring words that are assumed to be predictor variables. Many other machine learning algorithms are being used to detect spam emails, such as Decision trees, Support Vector Machines (SVM), Clustering techniques, Ensemble classifiers, Neural networks, and K-Nearest neighbor (Bhowmick & Hazarika, 2016).

Figure 1

Text classifier for spam detection (Kumar, 2019)



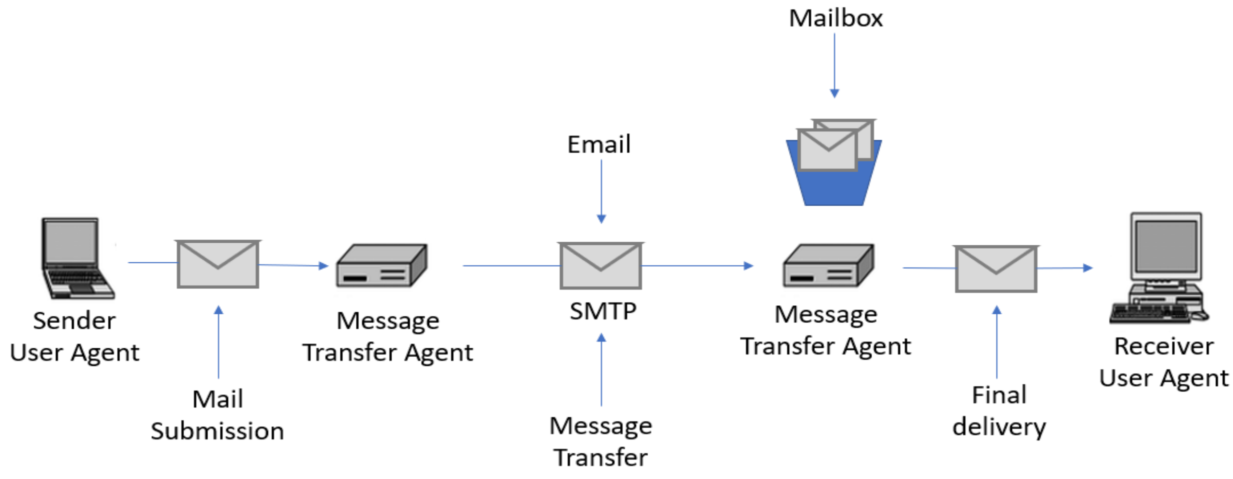
Spam filtering reduces the maximum of unsolicited emails. It carries out the process of rearranging the emails into definite standards. Spam filters aim at filtering or eliminating viruses. Filters block suspicious or unwanted emails, which cause a risk to network security from getting into the system. A server can carry a minimum amount of data and can go through it at a given time. Sometimes while receiving spam email messages, there are chances that the data we require might not be received on time; this can have an impact on many organizations. Spam costs organizations billions by decreasing productivity, according to some research. To prevent all these issues, it is important to continue to develop and maintain spam detection techniques.

The Architecture of an E-mail

The E-mail consists of two components: header and body. TCP/IP header consists of source and destination IP addresses, and then the SMTP envelope stores the email attributes (fields) such as source and destination e-mail addresses. The SMTP header contains the structured attributes such as sender e-mail ID, recipient e-mail ID, Subject, Timestamp, Date stamp, and Routing information, which can be traceable. All the attributes in the header session have a specific name and purpose. Here, Firstly the SMTP envelope sender address is delivered and then followed by the recipient's addresses, and lastly, the original message is delivered. The SMTP envelope addresses are used by the e-mail servers to deliver the e-mail to the recipients. And the recipients can only see the e-mail header and body. The source and destination addresses are stored in an SMTP envelope where the spammers utilize this e-mail feature for their own benefits. The other component of E-mail is its body, also known as an email message, which consists of unstructured information such as text, links, objects, and attachments that can contain malicious data (Saleh & Karim, 2019).

Figure 2

Architecture of an E-mail (Jameel & Mohammed, 2017)



Problem Statement

Spamming is causing a major problem by sending viruses, unwanted messages, and phishing through emails. These days, there are many people who try to steal confidential information by sending fake emails in the form of advertisements and emails which display awards or lottery winnings. Some of the issues faced by the users due to spam emails,

- Internet users are frustrated due to unsolicited emails.
- Important emails are being missed out.
- Reduces the performance of the Internet.
- Loss of millions of dollars worldwide.
- Mail servers can be crashed by spam.

Nature and Significance of the Problem

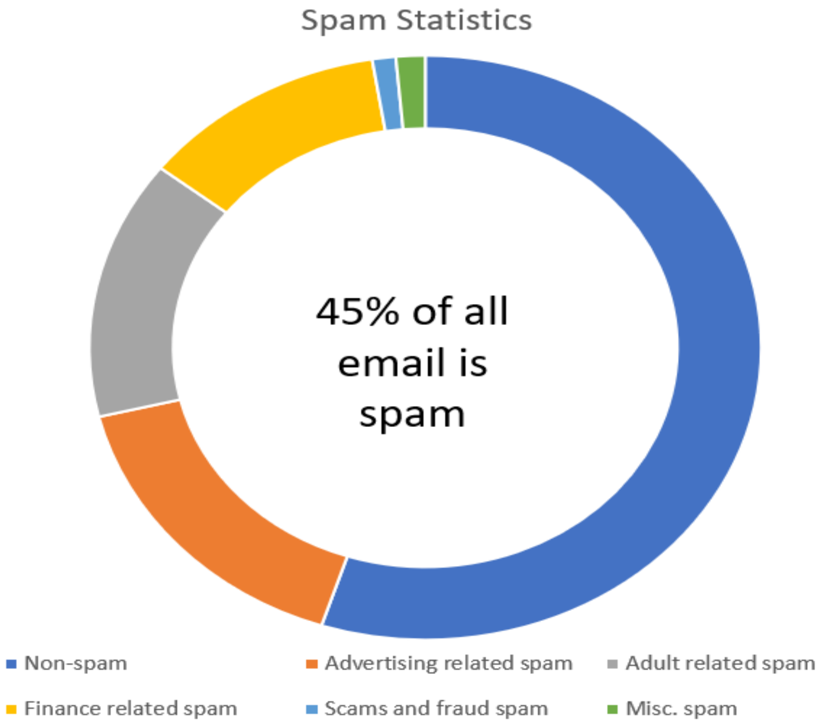
Internet users are facing more issues due to spamming. Despite the development of many detection methods/techniques, in a recent survey, 52% of participants expressed that spam has been a serious issue. Each occurring day, spam emails are responsible for 14.5 billion email messages globally. Spam accounts for 45% - 73% of emails worldwide and reckons an even greater percentage, according to some research organizations. The United States is positioned first in generating the unsolicited bulk emails, along with Korea being positioned as the second-largest (Sorkin, 2020).

Phishing is, also known as identity theft, accounts for 73% of spam emails. Around 36% of these unsolicited/unwanted bulk email messages are advertising-related, which are the most frequent type of spam. Approximately 31.7% of the unsolicited emails are subject to adult-related and is the second most popular type of spam. The third most common type of unwanted emails are related to financial issues, which is roughly 26.5%. While frauds and scams together hold approximately 2.5% of unsolicited email messages (Sorkin, 2020).

The public confidence and trust in communicating through the Internet have been decreased due to spam, as it is affecting both individuals and organizations. 53% of participants lost trust in email communications according to the study conducted in 2005 and this percentage reduced from 62% to 53% from the previous year. As it is affecting both the personal and corporate world, a study conducted found that 52% of the organizations stated that reducing spam email is being their biggest priority. Spamming reduces safety and productivity for the organizations (Corporate world) as it is an annoying issue. All the spam detection techniques developed are producing a belief in fighting against unsolicited bulk emails (Sorkin, 2020).

Figure 3

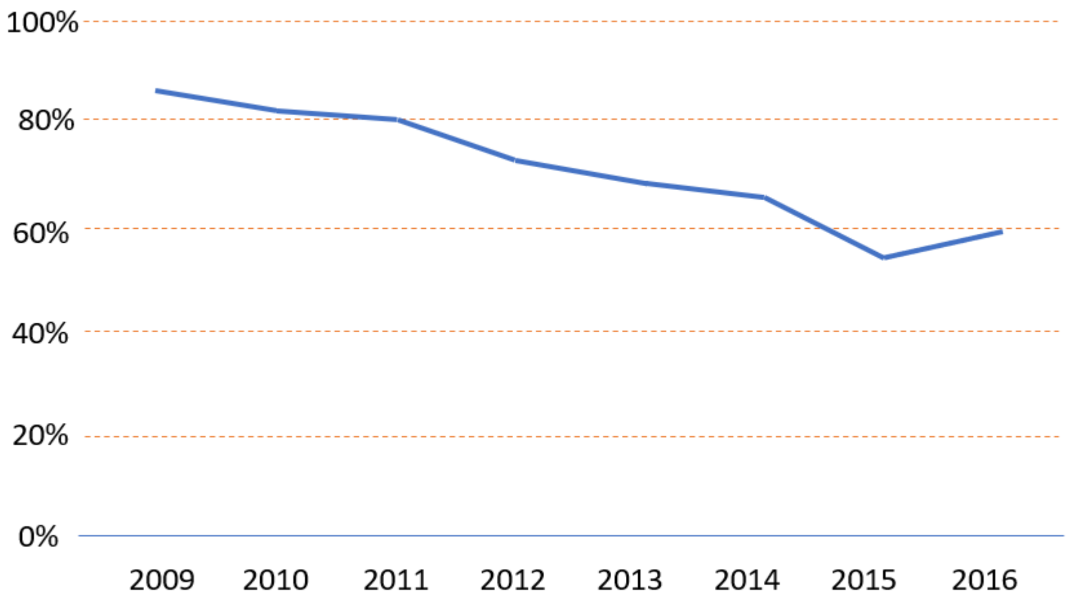
E-mail spam statistics (Bauer, 2018)



E-mail spam is still a problem in the current world and might not be resolved until there's the existence of e-mail communication (Hoffman, 2016). Spam detection techniques have become more effective in blocking spam e-mail messages over the decade. Statistics and studies show that spam is a major issue. The percentage of spamming has remained stable at around 70% over the years (Gudkova & Vergelis, 2017). The spam problem has not been resolved completely as most businesses are at a loss financially. The existing spam detection techniques have some strengths and limitations in the models developed, and no single technique/approach might be an effective solution. At the same time, most of the techniques implemented are performed accurately. All the developed spam detection techniques focus on the importance of maintaining their strengths as they are cost-effective when it comes to Network Resources and IT Administrations. Also, they reduce safety risks and increase security (Jamkatel & Gupta, 2018).

Figure 4

E-mail spam proportion over the years (Gudkova & Vergelis, 2017)



Objective of the Study

The objective of the study is to research how the current email spam detection techniques are detecting, preventing, and evaluating spam emails. The study also demonstrates the effectiveness and accuracy of each spam detection technique.

Study Questions/Hypotheses

1. What are the existing e-mail spam detection techniques developed?
2. How severe is the problem of e-mail spam?
3. How accurately are the existing e-mail spam detection techniques working?
4. Is the problem resolved?
5. Is it getting better or worse?
6. Are the current techniques able to address the problem?

Definition of Terms

- ISP: Internet Service Providers
- IP: Internet Protocol
- IT: Information Technology
- DNS: Domain Name System
- CR: Challenge-Response
- DCC: Distributed Checksum Clearinghouse
- SMTP: Simple Mail Transfer Protocol
- MTA: Mail Transfer Agent
- TCP: Transmission Control Protocol
- HTML: Hyper Text Markup Language
- OCR: Optical Character Recognition
- NB: Naive Bayesian
- ESP: E-mail Service Providers
- CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart

- OSH: Optimal Separating Hyper-plane
- SVM: Support Vector Machines
- SBPH: Sparse Binary Polynomial Hashing
- OSB: Orthogonal Sparse Bigrams
- URL: Uniform Resource Locator
- AUP: Acceptable Use Policy
- TOS: Terms of Service
- PTR DNS: Pointer Record Domain Name System
- RFC: Request for Comments
- DBL: Domain Block List
- SMTP-AUTH: Simple Mail Transfer Protocol – Authentication
- STARTTLS: Start Transport Layer Security
- DNSBL: Domain Name System Blacklist or Domain Name System – based Blackhole List
- ASSP: Anti – Spam SMTP Proxy
- CRM114: Controllable Regex Mutilator
- SPF: Sender Policy Framework
- DKIM: Domain Keys Identified Mail
- DMARC: Domain – based Message Authentication, Reporting and Conformance
- FQDN: Fully Qualified Domain Name
- URIBL: Uniform Resource Identifier Blackhole Lists
- RBL: Real-time Blackhole Lists
- SURBL: Spam URI Real-time Block Lists

Summary

This chapter covered the introduction of our research on identifying how severe the problem is of email spam, which is affecting businesses and individuals. All the spam detection techniques can detect/filter the email messages into spam or ham but cannot reduce spamming. There is a focus on the importance of developing the spam detection techniques to block the unsolicited/unwanted email messages and how the existing spam detection techniques are detecting, preventing, and evaluating the solutions for all the spam e-mail messages that are threatening the e-mail users (individuals and organizations). This study can be used as a reference for future research and would help many specialists, professionals and researchers working in this respective domain to improve and support the necessity for a personal and corporate world.

Chapter II: Background and Review of Literature

Introduction

Nowadays, all types of industries/organizations are unable to run their businesses without the source of the Internet. E-mail is an electronic mail where an individual/user can compose and receive messages from other individuals/users via network servers free of cost (*E-Mail*, 2021). E-mail has several functions in it and is a secured communication medium. E-mail communication websites such as G-mail, Yahoo, and MS Outlook ran through the Internet and were being used by individuals and corporate industries where millions of accounts can be created. Some confidential information is generated when creating each account.

With most of the use being e-mail messages, spam does come into existence, which is a dangerous threat and an annoying issue for computer security. Spam is the source of computer malfunctioning, viruses, phishing attacks, and worms. If any individual/employee of an organization/business opens a spam email and clicks on the link, then it will infect the entire computer system or steal any personal/confidential information. As we see it today, many e-mails being received are spam.

Spamming is a gesture of sending unwanted email messages without the recipient's consent, and the recipient finds it annoying. Recipients may have resulted in limitless financial loss and have fallen under the victim category of these email scams, which pretend to be from reputable organizations with the intention of allowing people to reveal personal data such as passwords and card verification value (CVV). All the E-mail providing websites such as G-mail, Yahoo, and MS Outlook has spam detection techniques in their spam filters to handle the threats effectively. Spam detection techniques can detect these unwanted bulk email messages and prevent them from entering the recipient's inbox.

Background Related to the Problem

One of the major issues taking place around the world is ‘Spam’. Electronic mail (E-mail) was identified as an outstanding advertising tool in the early 1990s as the internet obtained popularity. A person/user can send email messages to millions of people/users free of cost through the Internet. The first email spam recognized was sent to hundreds of users/people on May 1, 1978, through an advertisement by Digital Equipment Corporation for their products. This was sent by a marketer named ‘Gary Thuerk,’ and no further occurrences were made for a long period of time. Spammers accumulate e-mail addresses from websites, chat rooms, customers lists, etc., and these accumulated e-mail addresses can be sold to other spammers, too (*A History of Email Spam*, 2020). There are different types of E-mail spam (*Common Types of Email Spam*, 2019):

1. Commercial Ads
2. Unsolicited Ads
3. Phishing Scams
4. Chain Letters
5. Email Spoofing
6. Hoaxes
7. Money Scams
8. Anti-virus Spam
9. Malware Warnings
10. Political or Terrorist Spam
11. Trojan Horse Email
12. Adult Related Spam

Commercial Advertisements

This type of spam occurs most commonly. In general, all the unwanted bulk messages sent randomly are accounted for as spam. This comprises when authorized websites and companies that you signed up for send out newsletters, advertisements, and many other unwanted messages. Once you sign up for these commercial sites, this will instinctively add you to their mailing list for future communications.

In most cases, these types of messages may be a scam, but the offers might be genuine. It’s better to create another e-mail address for signing up the unnecessary sites so that there is no option for spam to end up in your main inbox (Varnsen, 2020).

Unsolicited Advertisements

These types of messages are received less often when it comes to the range of spam emails, but they are annoying as they pile up in the spam folder. Millions of e-mail advertisements are being sent every day, such as weight loss programs, online degree programs, product offerings, clearance sales, kicking-off merchandise, etc., and buying whatever from these offering e-mails is a bad choice (Varnsen, 2020).

Phishing Scams

It is difficult to identify this kind of e-mail spam. These scam sites are developed in such a way that they look the same as the official financial companies or any other large institutions like Paytm, PayPal, eBay, etc., and deceive people by offering their credentials so that the original accounts can be traced and utilized by the spammers or scammers. To avoid these types of issues, it’s better to visit an official company website and then sign up for it rather than clicking the URL links from the e-mail messages (Varnsen, 2020).

Chain Letters

There are many friends who will be sending us repetitive jokes or thrilling and exciting stories that are asked to be forwarded under some penalties, and this qualifies as one of the e-mail spam types. There are a variety of penalties such as ‘something may happen to you’, ‘you might be in trouble’, ‘you are going to have bad luck’ if you do not forward this e-mail message. Once you forward these types of e-mail messages, you will probably receive more spam e-mails (Varnsen, 2020).

Email Spoofing

This is a more threatening type of spam and takes place when spammers or scammers send e-mail messages to mislead you by impersonating other people's e-mail addresses whom you might know or have a relationship with. This develops belief as it comes from a known person’s e-mail address and is likely to be involved in a scam that is sent through that e-mail message. To avoid this issue, it is better to verify with an individual or the organization directly before providing confidential information or financial details (Varnsen, 2020).

Hoaxes

It’s easy to be involved in this type of spam as it looks more promising. This involves exciting offers which deceive people into believing them, such as ‘obtain your dream body by eating more food and working out less’, ‘get a luxurious car by signing up this link’, ‘become a billionaire in less than a month’. These URL links are created by spammers to grasp your curiosity to administer you to their malicious websites (*Common Types of Email Spam*, 2019).

Money Scams

This type of e-mail spam hurts users a lot as it is involved money. To achieve a huge amount of winnings later, apparently, you must grant some money initially. These spam e-mail messages are easy money assurances. Some e-mail spams include requesting money to donate to poor people or for families that are affected by disasters, such as the Nigerian prince scheme. In other cases, spammers offer scholarships to students and ask that some money be sent initially to receive it (*Common Types of Email Spam*, 2019).

Anti-Virus Spam

Every individual or organization would like to have their systems to be free from viruses. Sometimes we receive e-mail messages stating that our computer system is infected with a virus and to clean it up, to download this anti-virus software. Most individuals whose systems get infected start downloading the software provided in that e-mail message. The software originally infects the systems with worrying viruses, and to clean up the viruses installed from that e-mail message, the software asks for money. To avoid this type of problem, obtain and use anti-virus software from a trusted organization. Also, paid and free versions of anti-virus software are available for all kinds of computer operating systems. In that way, you do not need to download any other anti-virus software from those spam e-mail messages (Varnsen, 2020).

Malware Warnings

These are related to anti-virus spam. People might receive an e-mail message warning that their device has a malware infection, and these types of e-mail messages are likely to be malware warnings spam. The spammers convey that they have a solution to fix your issue if you provide some information they need. To avoid this type of problem, it is better not to respond (*Common Types of Email Spam*, 2019).

Political or Terrorist Spam

Sometimes you receive life-threatening e-mail messages to sneak personal/confidential information as it seems to be from politicians/terrorist/government offices like IRS, FBI, etc., stating that you are in trouble and that police will come and arrest you if you do not take any further step on this notice. To overcome these threats, the spammer demands you to pay cash as legal fees. To avoid these issues, just do not respond instead of panicking. Also, try to get confirmation directly from the company the e-mail originated from and react accordingly (Varnsen, 2020).

Trojan Horse Email

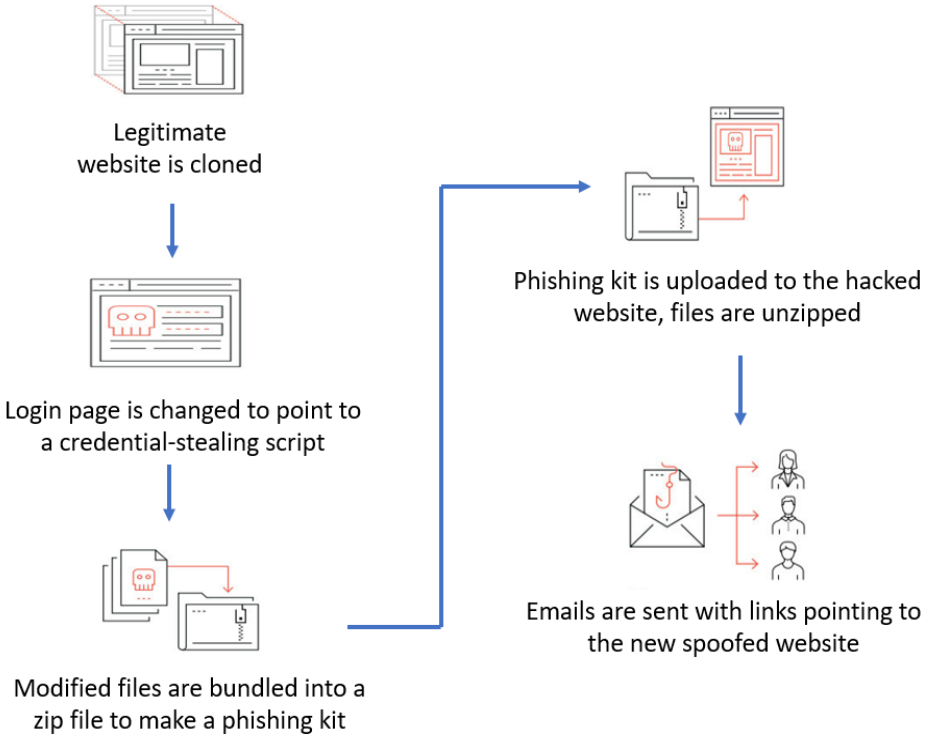
E-mail worms are the most disturbing bugs as it infects the user and the user's contact list. The successful and famous e-mail worm was the “I Love You” bug, which was created in 2000. Once the bug is downloaded, the attached document vanishes from the user's computer system and sends itself to all the user's contact list. To avoid these worms, before opening or downloading any attachments from any e-mail address, it is better to verify with the sender that it is free from malware (Varnsen, 2020).

Adult Related Spam

Spammers send adult-related images or videos through e-mail messages as it is one of the easiest moneymaking methods and enlarges people’s attentiveness. This is the main source for spammers to capitalize on the curiosity of people and create malfunctioning e-mail messages using improper images and videos. There is a possibility for spammers to threaten the recipients (victims) by blackmailing. To avoid this type of spam, do some research before visiting adult related sites (Varnsen, 2020).

Figure 5

Anatomy of how phishing works (Fruhlinger, 2020)


Legitimate website is cloned
Login page is changed to point to a credential-stealing script
Modified files are bundled into a zip file to make a phishing kit
Phishing kit is uploaded to the hacked website, files are unzipped
Emails are sent with links pointing to the new spoofed website

To be on the safer side from these types of spam e-mail messages, there are many ways to prevent e-mail spams from entering your inbox (Spector, 2016):

1. Do not respond to the spam
2. Hiding your e-mail address
3. Changing your e-mail addresses
4. Using a third-parties anti-spam detection technique
5. Training your detection techniques accordingly

Do Not Respond to the Spam

When you receive an e-mail message, do not open the e-mail if you recognize it as spam. If you doubt any opened e-mail message is spam, then do not click on the links and do not download any attachments from it. Instead, close the doubted e-mail message and contact the email sender straight away if it is from a known person or organization you are working with. Also, let the sender know that you have received a malicious e-mail message from their account (Spector, 2016).

Hiding your E-mail Address

There is an increased chance of getting spam e-mail messages if your e-mail address is known to many people. It is better to restrict your e-mail address within the organization you are working with. Try not to advertise your e-mail address on public websites unless it is necessary. It’s better to create and use a secondary e-mail address if you want to sign up for any online websites that have less importance. Avoid sharing your primary e-mail address with non-essential individuals, organizations, websites, and companies (Spector, 2016).

Changing your E-mail Address

If you are receiving many spam e-mails as you responded to them previously and your inbox is full of spam, then it’s better to change your e-mail address as this is an extreme situation to avoid spam e-mails. Inform all the individuals and authorized personnel about the change of your e-mail address so that you can receive the necessary e-mails to the new e-mail address. In this way, your spam count can drop down straight away dramatically (Spector, 2016).

Using a Third-Parties Anti-Spam Detection technique

This feature can protect you and your organization’s time and money because it can screen the incoming e-mails prior to reaching out to you. Most of the third-party e-mail anti-spam detection techniques will provide access to you from their servers if your server is unable to perform for some cause. There are fewer chances of being a victim as these detection techniques trace the spam effectively (Lackey, 2017).

Training your Detection Technique Accordingly

Once you find spam in your e-mail inbox, inform the mail client stating that this specific e-mail message is spam rather than deleting it. Then you can click on the ‘Report spam’ option so that it enters the spam folder. Train the clients regarding your false positives. When you open your spam folder and find some of the e-mail messages as legitimate, then inform the clients by clicking on the ‘Not Spam’ option. So, if you train your detection techniques accordingly, it works more effectively without the occurrence of mistakes (Spector, 2016).

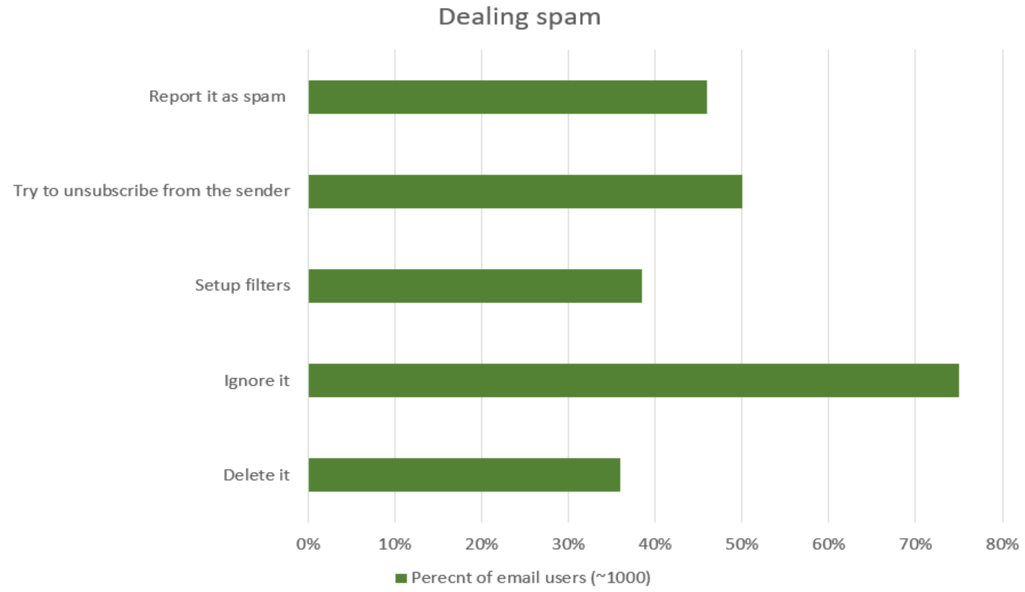
Dealing with the Spam Emails

Daily, many email users deal with spam emails, as you can see from the percentages in figure 6. An email user should deal with the email spam in the following way (Lessard, 2013):

1. Delete the email as soon as you see the weird content in it.
2. Ignore the email if you see something wrong with it.
3. Set up filters to avoid spam.
4. Try to unsubscribe from the sender.
5. Report it as spam to the service provider.

Figure 6

How do you typically deal with email spam (Lessard, 2013)



Literature Related to the Problem

Spam e-mail computer security threat remains an annoyance for all organizations and individuals forever, whereas many other computer security threats keep occurring. As a minimum, as it could, Spam e-mails can put a hold on your busy scheduled day by driving you to open some malicious e-mail messages (miracle offers) and deleting them. This leads to spam being able to ruin your company's servers, networks, and computer systems by unleashing the bugs (viruses). All the anti-spam detection techniques and professionals can keep down the spam range between 50 to 90 percent of all the e-mail messages. Downloading and installing anti-spam software/applications on your computer system or company's mail servers can reduce the number of spam e-mail messages that a person has to account for but cannot prevent sending unwanted bulk e-mail messages from spammers. All the anti-spam detection techniques filter the spam emails by different approaches and can use one or more techniques to spot the spam and prevent it from reaching the email inbox (Satterfield, 2006).

Most spam detection techniques run a series of checks on e-mail messages to regulate the probability of a message being spam or not. Some of the spam detection techniques allow e-mail messages to receive from necessary senders by blocking all the odd sender's email addresses. Other spam detection techniques need some information to interact with the recipient, while some methods are transparent to both the recipient and sender (Satterfield, 2006).

Nowadays, customers/users expect more quality features from their mailbox clients to be on the safer side from spammers, attackers and abusers who spread viruses and trojans through e-mail messages. The user's expectations to keep their email inboxes free from spam have been strengthened as the design of the security system should work on par with the technology being advanced as spam detection techniques developed over time, spammers, attackers, abusers, and fraudsters have evolved. Most of the users in today's world with the use of the Internet have the likelihood of carrying their confidential details and bank transactions over e-mail messages. The user might face lethal consequences if the attack takes place in a user's inbox (Pitkar, 2020).

Machine learning and Artificial intelligence detection techniques help in detecting the vulnerabilities and controlling the attacks in the system while also preventing the detection of classification samples for future oddities. This makes the technique even smarter to prevent spam attacks (Pitkar, 2020). To prevent domain spoofing, the efficient way is to verify the domain authentications registered in the domain name system with the sender's IP address. Most webmail providers come up with a 'not spam' option in the spam/junk folder to spot the false positives along with the 'Spam' option in the inbox folder (Rao & Reiley, 2012).

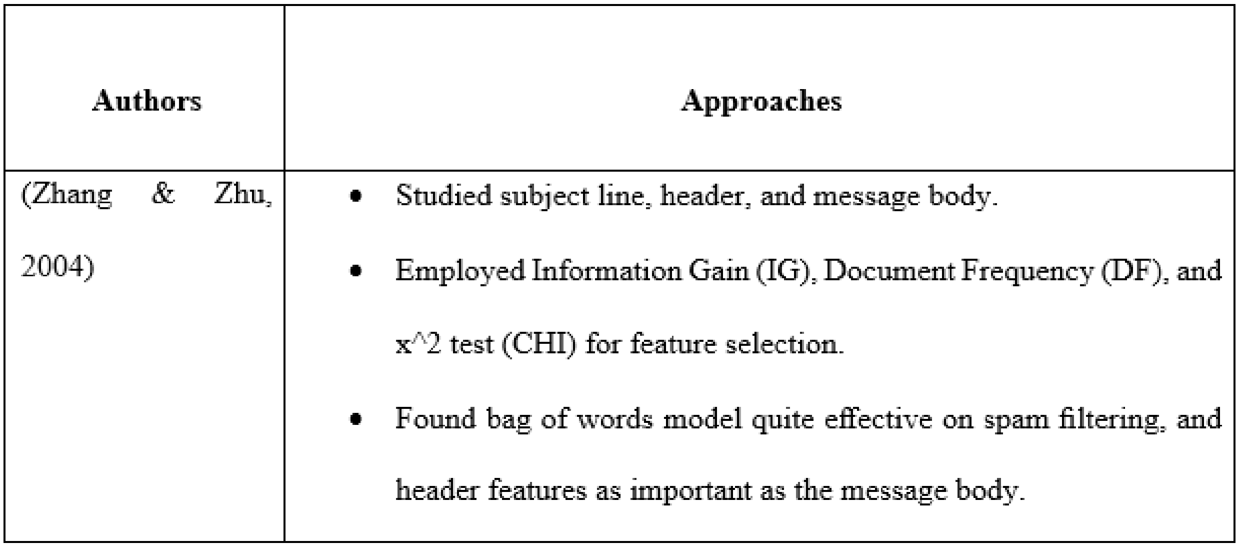
In recent years, many experts and detection techniques have progressed exceedingly well to secure emails efficiently. But the transporting security for the emails is not indicating the main issues as the ‘authentication’ is different from the ‘security’, which does not provide control over the email inbox. If a user can validate the sender of an email in the exchanged conversations, then the maximum amount of spam can be prevented. It is very important to secure an e-mail message as none of the technologies matches its benefits (Greve, 2019).

The summary of feature extraction and selection techniques is mentioned in table 1, along with the summary of machine learning techniques with their strengths and limitations according to the author's perspectives (Algorithm, Architecture, Methods, and Trends) were mentioned in table 2.

Table 1

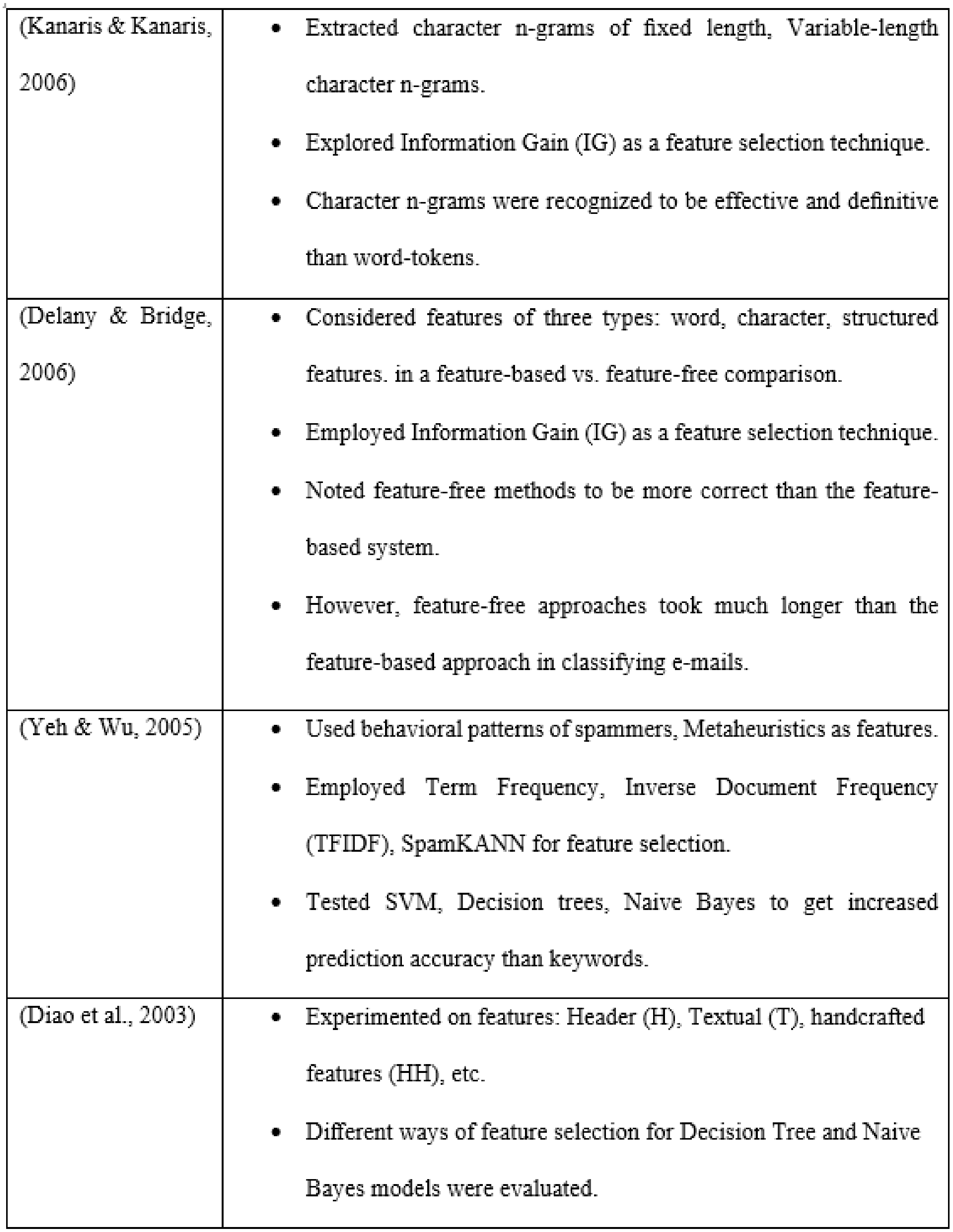
A summary of Feature Extraction and Feature Selection techniques in popular literature

(Bhowmick & Hazarika, 2016)



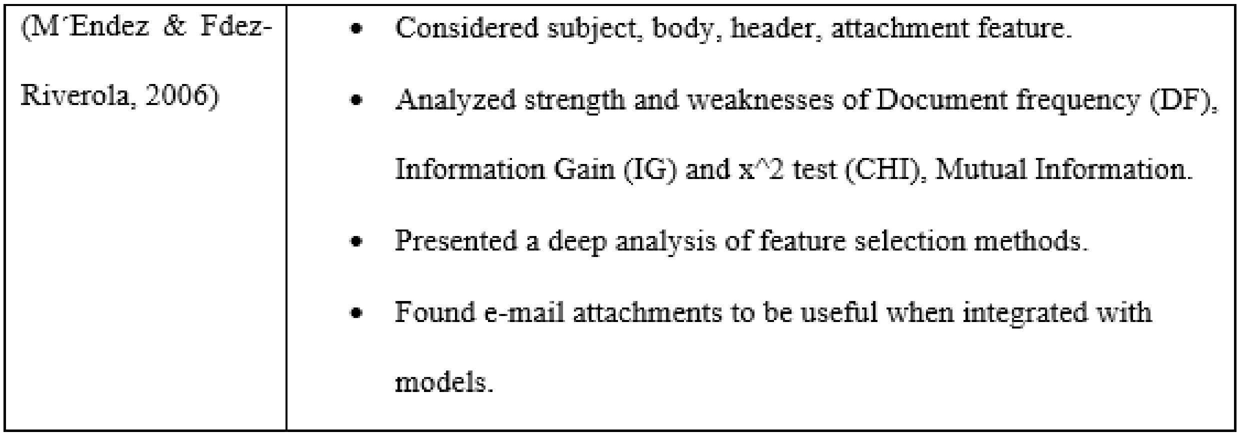
Authors	Approaches
(Zhang & Zhu, 2004)	• Studied subject line, header, and message body. • Employed Information Gain (IG), Document Frequency (DF), and x^2 test (CHI) for feature selection. • Found bag of words model quite effective on spam filtering, and header features as important as the message body.

Table 1 (Continued)



(Kanaris & Kanaris, 2006)	• Extracted character n-grams of fixed length, Variable-length character n-grams. • Explored Information Gain (IG) as a feature selection technique. • Character n-grams were recognized to be effective and definitive than word-tokens.
(Delany & Bridge, 2006)	• Considered features of three types: word, character, structured features. in a feature-based vs. feature-free comparison. • Employed Information Gain (IG) as a feature selection technique. • Noted feature-free methods to be more correct than the feature-based system. • However, feature-free approaches took much longer than the feature-based approach in classifying e-mails.
(Yeh & Wu, 2005)	• Used behavioral patterns of spammers, Metaheuristics as features. • Employed Term Frequency, Inverse Document Frequency (TFIDF), SpamKANN for feature selection. • Tested SVM, Decision trees, Naive Bayes to get increased prediction accuracy than keywords.
(Diao et al., 2003)	• Experimented on features: Header (H), Textual (T), handcrafted features (HH), etc. • Different ways of feature selection for Decision Tree and Naive Bayes models were evaluated.

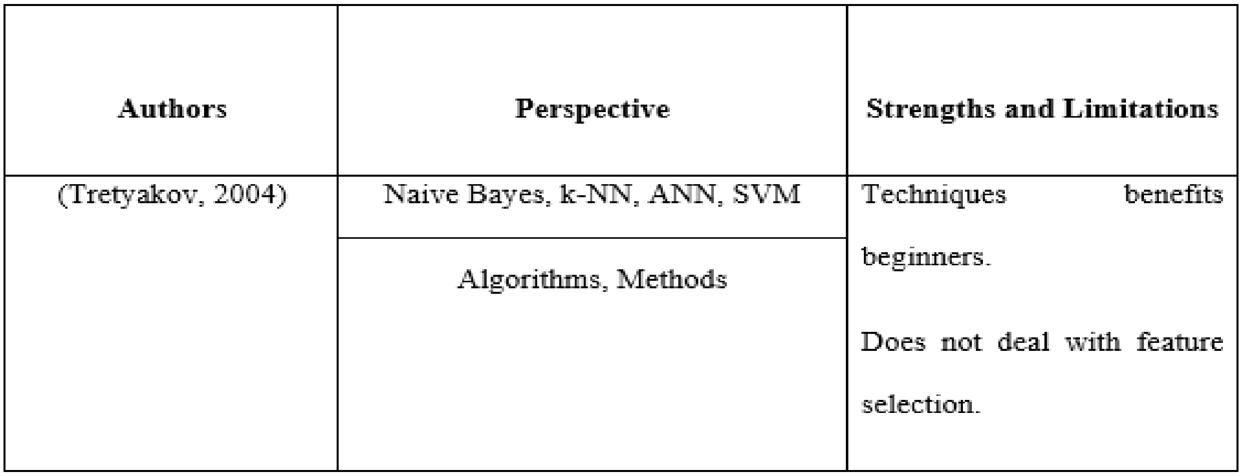
Table 1 (Continued)



(M´Endez & Fdez-Riverola, 2006)	- Considered subject, body, header, attachment feature. - Analyzed strength and weaknesses of Document frequency (DF), Information Gain (IG) and x^2 test (CHI), Mutual Information. - Presented a deep analysis of feature selection methods. - Found e-mail attachments to be useful when integrated with models.

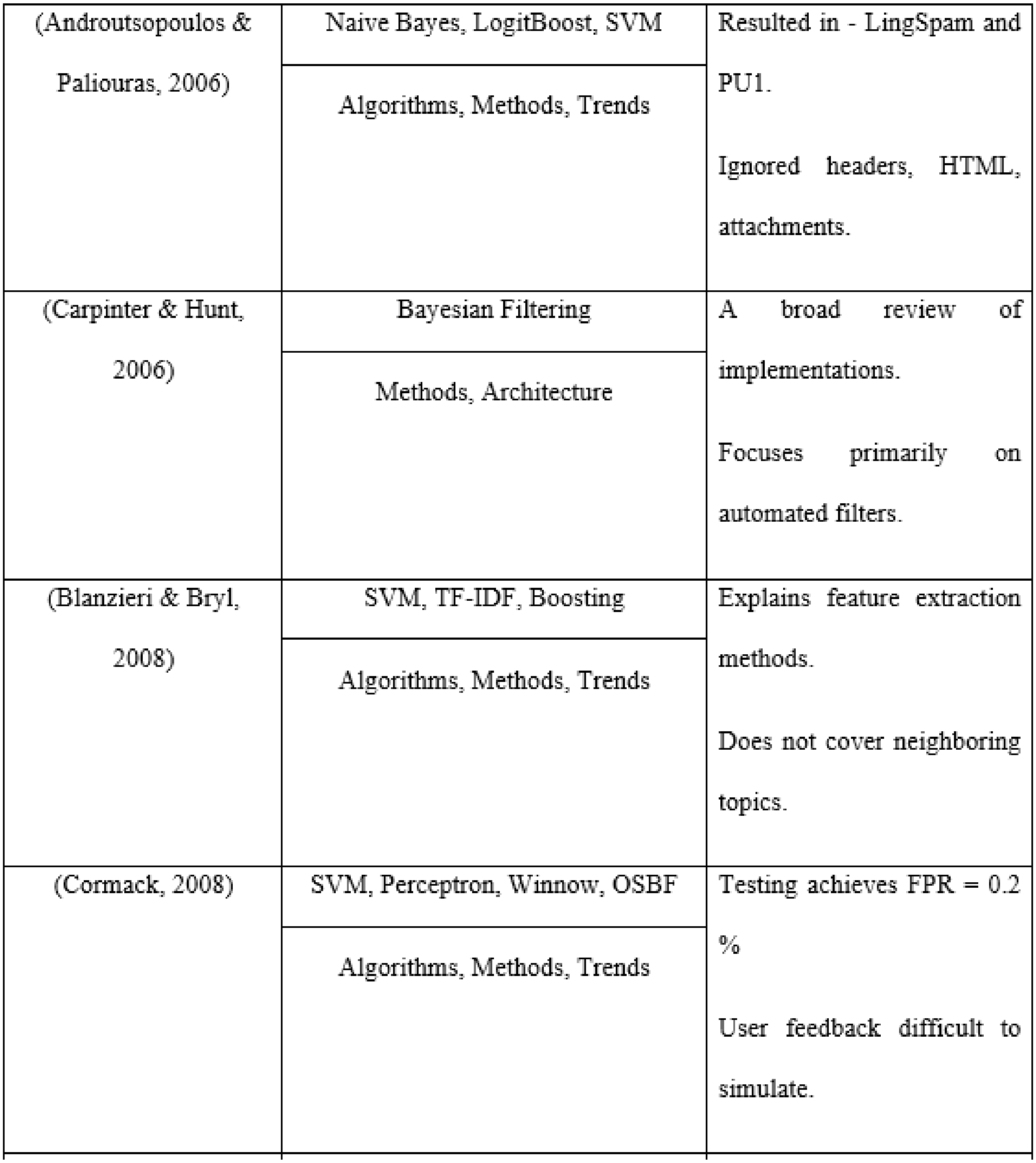
Table 2

A summary of popular machine learning techniques by authors according to their perspectives (Algorithm, Architecture, Methods, and Trends), *with their strengths and limitations* (Bhowmick & Hazarika, 2016)



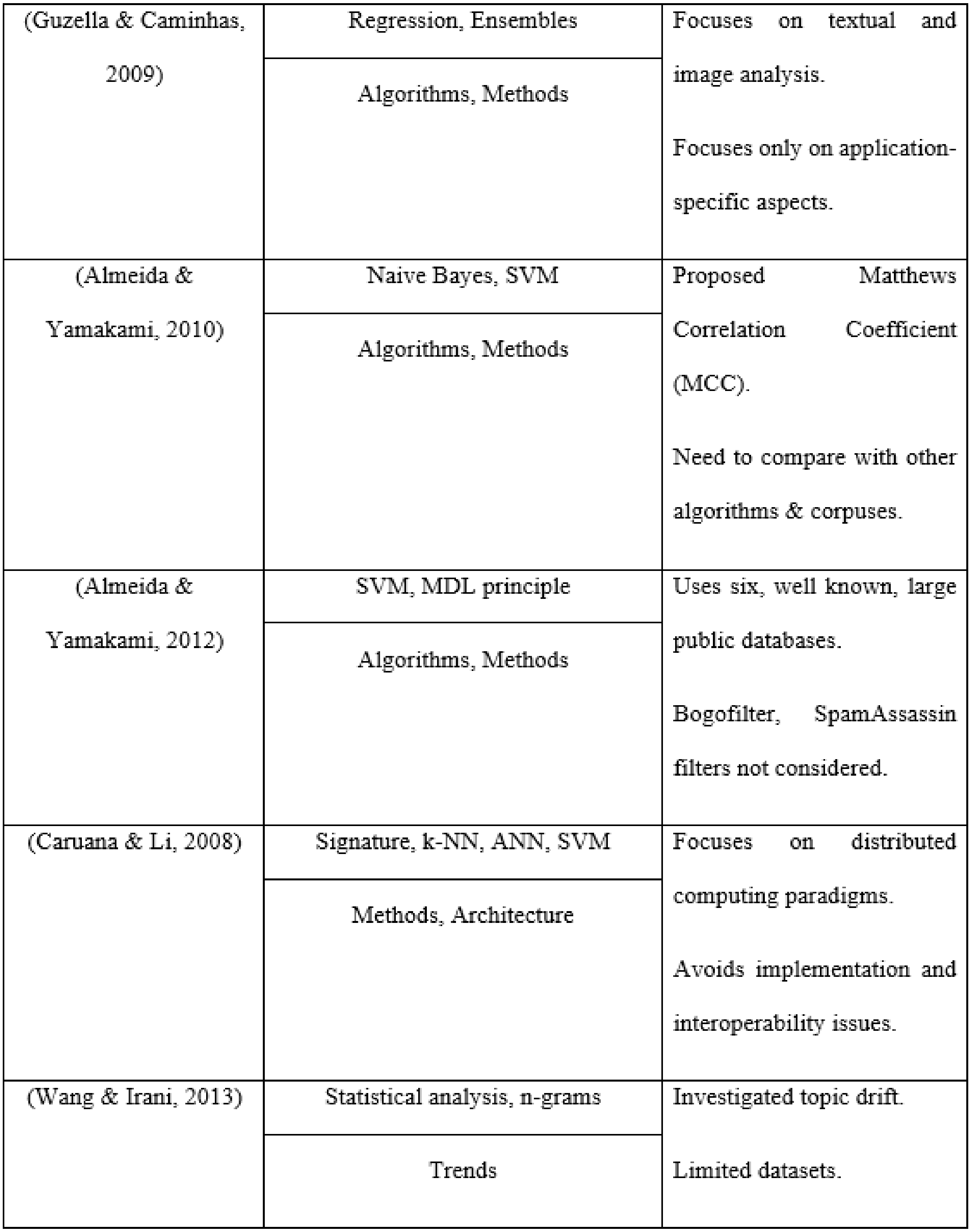
Authors	**Perspective**	**Strengths and Limitations**
(Tretyakov, 2004)	Naive Bayes, k-NN, ANN, SVM	Techniques benefits beginners. Does not deal with feature selection.
	Algorithms, Methods	

Table 2 (Continued)



(Androutsopoulos & Paliouras, 2006)	Naive Bayes, LogitBoost, SVM Algorithms, Methods, Trends	Resulted in - LingSpam and PU1. Ignored headers, HTML, attachments.
(Carpinter & Hunt, 2006)	Bayesian Filtering Methods, Architecture	A broad review of implementations. Focuses primarily on automated filters.
(Blanzieri & Bryl, 2008)	SVM, TF-IDF, Boosting Algorithms, Methods, Trends	Explains feature extraction methods. Does not cover neighboring topics.
(Cormack, 2008)	SVM, Perceptron, Winnow, OSBF Algorithms, Methods, Trends	Testing achieves FPR = 0.2 % User feedback difficult to simulate.

Table 2 (Continued)

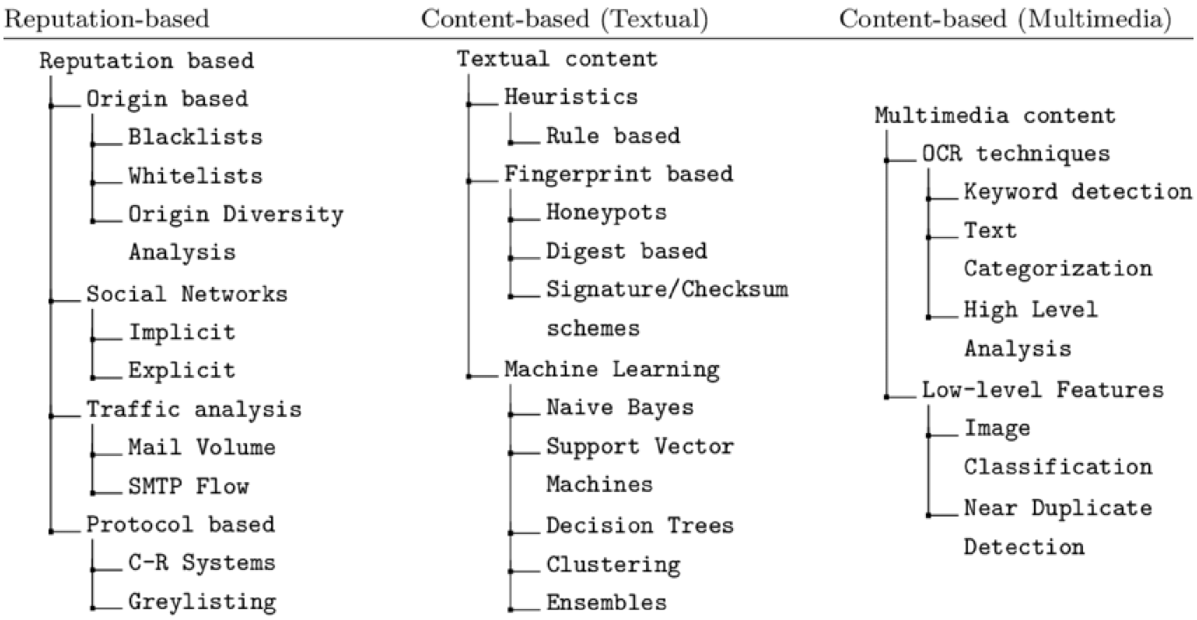


(Guzella & Caminhas, 2009)	Regression, Ensembles Algorithms, Methods	Focuses on textual and image analysis. Focuses only on application-specific aspects.
(Almeida & Yamakami, 2010)	Naive Bayes, SVM Algorithms, Methods	Proposed Matthews Correlation Coefficient (MCC). Need to compare with other algorithms & corpuses.
(Almeida & Yamakami, 2012)	SVM, MDL principle Algorithms, Methods	Uses six, well known, large public databases. Bogofilter, SpamAssassin filters not considered.
(Caruana & Li, 2008)	Signature, k-NN, ANN, SVM Methods, Architecture	Focuses on distributed computing paradigms. Avoids implementation and interoperability issues.
(Wang & Irani, 2013)	Statistical analysis, n-grams Trends	Investigated topic drift. Limited datasets.

Here are the different existing spam detection techniques based on reputation, textual and multimedia contents.

Table 3

Existing e-mail spam detection techniques (Bhowmick & Hazarika, 2016)



Reputation-based

- Reputation based
  - Origin based
    - Blacklists
    - Whitelists
    - Origin Diversity Analysis
  - Social Networks
    - Implicit
    - Explicit
  - Traffic analysis
    - Mail Volume
    - SMTP Flow
  - Protocol based
    - C-R Systems
    - Greylisting

Content-based (Textual)

- Textual content
  - Heuristics
    - Rule based
  - Fingerprint based
    - Honeypots
    - Digest based
    - Signature/Checksum schemes
  - Machine Learning
    - Naive Bayes
    - Support Vector Machines
    - Decision Trees
    - Clustering
    - Ensembles

Content-based (Multimedia)

- Multimedia content
  - OCR techniques
    - Keyword detection
    - Text Categorization
    - High Level Analysis
  - Low-level Features
    - Image Classification
    - Near Duplicate Detection

All the different existing spam detection techniques mentioned are successful in filtering spam e-mail messages. These techniques are based on Reputation, Word content (Textual) and Media content.

Summary

In today’s world, we can see the importance of e-mail messages as 95% of the businesses run through them by using this technology. So, the chances of an email getting attacked or spammed are high. We can see the various types of spam attacks taking place in today’s email world. Being cautious by not responding to the spam e-mail and reporting them to the mail providers rather than deleting them is the best way to prevent the spam e-mails. Many experts developed spam detection techniques with different approaches to filter spam emails before it reaches your inbox. Some of the developed spam detection techniques have some limitations in filtering out spam e-mails. Here we have explored the types of e-mail spam attacks that an individual or organization needs to be aware of and the ways to prevent e-mail spam messages from entering your inbox.

Chapter III: Methodology

Introduction

This chapter gives us an idea about how we would be proceeding with our study of "how the current email spam detection techniques are detecting, preventing and evaluating the spam emails". Here we will demonstrate the overall review of current and successful email spam detection techniques. We will review the techniques, taxonomy, and pertinent ideas. Many implemented techniques were stated in the previous chapters. Hybrid architectures on feature selections were used to increase efficiency by decreasing the error rate. We will gather the information and mainly focus on the data that is effective for us to evaluate the analysis. Here in this chapter, we introduce our methodology of how we would accomplish the goal of this study based on the resources we use.

Currently, to prevent spam email messages, various e-mail spam filtering methods have been developed using different concepts and algorithms. Here in this section, certain e-mail spam filtering techniques and the effectiveness of their processes are described,

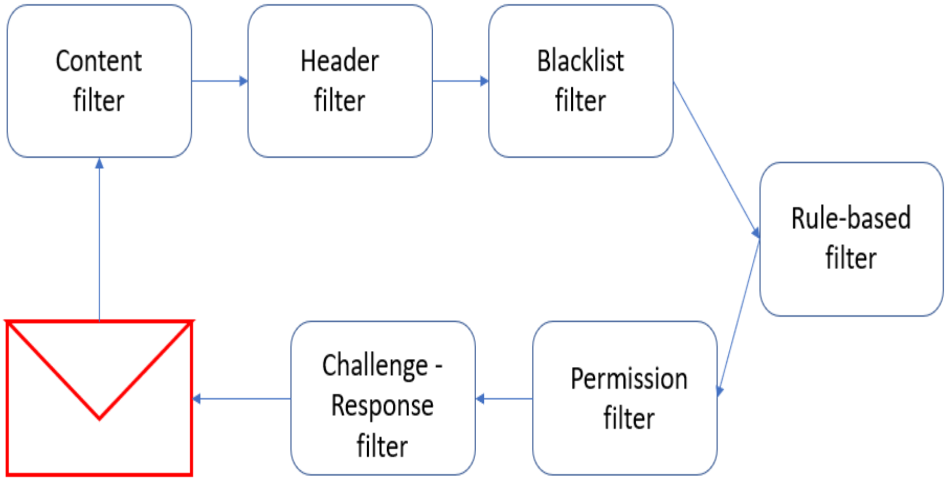
1. Standard Email Spam Filtering Technique
2. Client-side and Enterprise Level Email Spam Filtering Techniques
3. Case Base Email Spam Filtering Technique

Standard Email Spam Filtering Technique

To regulate whether the email message is spam or legitimate, the email spam filtering methods operate by a set of protocols. From figure 7, we can see that the standard email spam filtering technique executed the analysis by sticking to a few procedures and functioning as a classifier.

Figure 7

The standard process of email spam filtering technique (Bhuiyan & Ashiquzzaman, 2018)

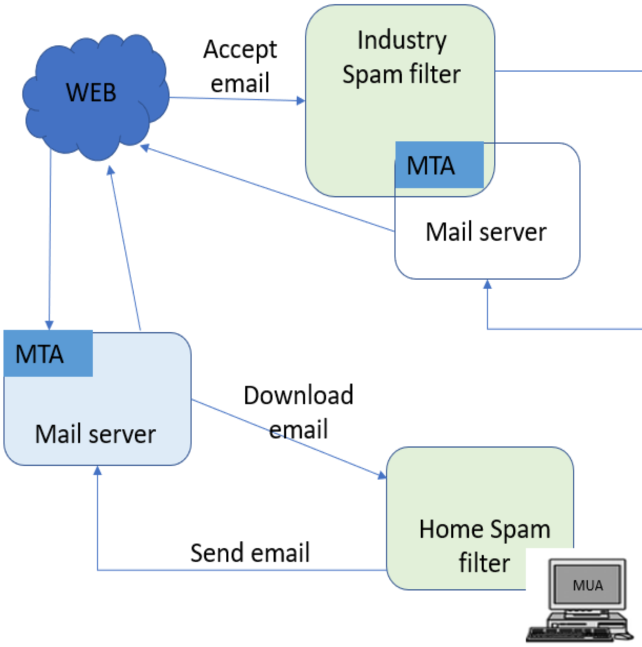


Content filter regulates the spam email message by implementing machine learning techniques. Next, the data derived from the email header will be functioned by header filter. The emails fetching from the blacklist file will be stopped by the blacklist filters which determines spam email messages. Based on a user-defined basis, the sender can be recognized through a subject line by Rule-based filters. By receiving the recipient’s pre-approval, the permission filters will send an email message. The Challenge-Response filter functions by implementing algorithms for receiving authorization from the sender to send an email message (Bhuiyan & Ashiquzzaman, 2018).

Client-side and Enterprise Level Email Spam Filtering Techniques

Figure 8

Client-side and Enterprise Level Email Spam Filtering Techniques (Bhuiyan & Ashiquzzaman, 2018)



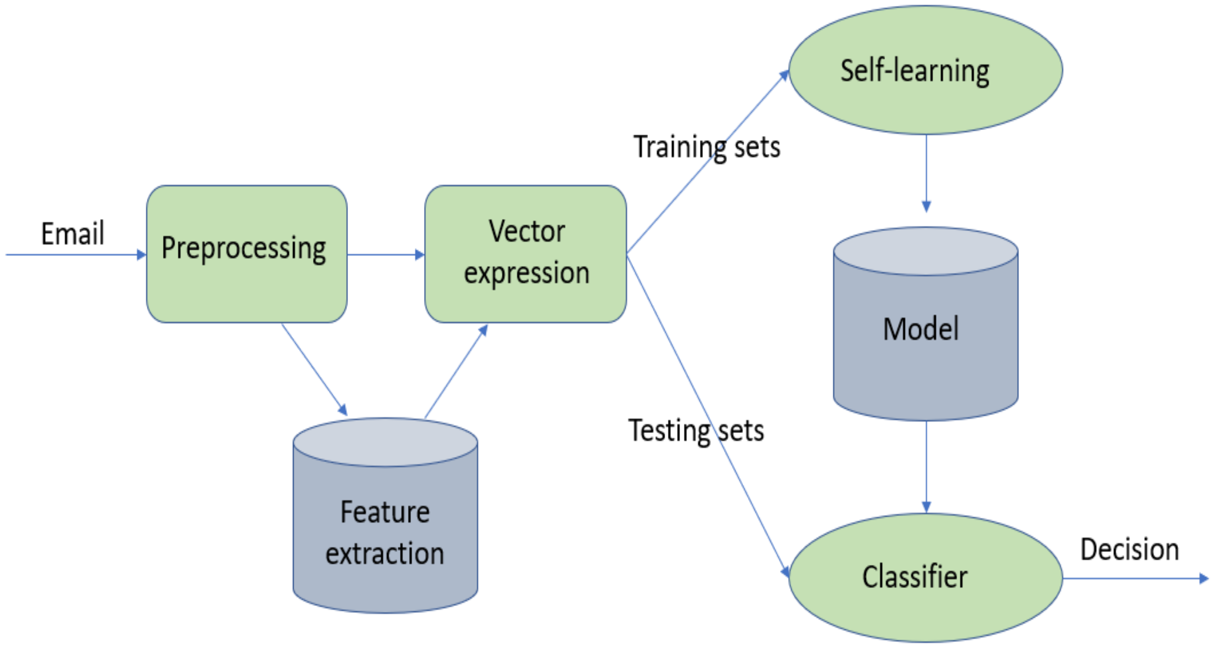
To secure email transmission for a single client, the client-level spam filtering system delivers certain frameworks. Using Internet Service Providers (ISP), clients can access email messages. By installing the frameworks on a personal computer (PC), clients can effortlessly filter spam emails. These frameworks communicate with the Mail User Agent (MUA) and filter out the inbox of clients by originating and managing the email messages (Bhuiyan & Ashiquzzaman, 2018).

In Enterprise level spam filtering, the installed frameworks on the mail server communicate with Mail Transfer Agent (MTA) to classify the incoming email messages and to categorize the spam email on the server itself. Based on this process, the user can filter the spam email messages more efficiently on that server by installing relevant frameworks on the system. A set of instructions are attached to an email message, which can compute a score-based principle that is viable, as these email spam filtering frameworks currently use principle-based scoring criteria. If the value of an email message exceeds the threshold value, then it is considered a spam email message. The functions are remodeled consistently to block the email messages automatically by implementing a list-based method, as the spammers are coming up with different approaches (Bhuiyan & Ashiquzzaman, 2018).

Case Base Email Spam Filtering Technique

Figure 9

Case Base Email Spam Filtering Technique (Sharma & Sharma, 2018)



This filtering system is one of the most important methods for Machine Learning techniques and is also known as a sample base filtering system. Figure 9 demonstrates a sample architecture of a case base filtering system in detail by implementing Machine learning techniques.

Initially, all the email messages (spam or ham) are extracted through the collection model from a user's email. Later, the first transmission begins with pre-processing procedures through analyzing the process, client interface, email data classification and highlighting feature extraction.

Here the vector expression classifies the data into ‘training set’ and ‘testing set’ so that the Machine Learning techniques are implemented on these two different data sets to regulate the email message as spam or ham. We can decide if an email message is a spam or ham through the self-learning model and classifier’s result (Bhuiyan & Ashiquzzaman, 2018).

Design of the Study

The design of this study is based on the category of approaches that the detection techniques implemented. The taxonomy of E-mail spam detection techniques was classified based on Reputation, Textual content, and Multimedia content. Approaches based on Origin, Social Networks, Protocols, and Traffic Analysis come under Reputation (Bayati & Jabbar, 2015). Methods based on Rule, Fingerprint and Machine learning fall under Textual (word) content. Optical Character Recognition (OCR) techniques, Community based, and Low-level features come under Multimedia content. We evaluated the techniques that were already implemented and demonstrated how these techniques are maintained (updated) with the evolution of spam. By considering all the aspects, we will provide awareness to the e-mail users on training the techniques with the false positives and on how to respond when you recognize an email as spam.

E-mail Spam Detection Techniques

Here, we are classifying e-mail spam detection techniques in detail from table 3.

1. Based on reputation
2. Based on word (Textual) content
3. Based on multimedia content

Table 4

Spam detection techniques based on Reputation

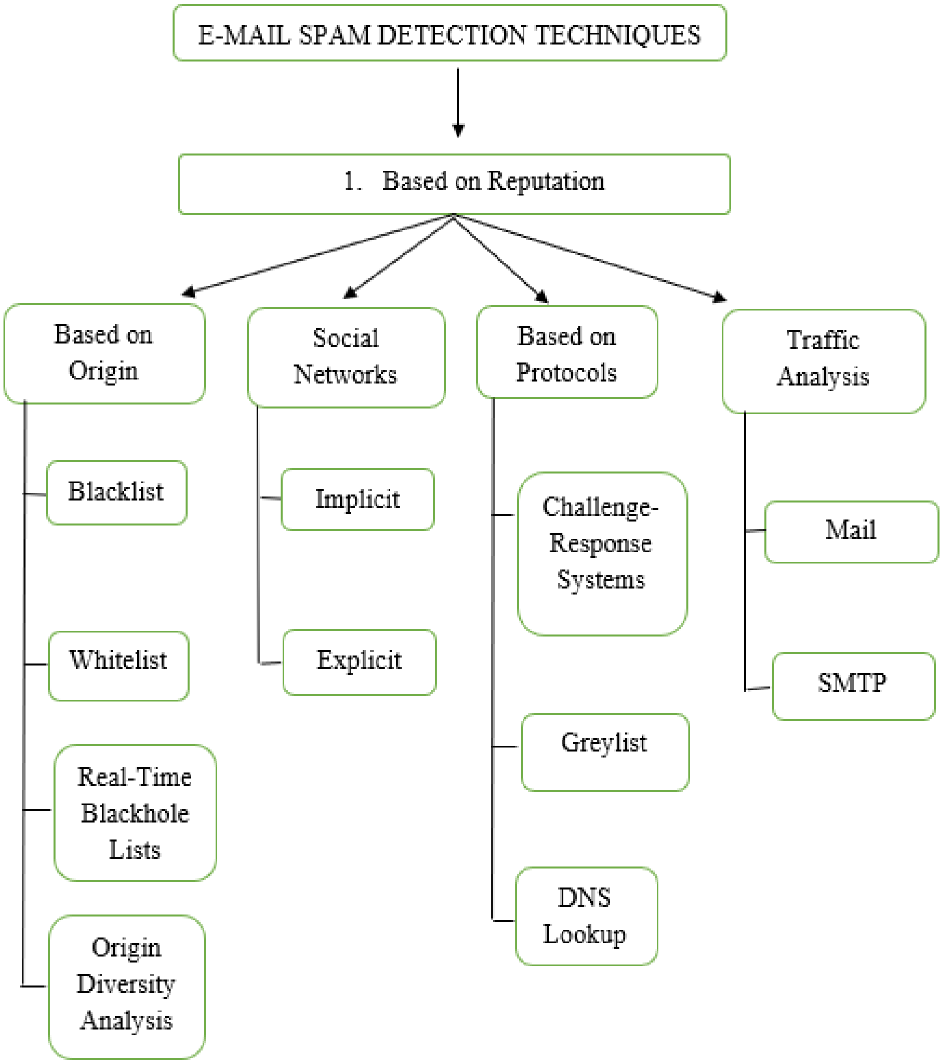


Table 5

Spam detection techniques based on Words (Textual) content

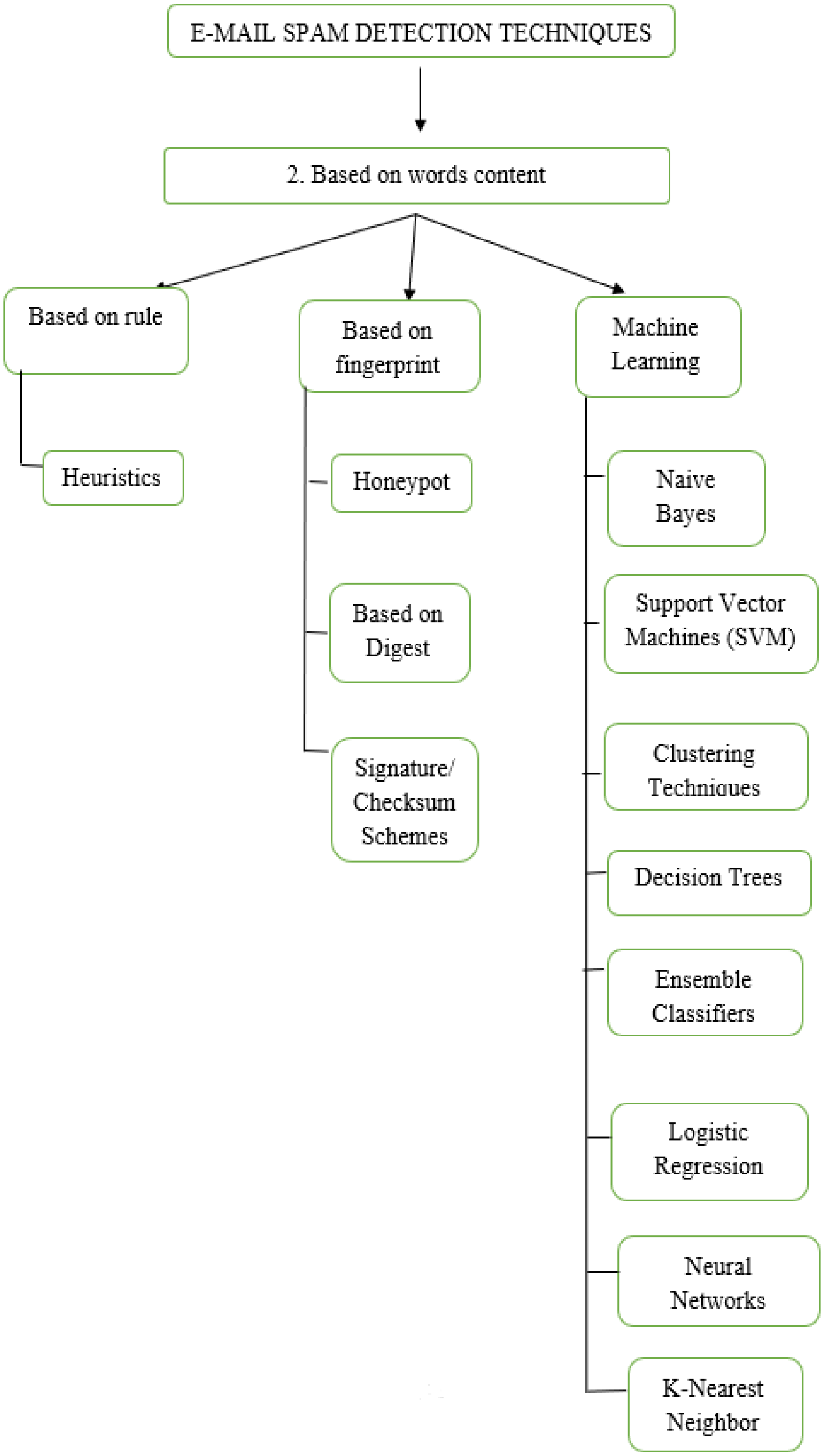
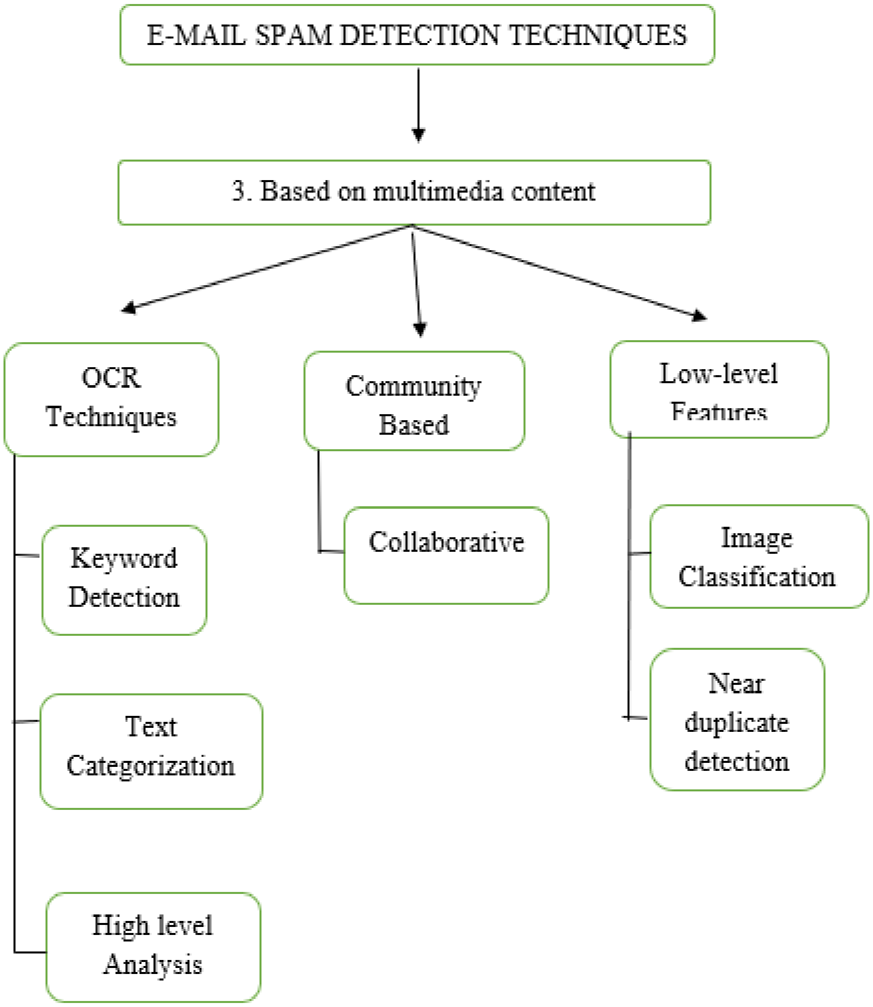


Table 6

Spam detection techniques based on Multimedia content



Examples and datasets from other research papers are considered in this study, which is useful in evaluating the performances. The study questions were considered while evaluating each detection technique. Many research resources have been explored for the proper analysis of the current email spam detection techniques. We have come across the different ways of approaches to detect spam e-mail messages while evaluating them. Intimating the false positives to the email providers will help in training the detection techniques.

Data Collection

We collected the data from Articles (Academic and general), Certified journals, IEEE papers, Google Scholar, Academic books, Research papers, well written papers, ACM Digital Library, Research Gate, and other online documents from the websites. From the collected information, we evaluated the techniques based on the performance of the detection and prevention and made sure how accurate are these techniques. Many researchers or specialists will not be able to share the details with respect to their approaches as they are confidential, so we use the internet as the major source for this study. We will be focusing on the approach of the detection technique and its strengths and limitations while evaluating. The Study Questions/Hypotheses that were mentioned will be considered and answered at the end of this study.

Tools and Techniques

Many filtering and detection techniques were developed to stop spam emails from entering the email user's inboxes. However, none of these detection techniques are the out-and-out solutions for the spam problem. All the filtering methods and the detection techniques have issues with their algorithms by obstructing some false positives (obstructing the legitimate emails wrongly) and by allowing false negatives into the user's inboxes (allowing the spam emails into the inboxes). The cost of rejecting legitimate emails from entering the inboxes is huge, which is associated with the loss of time and effort.

There are numerous existing email spam detection techniques. They are Challenge/response (C-R) systems, Checksum-based, Rule-based, Content-based (Textual and Multimedia), DNS based blacklists, Machine learning-based systems (Naïve Bayes, Support Vector Machines, Decision Trees, Clustering, Neural networks and so on), Cost-based, Reputation-based, Origin based, Traffic analysis, Protocol based, Social networks based, OCR techniques, Fingerprint-based, Heuristics, Hybrid filtering, Honeypots, Tarpits, Reverse DNS checks, Contact forms, Ham passwords, Egress spam filtering and many other techniques. All these techniques are categorized into different sections.

Data Presentation

These detection techniques can be classified into four sections, as mentioned in table 7:

1. Necessary actions needed by End-user techniques: The mandatory steps that should be followed by the email users.
2. Automated techniques by email administrators: Techniques that are operated by the email administrators.
3. Automated techniques by email senders: Steps that should be followed by the email senders.
4. Law enforcement officials and researchers: Legal measures needed to be taken by the law enforcement officials.

Table 7

Four sections of spam detection techniques ("Anti-Spam Techniques," 2020)

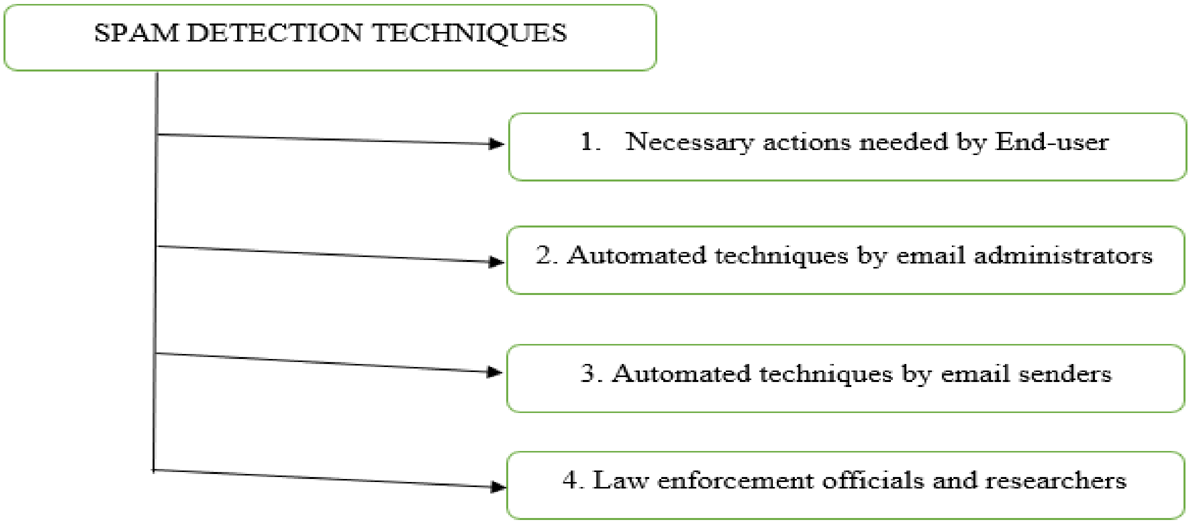

SPAM DETECTION TECHNIQUES
1. Necessary actions needed by End-user
2. Automated techniques by email administrators
3. Automated techniques by email senders
4. Law enforcement officials and researchers

Table 8

Necessary actions needed by End-user techniques ("Anti-Spam Techniques," 2020)

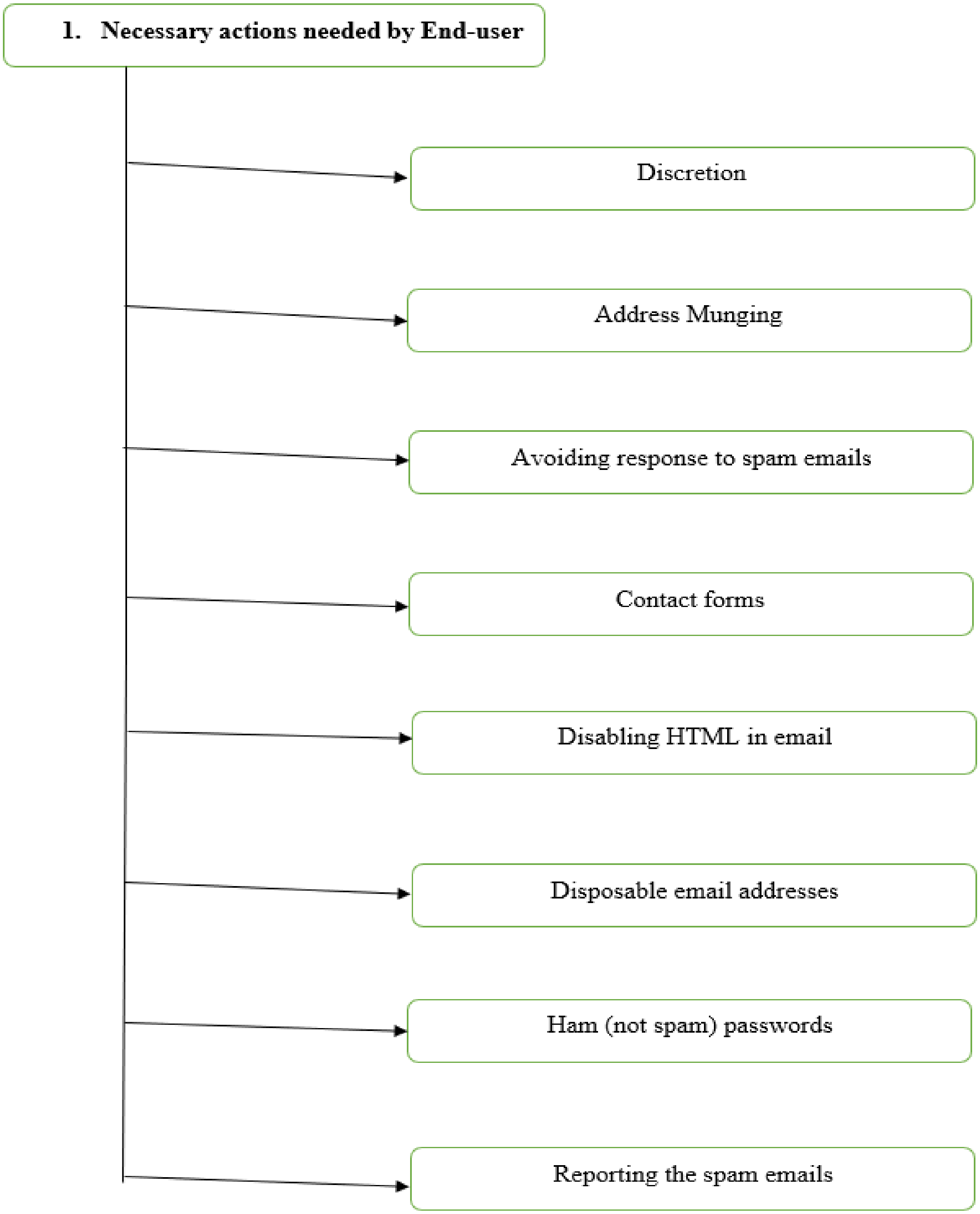

1. Necessary actions needed by End-user
Discretion
Address Munging
Avoiding response to spam emails
Contact forms
Disabling HTML in email
Disposable email addresses
Ham (not spam) passwords
Reporting the spam emails

Table 9

Automated techniques by email administrators (“Anti-Spam Techniques,” 2020)

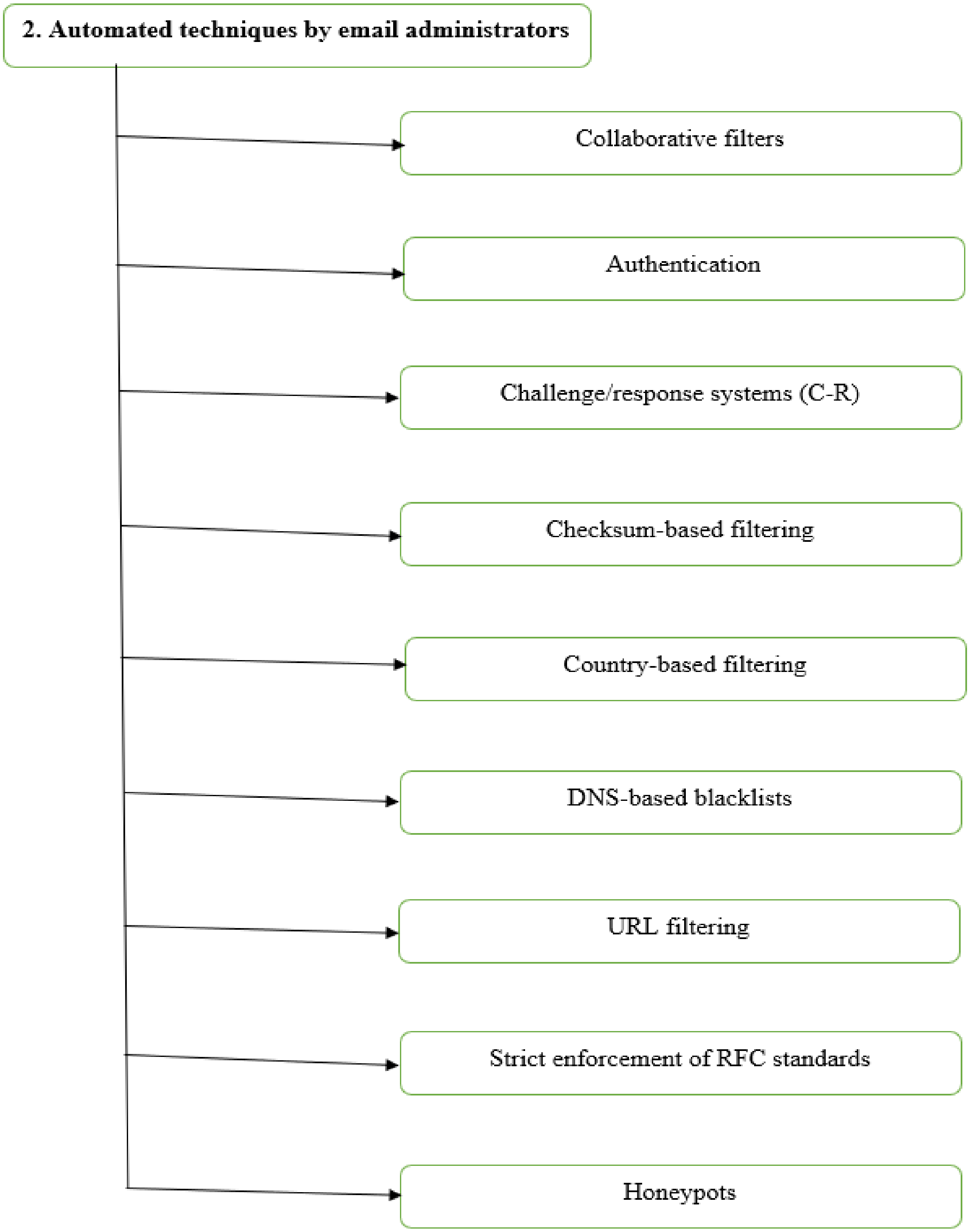


Table 9 (continued)

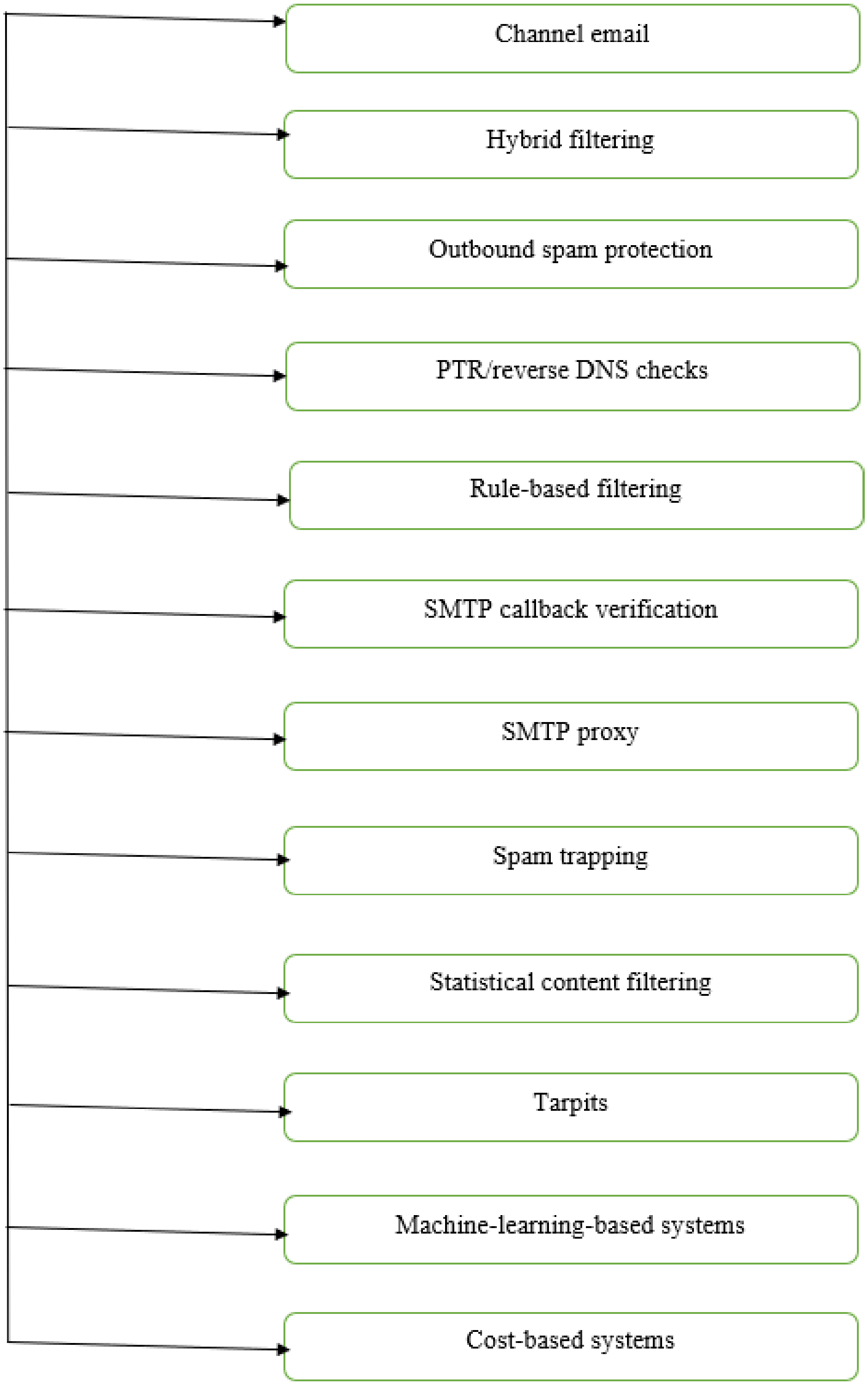


Table 10

Automated techniques by email senders (“Anti-Spam Techniques,” 2020)

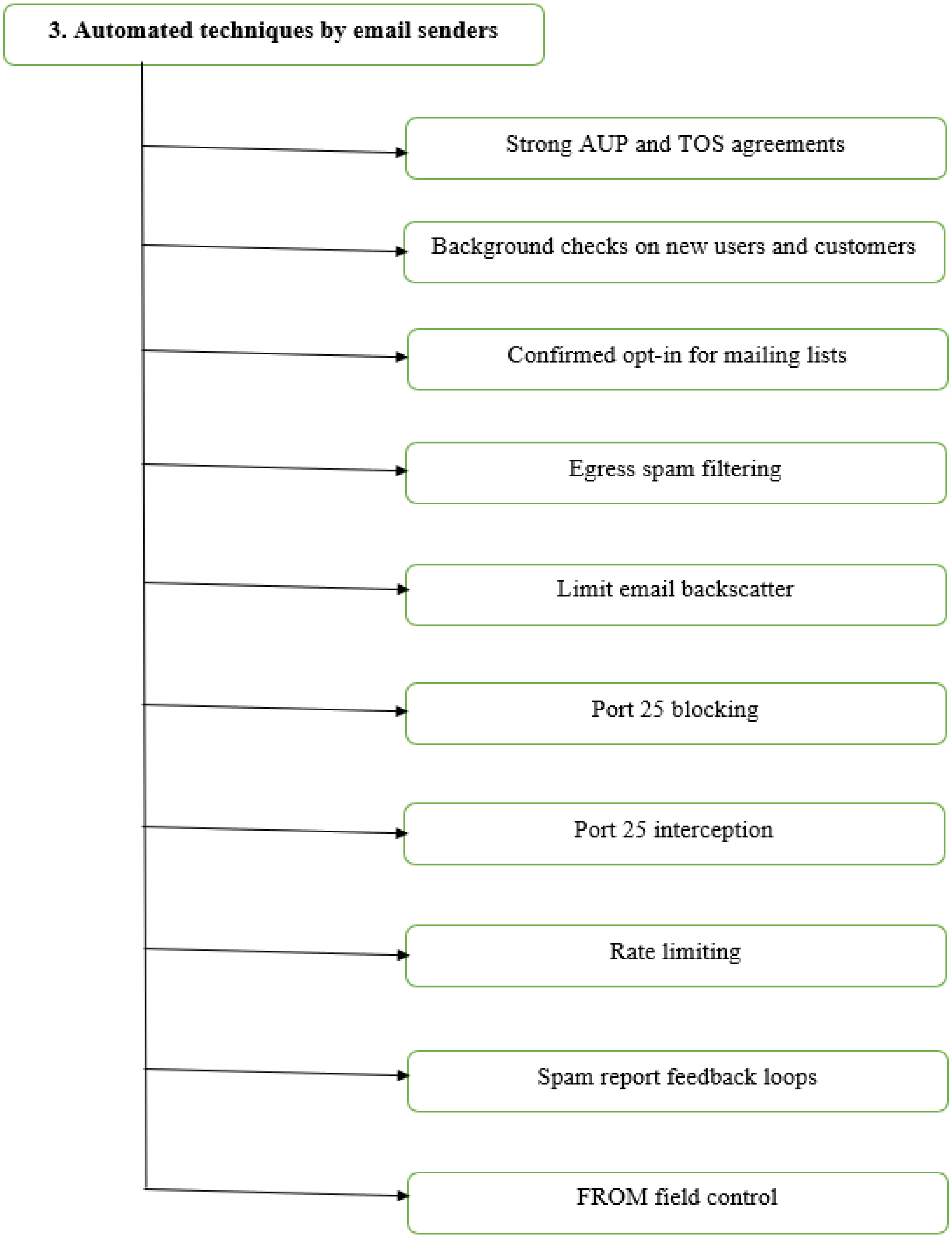
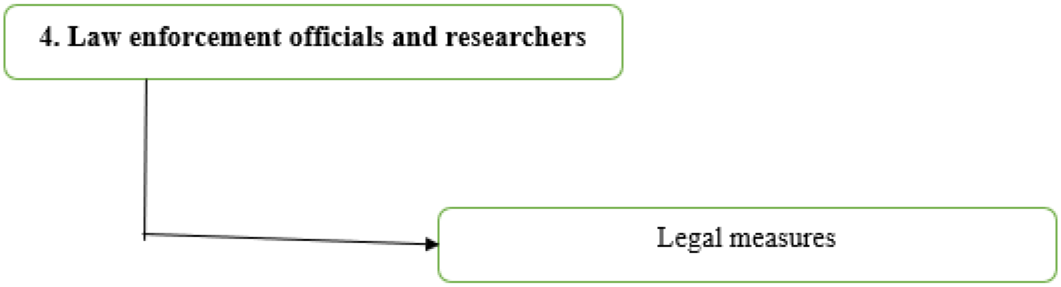

3. Automated techniques by email senders
Strong AUP and TOS agreements
Background checks on new users and customers
Confirmed opt-in for mailing lists
Egress spam filtering
Limit email backscatter
Port 25 blocking
Port 25 interception
Rate limiting
Spam report feedback loops
FROM field control

Table 11

Law enforcement officials and researchers ("Anti-Spam Techniques," 2020)



Summary

This chapter describes the approach of the study regarding email spam detection techniques. Also, it demonstrates how the process will be performed and what kind of resources are used. The overall timeline is also assessed for completing the study. The external resources and information from many other researchers will assist us in progressing this study. Most of the existing email spam detection techniques are considered for analyzing their approaches to filter spam email messages. The detection techniques are categorized in this chapter. There are a few downsides and advantages to the developed detection techniques.

Chapter IV: Data Analysis

Introduction

We have a taxonomy of e-mail spam detection techniques that would help us in proceeding with the evaluation. We will collect as much data as we can to improvise the taxonomy and make the necessary changes. There are standard email spam filtering methods provided by the clients to the users. Here we would also observe the awareness of users with regards to spam e-mail messages.

This study focuses mainly on the evaluation of the existing e-mail spam detection techniques based on the efficiency of the filtering process and its accuracy. Different aspects will be taken into consideration while evaluating the performance of the detection techniques. This evaluation would be helpful for all email users globally.

There are numerous spam detection techniques developed by many organizations. Spam email messages can be classified, filtered, and detected by these detection techniques. Along with the techniques, every email user should be responsible for preventing spam. The techniques are categorized based on the responsibilities of end-users, administrators, senders, and law enforcement officials. Not every technique is the right solution for preventing spam. Each technique has a few downsides along with advantages.

Process of filtering Spam Email

In general, the email message has two sections. One is the header, and the other is the body. The data regarding the content of an email message is displayed in the header section. It contains the sender address, receiver address, subject field, and timestamp. The user can view the path of an email message through the header section. The body is an essential part of an email message which doesn’t contain predetermined information. It might contain video, webpage, text, HTML, images, analog data, digital data, files, and audio (Dada et al., 2019).

Here, there are a few mandatory steps that need to be monitored when the data of an email message is validated.

They are pre-processing tokenization and feature selection.

1. Pre-processing:

    Once an incoming email message is received, this is the primary step that will be computed, and it comprises tokenization.

2. Tokenization:

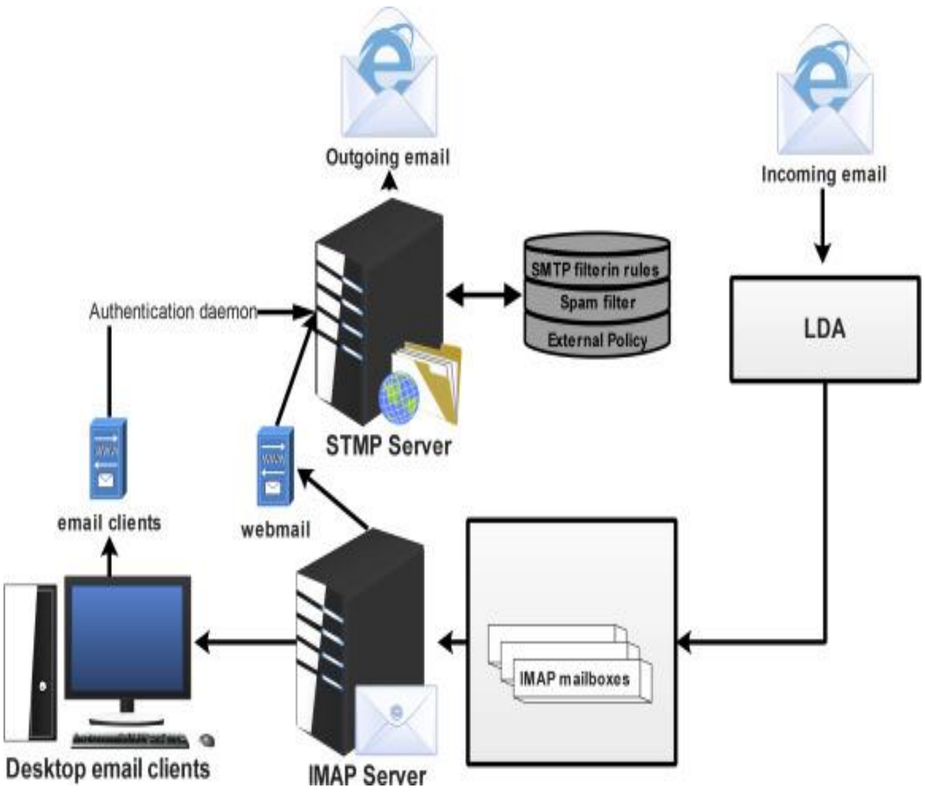
    In the body section of an email message, this pulls out the words or phrases and modifies the message in a meaningful way. This divides an email message into a pattern of indicative symbols known as tokens. Symbols are drawn out from the header, body, and subject of an email message. Replacing the data with the indicative symbols might extract all the words and features from an email but not the meaning (Dada et al., 2019).

3. Feature selection:

    The feature selection step is next to the pre-processing step. This is a sort of depletion in the size of a spatial presentation that successfully epitomizes interesting segments of an email message (which is a compressed feature vector). If the content of an email message is too large, and if the compressed feature is required to concise the image matching or compiling the text, then this technique is more useful (Dada et al., 2019).

Figure 10

Email server spam filtering architecture (Dada et al., 2019)



Data Analysis

We consider all the approaches the techniques for detecting spam email messages and analyze their process and disadvantages. Many researchers and organizations have provided their ideas and feedback about numerous spam detection techniques. Most of the techniques have some limitations when detecting spam email messages. Some of the techniques require proper training initially. The information collected from Articles, Journals, Research papers, Websites, IEEE papers, Google Scholar, and other online documents are the main sources for our study.

Necessary Actions Needed to be considered by End-User Techniques

With the intention of lowering the risks of receiving spam emails, there are various detection techniques that the users use to limit the accessibility of their email addresses, as mentioned in table 8.

- Discretion:

  Sharing and forwarding the email addresses within the bounded group of individuals is the simplest way of reducing the possibility that the addresses will be picked out by the spammers. Likewise, instead of using “cc:field”, the email addresses can be placed in “bcc:field” when sharing and forwarding an email message to a group of recipients who don’t have any connection with each other. By using “bcc:field”, the recipients cannot see the other recipients' email addresses in that group (“Anti-Spam Techniques,” 2020).

- Munging an email address

  In general, email addresses advertised on websites, and chatrooms are unprotected and vulnerable, which could lead to email address scraping. The act of concealing an email address to stop it from being accumulated automatically by the spammers is address munging. This address munging can block the computer software from spotting the original address, but a user can still read it to regenerate the real address. For example, an email address such as “some.one@xyz.com” becomes “some dot one at xyz dot com”. An email address advertised in public has a high chance of being accumulated automatically by computer software used by the spammers, whereas emails exchanged between the users privately are unlikely to be accumulated (“Anti-Spam Techniques,” 2020).

- Avoid responding to spam:

  Once you respond to spam, the spammers consider responses as the legitimate email address. If you consider an email message spam, do not open it. Try not to open any links and attachments associated with it. If you receive malicious content from a known user, then communicate with the sender of that email and let him know. Most spam emails have website links that the recipient is administered to follow, which are more dangerous. Sometimes, responding to the spam email messages results in failed deliveries, as the sender addresses are forged in many of the unsolicited bulk email messages. It might deliver to unknown users (Innocent users). So, it's better not to respond to spam ("Anti-Spam Techniques," 2020).

- Contact forms:

  In some situations, businesses and few correspondents avoid posting their email addresses and request contact through the contact form on the websites. This information is forwarded through email again. This way of contacting is troublesome for users as they don't use their email client, and deliveries are not notified. These contact forms cannot work without a relevant technology website, which is a disadvantage. Sometimes, the emails are sent to the email addresses provided by the individuals through these contact forms, which allows for sending unsolicited bulk emails ("Anti-Spam Techniques," 2020).

- Disable HTML in an email:

  In recent years, most email systems have been integrated with the software application functionalities like HTML displays, images, and URLs. If an individual or correspondent tries to read a spam email message, then staying away from or disabling

HTML will help from preventing a few issues but not a solution for avoiding spam. Some of the images are offensive, which are traced by the bugs on websites and being picked out by JavaScript (JS) depending upon the vulnerabilities of the securities in the HTML providers.

These email providers are composed to not dispose of HTML displays and provide no option for downloading attachments and images automatically, which could lower the chances of being victims by the spammers (“Anti-Spam Techniques,” 2020).

- Disposable email addresses:

In a few situations, without the assurance of the website holders that they are not using them for composing the spam emails, an email user needs to provide an email address to the websites. So, in these criteria, to lower the chances of risks, it’s better to give a disposable email address where the user can disable it after forwarding emails to an original account.

Many email clients come up with the disposable email address forwarding options, and these can be disabled after forwarding a maximum given several email messages, or after certain time intervals, or can be disabled manually. These can be used to trace the website holders by the email users to know if the email address is disclosed or not (“Anti-Spam Techniques,” 2020).

- Ham passwords:

Some of the services use “ham passwords” and request the unknown senders to add a password in their email that describes the email message as a “ham email message”. In general, ham passwords are inserted in the subject line of the message, and these ham passwords and email addresses are presented on the websites.

The email messages that are recognized as ham by the filtering techniques will be delivered to the recipients as these ham passwords are integrated with filtering techniques (“Anti-Spam Techniques,” 2020).

- Reporting spam:

  Reporting spam by tracing down the spammer’s credentials can block their services by aborting and is also reported as a criminal offense. Though it’s difficult, spammers can still be traced by the online tools available. But these tools are not accurately performed to trace.

  Once you report spam, the spammers switch their functioning to different URLs and IP (Internet Protocols) addresses. So, reporting spam with this approach hasn’t played a huge part in diminishing spam. Spammers in most countries send unsolicited and misleading emails to the officials who work under the agencies operated by the federal governments.

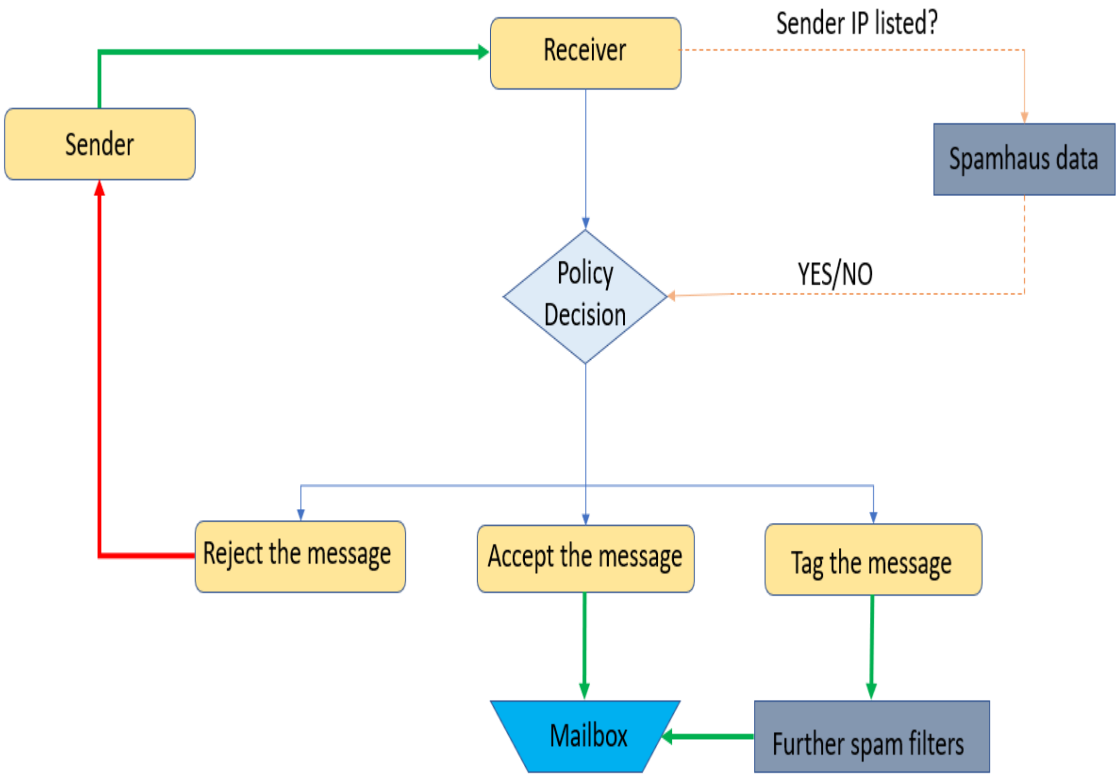
  All these are end-user techniques that are the necessary steps needed to be taken by the individuals to stay away from spam email messages. All the email users can prevent spam email messages by following these steps (“Anti-Spam Techniques,” 2020).

Automated Techniques by Email Administrators

To mitigate the spam in their inboxes, an email administrator can use the services of software applications, which are in huge numbers nowadays, as stated in table 9. Most spam email messages are blocked at the SMTP (Simple Mail Transfer Protocol) association stage, but if an email message gets an acceptance, then the data is examined further and is separated if it is classified as spam.

Figure 11

Controlling spam email messages (*Understanding DNSBL Filtering*, 1998)



Many software applications are evolved to recognize the email as authorized for the domain name holders. To list the authorized sites for sending an email, a domain name system (DNS) is used by most software applications. Also, many other email authentication protocols such as sender policy framework (SPF), domain keys identified mail (DKIM) and domain-based message authentication, reporting and conformance (DMARC) are broadly used with the developing technologies. With these software systems, it would be difficult for the spammers to spoof the email addresses, which is the simplest way. These systems cannot stop spam completely but make it harder for phishing and email frauds (“Anti-Spam Techniques,” 2020).

- Challenge/response systems (C-R):

  To deliver the email messages to the recipients by the unknown senders, there are numerous tests to be cleared. These procedures are used by email providers and many other internet service providers (ISPs) to reduce spam. This technique is titled “challenge/response systems” (“Anti-Spam Techniques,” 2020).

- Checksum-based filtering:

  These filters make use of the facts in the form of receiving bulk email messages that contain some unique differences. Also, checksum-based filters detect and diminish the differences between the email messages until what resides in a checksum and searching for that checksum in the database. The checksums of messages which are considered spam by the email recipients are accumulated in the database, such as Distributed Checksum Clearinghouse (DCC).

  Few email users have an option from their email providers to nominate the email as spam if it is one. So, if the checksum is found in the database after filtering an email, then the email message is most likely to be considered a spam. To avoid detecting spam with this technique, spammers usually include an identical hidden bug (called hash busters) in all the email messages they send to the recipients, which contains identical checksums (“Anti-Spam Techniques,” 2020).

- Country-based filtering:

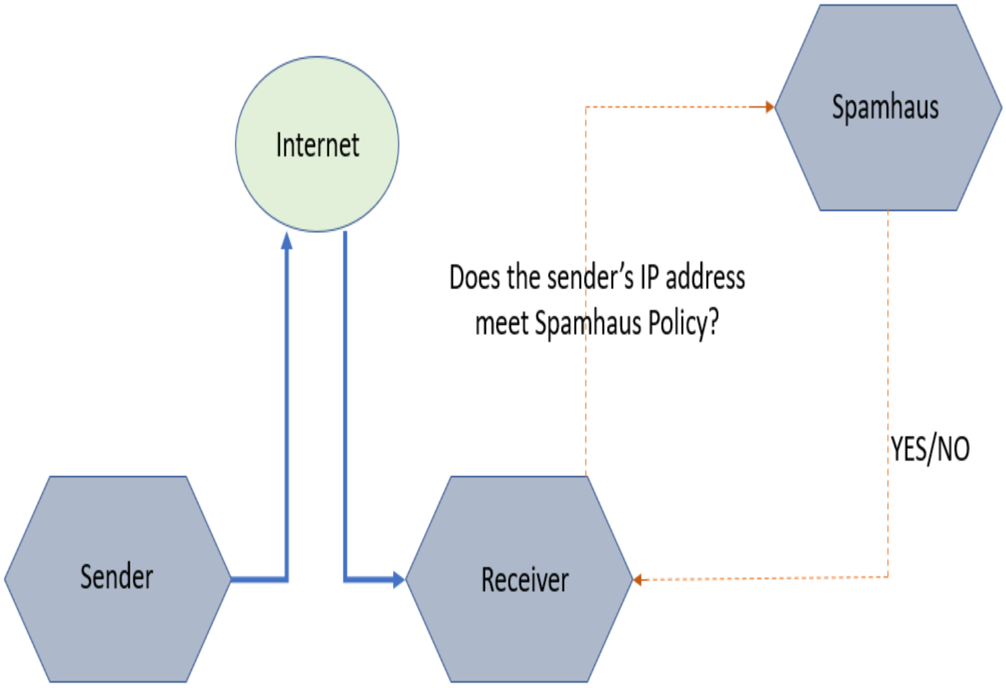
  Few countries block their email communication from specific countries (that send spam in large volumes) through their email servers. By using a country-based filtering technique, the emails can be blocked from the specified countries based on the sender’s IP address. So, there is a chance of blocking some genuine emails since it is filtered based on the origin of the country ("Anti-Spam Techniques," 2020).

- DNS-based blacklists:

Commercial and free DNS-based blacklists are available in huge numbers. This technique grants the mail servers to verify the IP address of the incoming email messages. If the IP address is listed, then the email message will be blocked. Here, administrators can select from the results of the DNS-based blacklists and Real-time Blackhole Lists (RBL), where there are various policies such as websites that avoid spam, open mail relays (proxies), and Internet Service Providers (ISPs) who encourage spam ("Anti-Spam Techniques," 2020).

Figure 12

Domain-Based Blacklists flow (*Understanding DNSBL Filtering*, 1998)



- URL filtering:

  Many phishing or spam email messages has URLs in them, where the victims are attracted to open them by clicking. This is the most known technique from the early 2000s. URL filtering technique extract URLs from the email messages and search them in the 'spamhaus' (tracing email spammers) Domain Block List (DBL) database and in URIBL (Uniform Resource Identifier Blackhole Lists), SURBL (Spam URI Real-time Block Lists) databases ("Anti-Spam Techniques," 2020).

- Strict enforcement of RFC (Request for Comments) standards:

  In general, most spammers use faulty software which are not able to follow the standards because they do not gain full access to the computer system which they are utilizing to send spam email messages. Email administrators can minimize spam remarkably by tightening the limits on the variance from RFC standards that are accepted by Mail Transfer Agent (MTA). This technique has a chance of blocking email messages from designated email servers ("Anti-Spam Techniques," 2020).

  a. Greeting delay:

     Before sending any email messages, the sending email server must wait until it receives the Simple Mail Transfer Protocol (SMTP) greeting banner. The receiving email servers can put a hold intentionally until it detects any spam and can reject the sending servers that do not wish to wait.

  b. Temporary rejection:

     The Simple Mail Transfer Protocol (SMTP) protocol permits the rejection of the incoming email message temporarily, and the greylisting technique is developed on this fact. The greylisting technique rejects the email messages temporarily that are sent from the non-recognized senders or email servers based on the standard syntax errors. All the Mail Transfer Agents (MTAs) will try to deliver the temporarily rejected email messages later. Here, the spammer's email messages will not be delivered. First-time senders come across few delays in delivering their email messages to the recipients, which is a disadvantage of this technique.

c. HELO/EHLO checking:

The Simple Mail Transfer Protocol (SMTP) server might validate the domain name in the EHLO (Extended HELO) command to match the IP address of the email providers. But if the validation fails, the SMTP server shouldn’t stop accepting the email messages based on this criterion. The software systems can be designed to

- Abort the association with the hosts that produce an incorrect HELO. For instance, HELO is an IP address that is not enclosed by the square braces or is not a fully qualified domain name (FQDN - absolute domain name).
- Abort the association with the hosts that provide fraudulent and deceitful HELO.
- Avoid accepting the email messages from the hosts who provide HELO arguments that do not sort out in Domain Name System (DNS).

d. Invalid pipelining:

Many Simple Mail Transfer Protocol (SMTP) commands are permitted to be positioned in a single network packet which are pipelined. For instance, once an email message is composed with a CC header in it, then the SMTP “RCPT TO (determines recipients of the email message)” commands are positioned in one network packet rather than positioned individually. At specific junctures, the SMTP protocol verifies the errors and organizes everything. The Mail Transfer Agents (MTAs) detect the invalid pipelining and abort the email messages that are composed with this approach. But most the spammers compose everything in one network packet as they do not worry about the errors, which is more effective.

e. Nolisting:

For any domain, the email servers are defined in an essentialized list through mail exchanger records. Here in this process, the nolisting technique adds a mail exchanger record that aims at the lowest preferred server as the foremost – (where the primary email contact will be failed to deliver). Once the email message is failed to deliver, the spammers will proceed with the following victims rather than retrying it to send. The legitimate and prioritized email servers should try again with the following higher-numbered mail exchanger record so that the legitimate email message will be delivered to the recipient with a short delay.

f. Quit detection:

Using the QUIT command, the SMTP connection needs to be closed. Once the spam is sent, most of the spammers do not tend to close the connection correctly as it is time taking. So, several MTAs can detect improperly closed connections and can evaluate how trustable the sender is.

- Honeypots:

This technique designs a replica of MTA or proxy TCP/IP servers that generate the impression of being an open proxy/mail relay. Spammers spot this kind of host after probing systems for proxies/open mail relays. They start trying to compose the email messages through them and eventually pass on the information regarding the origin of the spam that they are composing to the host that handles this honeypot technique. This approach blocks the email sending attempts by the spammers and hands them over to DNSBLs. Also, analyze the spammer's identification for blocking them by storing their information (“Anti-Spam Techniques,” 2020).

- Hybrid filtering:

  Most of the email providers use spamassassin, policyd-weight and many other different tests for scanning and detecting spam email messages. They allocate a numerical grade for each of the tests. Once an email message is tested with this criterion, the grades are computed, and if the grade exceeds a given value, then the email message is indicated as spam and will be rejected. With this technique, false positives are less likely to take place as no spam test can individually indicate the email message as spam (“Anti-Spam Techniques,” 2020).

- Outbound spam protection:

  Once an email message leaves that network, the outbound spam protection inspects the email traffic. Any recognized spam email messages are blocked, and the source of the spam email traffic is disconnected. Due to spam, the spam recipients are impacted primarily. So, composing networks will encounter financial losses as they waste the bandwidths. Also, the spam IP addresses can be blocked by the recipient networks. This technique can trace the spam sources and the system users can correct them by vanishing viruses from the infected machines on their networks (“Anti-Spam Techniques,” 2020).

- PTR/reverse DNS checks:

  Pointer (PTR) record is one of a Domain Name System (DNS) record. In reverse DNS, the PTR DNS records can be useful for numerous things, such as:

    - The Forward-Confirmed reverse DNS (FCrDNS) validation is used by the many email servers (Mail Transfer Agents) and the legitimate domain names are placed in the 'Received:' header field.
    - By using the domain names that are provided in the SMTP EHLO and HELO commands, a few email servers (Mail Transfer Agents) conduct Forward-Confirmed reverse DNS (FCrDNS) validations.
    - The domain names can be verified in the reverse DNS checks to know if these originated from the spam designated IP addresses. Most of the email messages that are composed of these computer systems is spam. Email messages having common reverse DNS names will not be accepted by most of the MTAs.
    - An authentication can be built by the FCrDNS validations between the relationships of the holder of the domain name and the holder of the network who has provided the IP address.
    - This authentication can also be utilized for whitelisting technique purposes as most of the spammers cannot get out of this validation even if they use the virus-affected computer systems for forging the domain names ("Anti-Spam Techniques," 2020).

- Rule-based filtering:

Rule-based filtering, also known as the content-based filtering technique, operates by using specific lists of words or by using phrases that are not accepted in the email messages. If the website encounters any spam advertising phrases, then the email directors/providers include those phrases in the filtering techniques. For instance, phrases like "selected winner", "herbal Viagra", and "awarded lotteries". The email messages having these spam phrases will be rejected by the email MTAs (servers). The heuristic filtering technique is one of the rule-based filtering techniques.

The header filtering technique considers the header of an email message that holds the data regarding the origin, content, and destination of the message. Spammers conceal their information by spoofing the fields in the header section and framing the email message to appear more legitimately. Most of the spoofing patterns are detected with this technique and breaching the header format can reject the email message (Bansal & Bhatia, 2017).

- SMTP callback verification:

  As most part of the spam is generated from the forged and incorrect sender email addresses, spam can also be detected by verifying and considering the sender email addresses as legitimate. By connecting SMTP to the mail exchanger, the sender address can be validated by the email MTAs (servers).

  The callback verification technique has disadvantages:

  - As most of the spam is generated from the forged sender addresses, so all callback verifications are performed to the faultless email servers which are not related to the spam.
  - Once a spammer sends an email message using the forged sender address, then if the receiving MTA performs a callback verification by using the forged sender address (MAIL FROM command), then the IP address of the receiving MTAs is blacklisted.
  - Some of the email providers enable VRFY, and EXPN commands to validate the email addresses that are benefited by the spammers and leave the SMTP

servers that are at the receiving end with no potential path to verify the sender's email addresses (“Anti-Spam Techniques,” 2020).

- SMTP proxy:

SMTP proxy will tackle the spam in actual time (real-time) by collaborating with the sender’s authorities, by giving feedback to the ham users in real-time, and by evicting a necessity for quarantine (“Anti-Spam Techniques,” 2020).

- Spamtrapping:

An email address is seeded where the common users cannot find it, but the spammers can find it. So, once the email address is composed, then the sender should be a spammer and will be blacklisted.

For instance, an email address “example@xyz.com” is positioned in the HTML source of a site where it is not shown on the page. So, common users cannot view it, but the spammers can find it as they use the scrapers to collect the email addresses from the source HTML. So, once the spammer uses this email address, the spamtrapping technique detects it (“Anti-Spam Techniques,” 2020).

- Statistical content filtering:

Statistical content filtering, also known as Bayesian spam filtering, can operate with no administrative continuity. This technique satisfies the end user’s requirements where the end users can tag the email messages as ham or spam, and the filtering method masters from these marked tags. The filtering software reacts to the changes immediately if the end-users tag the email messages. This technique verifies the headers and transport system along with the content of the email message.

Some of the statistical content filtering software are DSPAM (free software statistical spam filter), ASSP (Ant-spam SMTP Proxy), Bogofilter, SpamBayes, Mailwasher, Mozilla Thunderbird, CRM114 (Controllable Regex Mutilator) and SpamAssassin (“Anti-Spam Techniques,” 2020).

- Tarpits:

Tarpit is an email server software that deliberately reacts very slowly to the email provider's commands. Using tarpit, the legitimate email messages are accepted in a regular way but recognized spam emails or considered open mail relays are processed slowly. The website slows down its operation where the spammers have forcefully driven email messages into the email servers.

Tarpit slows down an attack based on the internet speed and the email servers. Most email systems disconnect once the servers react slowly, which is likely to reduce spam. To slow down the speed of the attack is the basic idea of this approach, where the culprits waste their time by failing remarkably. In the process, some of the ham email systems also fail to deal precisely with the significant delays.

Organizations can establish tarpit if it can determine the protocols, ports, and addresses for deceiving. This approach comprises a router where ham email traffic is sent to their respective servers while the others are passed to the tarpit. Honeyd, Labrea tarpits, IP-level tarpits and SMTP tarpits are some the examples of tarpits (“Anti-Spam Techniques,” 2020).

- Machine-learning based systems:

Many machine-learning-based techniques, also known as artificial intelligence systems, are utilized to detect and filter spam email messages. These techniques train their email networks with probability strategies. Validates the recurrence of words that are identified in the spam email messages with the incoming ham email messages.

Some of the machine-learning-based techniques are Bayesian filters, Support Vector Machines (SVM), Decision trees and artificial neural network algorithms ("Anti-Spam Techniques," 2020).

a. Bayesian filters:

This filtering technique is one of the modern types of machine-learning-based filtering. To vary the email messages between spam and ham, this technique utilizes the laws of numerical probability. Initially, by manually indicating each email message as ham or spam, this process must be trained by the end clients so that the Bayesian filtering technique can operate significantly to block the spam email messages. Thereafter, this filtering technique operates with the phrases that are identified in both ham and spam email messages by marking them to their respective lists.

This technique validates the content in the email message and then verifies the phrases in the marked lists to determine the probability of an email message being spam or ham. If the word "cheap" is popped out 20 times out of 25 spam email messages and five times out of 75 ham email messages, then an incoming email message having the word "cheap" in it is likely to be spam. This technique operates effectively when it is being used for a longer period as it can develop the word lists from the incoming email messages that are received by the recipients. This filtering technique must be trained initially, where the end email users must delete a few spam messages manually until the filter operates effectively (Satterfield, 2006).

b. Support Vector Machine (SVM):

Support Vector Machine (SVM) is a machine-learning-based system that operates efficiently in blocking spam email messages. This technique is a supervised learning model which can validate the content of an email message with suitable patterns and can classify it as spam or ham. This filtering technique should be trained at the beginning, where they use email corpus data. This is of a sparse data format, which gives high accuracy values. SVM is one of the proven successful classification techniques with its accuracy (Dada et al., 2019).

c. Decision trees:

This technique fully functions with the feature selection and variable analysis in the training where they use email corpus data. Here, the functioning of the technique doesn’t rely on the connections among parameters. A decision tree can provide proper solutions to the issues. It can open all the conceivable alternatives and directs each alternative to its end in a single frame where it can be assessed directly among the various branches of the tree. If there isn’t proper pruning, then it will be difficult to operate the tree growth, which is a disadvantage of this technique.

Some of the types of decision trees are Naïve Bayes Tree Classifier, C4.5/J48 Decision Tree Algorithm and (LMT) Logistic Model Tree Induction (Dada et al., 2019).

d. Clustering technique:

This technique is an unsupervised learning model that is applied to spam email datasets. Here, a bunch of patterns are classified into associated classes. This approach can classify the objects or case studies into relatively equivalent assortments known as clusters. Certain clustering algorithms can classify the spam email datasets into spam or ham clusters. This technique operates effectively when compared to a few semi-supervised techniques. Also, an intimidating technique for detecting and filtering spam email messages. The objects and case studies are classified in a way where the objects are equivalent to one another in the same group than to the objects that are in the other group.

Clustering techniques consist of two different types and they are K-nearest neighbors (kNN) clustering and density-based clustering. These two clustering techniques are used to classify the spam email messages and are exploited to solve the issues. Here, the density-based clustering technique is capable of operating encrypted email messages, consequently maintaining their confidentiality and can identify sensitive comparators. K-nearest neighbors (kNN) clustering technique doesn’t depend on the data assumptions made from the provided probability distribution as this is a distribution-free technique (Dada et al., 2019).

e. Neural networks:

This technique isn’t typically used for detecting spam email messages, as this can be anticipated easily. Neural networks are interrelated sets of simple processing components that convey each other with suitably weighted associations. Every component receives inputs from the adjacent components and from a few other sources, and the output is computed and conveyed to other adjacent components. Here, the channel is available to polish the associated weights. This technique has a formidable algorithm to classify spam email messages. In general, there are three types of processing components.

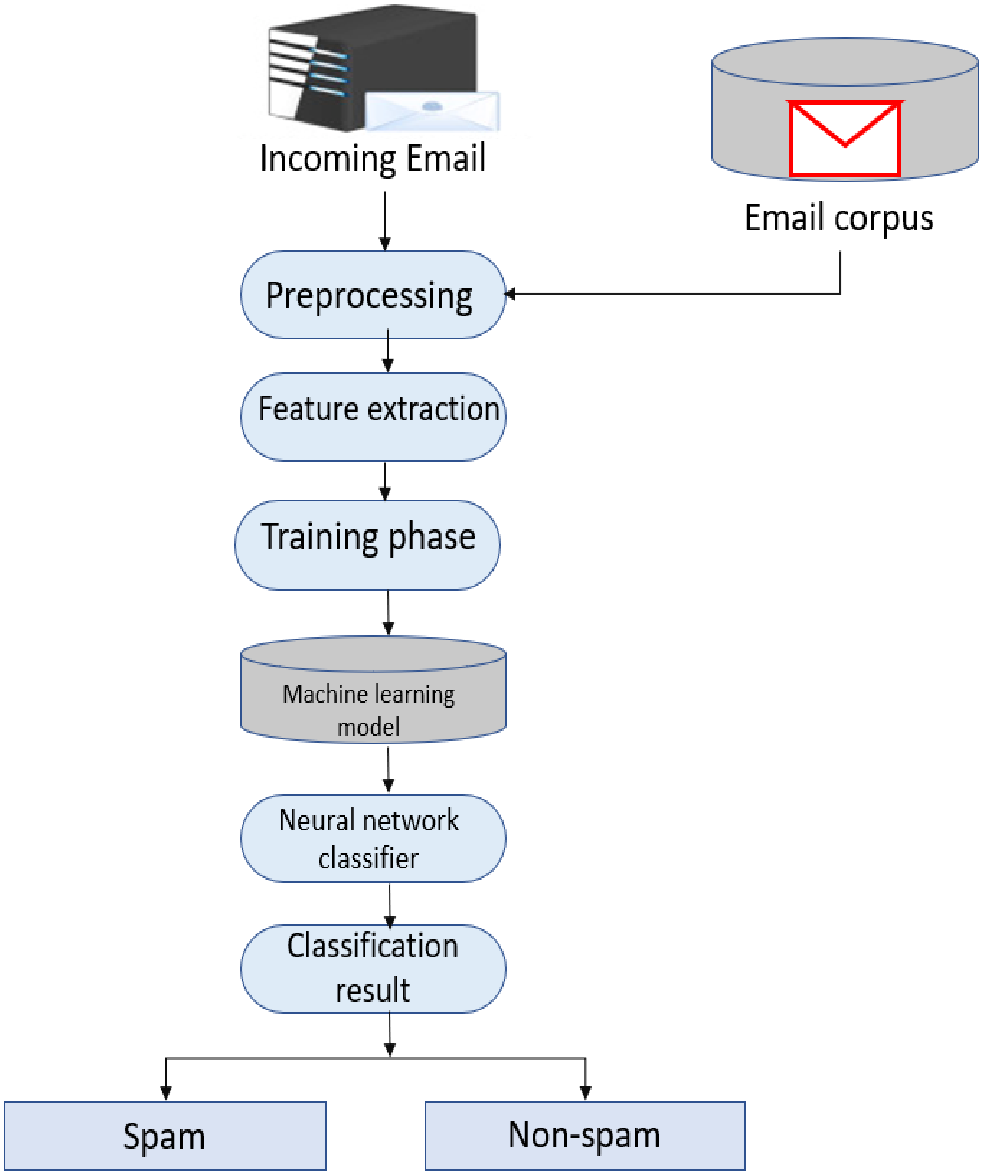
1. Input component: Receives data from external sources.
2. Output component: Convey's signal to the external sources (outside) of the network.
3. Hidden component: Receives and conveys the data inside the network.

Also, the neural network has two kinds of training

1. Supervised: In this network, a training dataset is provided with a group of inputs and their suitable output patterns.
2. Unsupervised: Here, the network should train by itself by generating a set of patterns as there is no training dataset provided (Dada et al., 2019).

Figure 13

The architecture of neural network spam email classifier (Dada et al., 2019)



- Cost-based systems:

Spamming is eased with the fact of composing email messages in large volumes. Since composing an email message is very inexpensive, some individuals suggested that the email senders need to pay some cost for composing an email message. So, composing bulk email messages will be very expensive for spammers. One of the known anti-spam lawyers (Daniel Balsam) brings in lawsuits against email spammers and is trying to make spam less beneficial (Dada et al., 2019).

- Channel email:

  This technique is the latest proposition for composing an email message which dispenses the anti-spam methods by injecting validation when an initial email message is composed of the new recipients. This technique possibly uses a 'bounce message' mechanism, where backscatter doesn't take place (Dada et al., 2019).

- Collaborative filters:

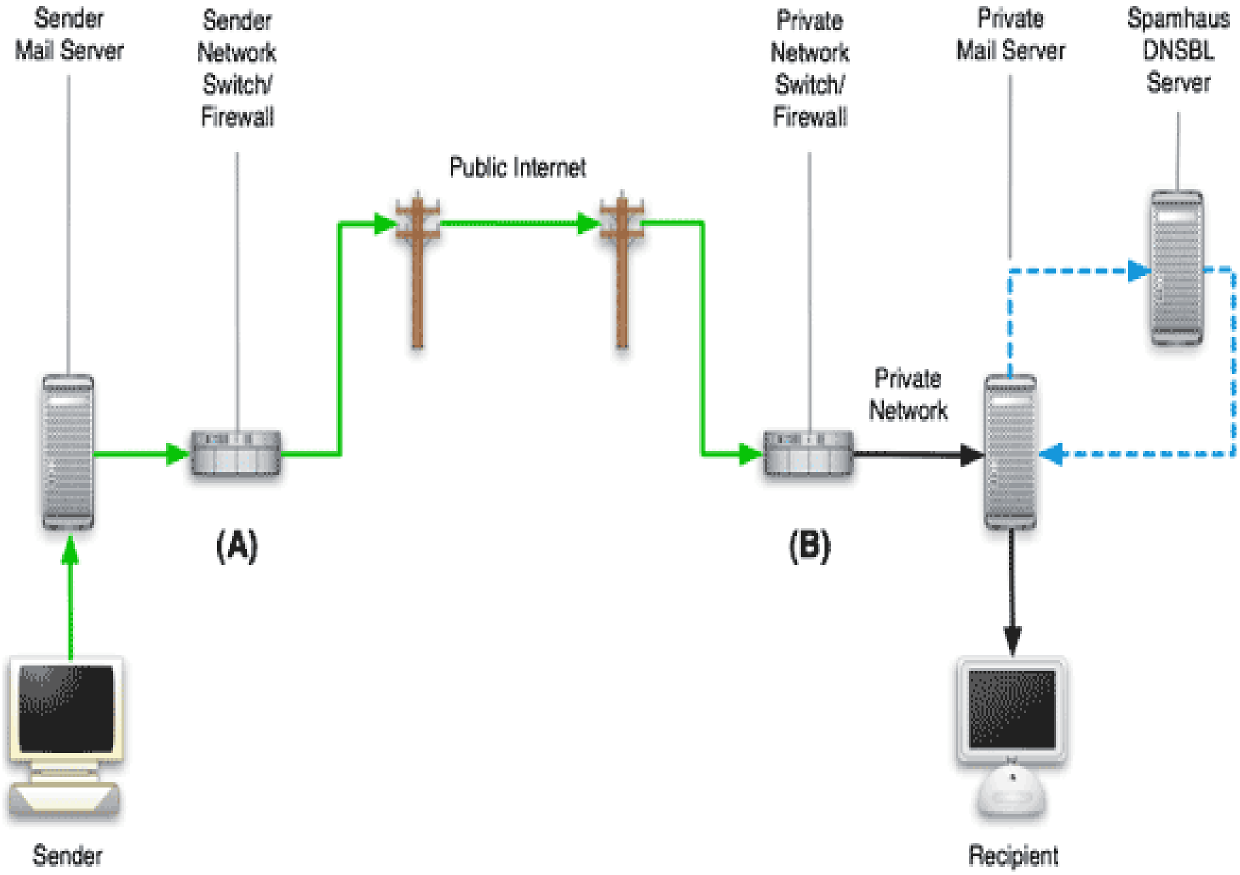
  This is a community-based filtering technique where the content is filtered based on the inputs collected from the end email users globally. Here, the users can indicate the incoming email message as spam or ham. Once the user marks the incoming email message, it will be reported to the database. If a specific email message is flagged as spam by certain users, then this filtering technique blocks that email message before it reaches other communities' inboxes. The disadvantage of this collaborative content filtering technique is any spammer can pretend as a ham email user of that community system where they can falsely mark the spam email messages as ham email messages (Satterfield, 2006).

Automated Techniques for Email Senders

Many of the techniques were used by the email senders in order not to compose any spam email messages, as described in table 10. Inability to handle the volume of spam composed that is considered by the recipients of an email message can even block the ham email messages. Also, the sender of an email message can be blacklisted.

Figure 14

Rights of a sender -Vs.- Rights of a receiver (*Understanding DNSBL Filtering*, 1998)



- Background checks on new users and customers:

Most of the spammer's email accounts are deactivated regularly as they breach the email policies. So, these spammers will be registering new accounts all the time. Once an ISP is considered as the source of spam, then the email clients implement CAPTCHAs to validate the new accounts, whether they are being registered by the individuals or by the automated spam bots. Before new customers register their accounts, the respective credit cards are validated by verifying the ‘spamhaus’ list and required background checks are performed (“Anti-Spam Techniques,” 2020).

- Confirmed opt-in for mailing lists:

  The spammers can try to subscribe to other email user addresses in the mailing catalog to annoy or can make the appearance of the user or organization to be spam. So, to avoid this kind of spam, many mailing catalogs encourage “confirmed opt-in” technique to be implemented by default. So, once an email address is submitted for subscription to the mailing catalog, this technique sends a notification to the submitted address. The confirmation notification sent by this technique has no spam content in it. If a recipient acknowledges the confirmation notification, then the submitted email address is added to the mailing catalog (“Anti-Spam Techniques,” 2020).

- Egress spam filtering:

  Recently, all the email providers are performing the same kind of spam detection validations on the incoming email messages that are composed by their customers and correspondents as for the incoming email messages that are composed by the other users. This process secures the reputation of the email provider as it can be damaged if a system is infected with spam viruses. This process is known as egress spam filtering (“Anti-Spam Techniques,” 2020).

- Limit email backscatter:

  Once the recipient email server primarily accepts the email message and later identifies it as spam, or it is composed to the unknown recipient, then it sends a bounce message to the original sender. The bounce message will be backscatter spam if the information of the sender on the composed email message is forged from the innocent user. Due to this, the rejection of the composed email messages takes place at the SMTP connection stage using error syntaxes where the sending email servers are still in connection. In this scenario, the issue will be reported to the original sender by the sending email servers (“Anti-Spam Techniques,” 2020).

- Port 25 blocking:

  The routers and firewalls can be designed in such a way that the acceptance of SMTP traffic (TCP port 25) can be stopped from the systems that are not required to compose any email messages or not required to run MTAs on the network servers. Based on the requests made by the users, if ISPs don’t turn off the blocking mechanism, then it can be problematic as these ISPs block the users.

  Still, from these systems, an email message can be composed to the configured recipients through TCP port 25, and the other recipients can receive it through email submission port 587 (“Anti-Spam Techniques,” 2020).

- Port 25 interception:

  To intercept Simple Mail Transfer Protocol (SMTP) traffic (TCP port 25), the NAT (Network Address Translation) is used and is administered to the email servers, which imposes egress spam filtering. This process can be the reason behind email privacy issues. If the usage of an email submission port 587 is not taking place, then the usage of SMTP-AUTH (SMTP Authentication) and STARTTLS (Start Transport Layer Security – Command given between the server and email program) will be impossible to happen (“Anti-Spam Techniques,” 2020).

- Rate limiting:

  Suddenly, a few computer systems started composing email messages in large volumes, which are known as virus-affected computers. Limiting the rate of the email messages that can be composed by considering what is required in general for the computer systems can slow down the large volumes of spam before performing the manual inspection. Still, the ham email messages can be composed ("Anti-Spam Techniques," 2020).

- Spam report feedback loops:

  ISPs (Internet Service Providers) can obtain knowledge of the spam issues by observing the reports of the spam before the spammers destroy their reputation and make their email servers to be blacklisted. These reports can be monitored from spamcop (spam email reporting service), network abuse clearinghouse (American web portal), AOL's feedback loop, domain abuse at the mailbox and so on ("Anti-Spam Techniques," 2020).

- FROM field control:

  Most of the spammers compose spam email messages using forged FROM email addresses. To ensure that the senders are using their original FROM email address in an outgoing email message, the controls are implemented on the SMTP email servers. In a database that is subjected to email clients, every individual has a record with one email address. Here, the SMTP email server verifies the FROM email address of an outgoing email message with the user's belonging email address that is provided for the SMTP authentication purposes. If the SMTP email server detects the FROM email address of an outgoing email message as a forged email address, then it will send an error notification to that email user ("Anti-Spam Techniques," 2020).

- Strong AUP and TOS agreements:

  Almost all the email providers and ISPs (Internet Service Providers) own either a TOS (Terms of Service) or an AUP (Acceptable Use Policy) agreement. This could deflate the spammers from utilizing their computer systems. For violating the terms and conditions, the spammers are terminated from the services ("Anti-Spam Techniques," 2020).

Law Enforcement Officials and Researchers

- Legal measures:

  Most countries implemented certain legislations to outlaw spam. Suitable legislations and their implementations can impact spamming remarkably. Here, certain words or text is provided by the legislation to the email senders to include them in their email messages where the bulk ham email messages can be identified easily.

  Progressively, these spam detection techniques have prompted the association between the researchers, analysts, law enforcement officials, ISPs (Internet Service Providers) and many other financial service organizations in the form of tracing spam emails, monitoring spam, phishing, and identity theft and collecting evidence for the issues occurred. If the analysis of a website is considered a source of spam, then they can follow up with their domain registrars by showing good outcomes ("Anti-Spam Techniques," 2020).

Summary

Here, in this chapter, we analyzed most of the existing email spam detection techniques. All the detection techniques aren't the right solution to solving the spam issues. Each technique needs to develop its filtering process as there are a few downsides. The issues related to spam are increasing as these techniques aren't accurate in detecting spam email messages. Initially, some of these techniques require manual training as there is a scope for false positives (rejecting ham email messages) and false negatives (not rejecting spam email messages). Spammers are pretending to be ham email users and misusing these email spam detection techniques for their benefits, which is destroying the trust in email usage. Also, this is denting the accuracy of detection techniques. Almost all the techniques with their approaches to filtering spam email messages are described. The accuracy of the techniques is decreasing as the spammers come up with alternatives. Since all the email messages do not contain predetermined values or pre-defined data, it's everyday learning for all the existing email spam detection techniques.

Study Questions/Hypotheses

There are some study questions mentioned in chapter 1, which would help in the development of data analysis. As stated earlier, all the mentioned E-mail spam detection techniques are the key sources in our study. The listed study questions/hypotheses will be analyzed and evaluated accordingly.

1. What are the existing e-mail spam detection techniques developed?
    a. There are various detection techniques listed
        - Based on reputation
        - Based on word (Textual) content
        - Based on multimedia content
        - Based on the responsibilities of email users, administrators, senders, and law enforcement officials

    b. The analysis is evaluated based on how far these techniques are detecting e-mail spam messages.
2. How severe is the problem of e-mail spam?

    Globally, most e-mail users would face e-mail spamming problems. The severity of the problem is huge. Due to spam, the belief in the email users in the electronic environment is decreasing. The increasing volume of spam makes email users less likely to use the email services. A national survey indicates that spam is degrading the integrity of an email and online experiences. The following are the key stats from the national survey (Fallows, 2003):

- 25% of the email users lowered their email usage due to the increased volume of spam, and 60% of these users say the impact is huge.
- The trust in an email has been reduced due to spam in 52% of email users.
- Due to spam, 70% of email users experienced annoying being online.
- The incoming email can be blocked by filtering techniques, which is a worrying sign in 30% of email users.
- Due to filtering techniques, 23% of the email users are worried as their emails to others might be blocked.
- Over 75% of email users are worried about the flow of spam, which can't be stopped.
- 80% of the email users are worried about misleading and fraudulent spam content.
- 76% of the email users are worried by disrespectful and vulgar spam content.

3. How accurately are the existing e-mail spam detection techniques working?

Presently, spam emails are being increased depending on various criteria such as stock advice, advertisements, marketing, chain letter and so on. Using different algorithms and concepts, there are various filtering techniques developed to restrict spam emails. According to the national survey, the impacted percentage of the email users is high, which suggests that the existing e-mail spam detection techniques aren't accurate (Fallows, 2003).

4. Is the problem resolved?

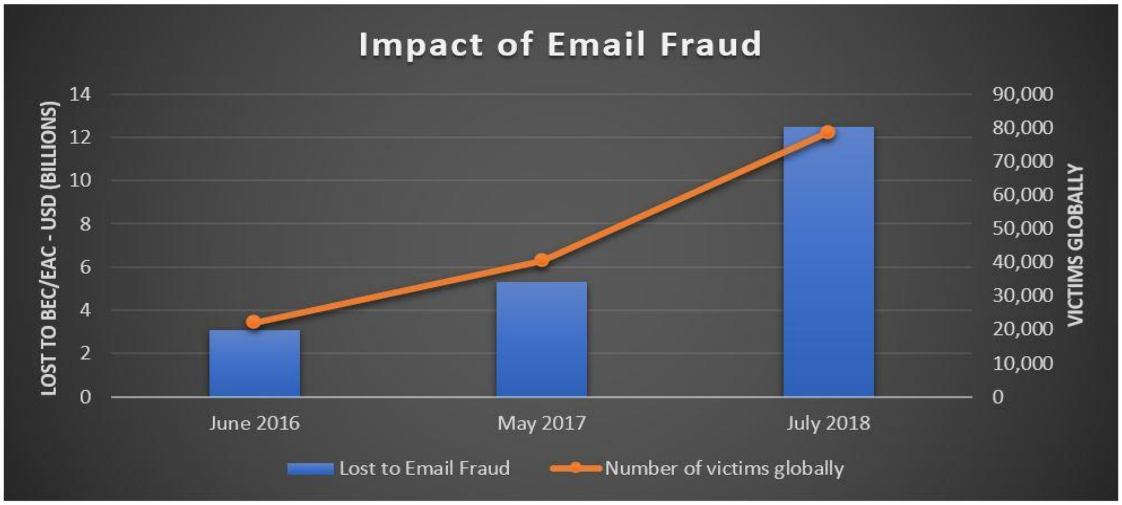
As of now, the national survey suggests that a lot of email users are facing problems due to spam. Though there are various filtering and detection techniques developed, there is still a lot of improvement required to resolve the problem completely (Fallows, 2003).

5. Is it getting better or worse?

Since spam is a persistent issue, the problem is getting worse. Here are a few statistics which could describe the impact of spam emails.

Figure 15

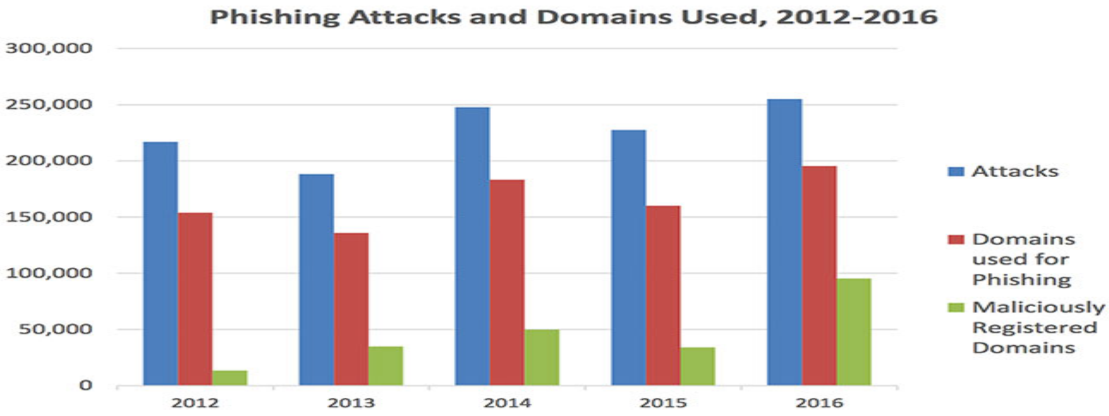
Impact of fraud emails (Guntrip, 2018)



The impact of fraud emails is increasing year by year, which suggests that the problem is getting worse.

Figure 16

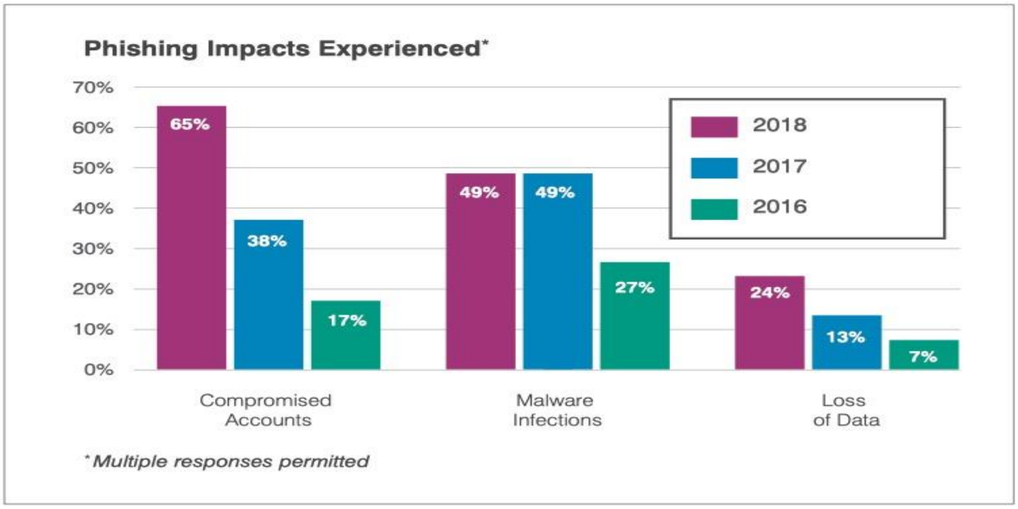
Phishing Attacks and Domains Used, 2012 – 2016 (Aaron & Rasmussen, 2017)



Phishing attacks and maliciously registered domains are increasing overall, which affects the trust of email users. In 2016, the attacks, domains used for phishing and maliciously registered domains were in high volume when compared to 2012. This could describe that the spam email problem is getting worse. (Aaron & Rasmussen, 2017)

Figure 17

Phishing impacts Experienced (*Phishing | Revealing the Most Vulnerable Targets*, 2019)



Due to the impact of phishing, there is a high number of compromised accounts in 2018. The loss of data (information) and malware infections have been increasing year by year.

6. Are the current techniques able to address the problem?

   Most of the current detection techniques are able to address the problem, but not accurately. There are false positives that need to be addressed, and some of the algorithms are not accurately detecting spam E-mail messages.

Chapter V: Recommendations, Conclusion, and Future Work

Introduction

In this chapter, we emphasize more on the general considerations and remarks made based on the previously described chapters regarding existing email spam detection techniques. Many email spam detection techniques with their processes are discussed, and their approaches to detecting spam email messages are analyzed. Since spammers are coming up with various alternatives, there is a scope to learn and develop all the existing email spam detection techniques. These techniques can be improvised according to the challenges they face while detecting. Here, in this chapter, we discuss the recommendations, future work and conclusion of the study. Most spam detection techniques have a few limitations along with strengths. Thus, the existing email spam detection techniques are studied and analyzed in our research. Though few spam detection techniques have a high success rate in detecting, they aren't 100% accurate in solving the spam issues. Since these techniques are not 100% accurate in detecting spam email messages, there is a scope for spammers to compose unsolicited bulk emails.

Recommendations

The recommendations need to be described to overcome the limitations and downsides of email spam detection techniques. Spam is a never-ending issue as spammers come up with a variety of scams to exploit, and no detection technique has a proper solution to prevent it. All the email users need to be more responsible from their end by creating ham passwords, using disposable email addresses whenever required, reporting spam, and not responding to spam email messages. All the email spam detection techniques need to be improvised and develop their mechanisms according to the challenges they encounter while detecting. Highly recommended to use unique and multi-layer spam filtering techniques. All the email providers should follow the standards and policies. Any user violating the email rules should be terminated. The email user should report all the false positives (rejecting ham email messages) and false negatives (not rejecting spam email messages) to their email providers. The current email spam detection techniques need to be advanced in terms of technology. If a detection technique is well developed in advance, then its accuracy in detecting spam email messages would also be high. Maintaining the anti-spam techniques up to date is also important for its performance. There is a scope to work more on the downsides of the techniques where it can improve the accuracy in detecting spam email messages. Any email spam detection technique has its own strengths in detecting and is useful for all organizations and individuals in keeping away from spam.

Conclusion

A huge number of email spam detection techniques were developed and are available. Some spam detection techniques are being developed. None of the filtering techniques have the right solutions as each of them has a few downsides where the spammers can be benefited. One of the possible ways to prevent spam is to use unique and multi-layer filtering. Most spammers modify the email messages where they can be escaped from detection by one sort of filtering technique, but it’s difficult to evade multi-layer filtering techniques. In this study, we discussed the strengths and downsides of a few email spam detection techniques. Additionally, some techniques are obsolete because spammers have fully exploited them. These email spam detection techniques have been categorized according to the responsibilities of users, administrators, senders, and law enforcement officials. All individuals have a role in preventing spam. There are a few recommendations mentioned in this chapter. The process of spam filtering methods is explained. The problem is getting worse as the impact of spam is huge, and many of the domains are being registered maliciously. We can monitor the loss of data, malware-infected systems, and many compromised email accounts due to spam. Here, organizations and individuals should always be more responsible for their ends and try to use multi-layer filtering techniques to detect spam email messages more accurately.

Future Work

The possibility of learning and improvising detection algorithms never goes away. New methods can be developed to reduce spam. There should be an emphasis on whether each technique differentiates itself from the others in terms of detecting and filtering spam. In moving from obscure techniques to image spam, spammers are expanding the features they use to circulate their spam across the networks. Spam is of a very effective texture, and spammers' reactivity in response is leading to more studies on existing email spam detection techniques. Spam is a never-ending problem which poses several intriguing challenges to spam detection techniques. There is a need to control drift in the ideas as they change in unexpected ways over a period and are difficult to predict. The rest of them involve dealing with false positives, identifying emerging spam threats, and prioritizing email messages. Spam classification in real-time is a vital feature to be implemented because most existing spam classification systems are not capable of handling real-time data. Using ensemble learning, spam detection systems could be made more accurate and reliable by increasing their security. To establish the correctness and discover ideal parameters for the operation, both feature detectors and classifiers need to be validated and tuned. There's a need to implement an integrated mail filtering system and perform an evaluation of the overall system. It is necessary to develop a spam filtering system that can handle a vast amount of multimedia data by providing enhanced spam email filtering techniques.

References

A history of email spam. (2020). Think Automation. Retrieved February 8, 2021, from https://www.thinkautomation.com/histories/the-history-of-email-spam/

Aaron, G., & Rasmussen, R. (2017, June 28). *Criminalization of DNS for phishing continues to advance*. Help Net Security. Retrieved February 15, 2021, from https://www.helpnetsecurity.com/2017/06/28/criminalization-dns-phishing/

Almeida, T. A., & Yamakami, A. (2010). *Content-Based Spam Filtering*. Citeseerx. Retrieved January 27, 2021, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.390.3432&rep=rep1&type=pdf

Almeida, T. A., & Yamakami, A. (2012, January). *Advances in spam filtering techniques*. Research Gate. Retrieved December 12, 2020, from https://www.researchgate.net/publication/267067074_Advances_in_Spam_Filtering_Techniques

Androutsopoulos, I., & Paliouras, G. (2006, October). *Learning to Filter Unsolicited Commercial E-Mail*. Semantic Scholar. Retrieved February 3, 2021, from https://pdfs.semanticscholar.org/fbff/6e316722053f5233f4c7869cc18e705af2e3.pdf

Anti-spam techniques. (2020, October 24). In *Wikipedia*. https://en.wikipedia.org/wiki/Anti-spam_techniques

Bansal, E., & Bhatia, P. K. (2017, March). *A survey of various machine learning algorithms on email spamming*. IRAJ. Retrieved January 15, 2021, from http://www.iraj.in/journal/journal_file/journal_pdf/12-351-149622523082-87.pdf

Bauer, E. (2018, February 1). *15 outrageous email spam statistics that still ring true in 2018*. Propeller. Retrieved April 12, 2021, from https://www.propellercrm.com/blog/email-spam-statistics

Bayati, M. A., & Jabbar, S. F. (2015, August). *Developing a spam email detector*. ResearchGate. Retrieved January 9, 2021, from https://www.researchgate.net/publication/326177337_Developing_a_spam_Email_Detector

Bhowmick, A., & Hazarika, S. M. (2016, June 3). *E-mail spam filtering: A review of techniques and trends*. ResearchGate. Retrieved December 17, 2020, from https://www.researchgate.net/publication/320703241_E-Mail_Spam_Filtering_A_Review_of_Techniques_and_Trends

Bhuiyan, H., & Ashiquzzaman, A. (2018, January). *A survey of existing e-mail spam filtering methods considering machine learning techniques*. Research Gate. Retrieved February 21, 2021, from https://www.researchgate.net/publication/332865507_A_Survey_of_Existing_E-Mail_Spam_Filtering_Methods_Considering_Machine_Learning_Techniques

Blanzieri, E., & Bryl, A. (2008, March 1). *A survey of learning-based techniques of email spam filtering*. ACM Digital Library. Retrieved February 1, 2021, from https://dl.acm.org/doi/10.1007/s10462-009-9109-6

Carpinter, J., & Hunt, R. (2006). *Tightening the net: A review of current and next generation spam filtering tools*. Apricot. Retrieved March 25, 2021, from https://www.apricot.net/apricot2006/slides/conf/wednesday/spam-DOC_Hunt.pdf

Caruana, G., & Li, M. (2008, March 5). *A survey of emerging approaches to spam filtering*. ACM Digital Library. Retrieved March 7, 2021, from https://dl.acm.org/doi/10.1145/2089125.2089129

Common types of email spam. (2019, October 1). Gatefy. Retrieved January 13, 2021, from https://gatefy.com/posts/7-most-common-types-email-spam/

Cormack, G. V. (2008, April 1). *Email spam filtering: A systematic review*. ACM Digital Library. Retrieved January 21, 2021, from https://dl.acm.org/doi/10.1561/1500000006

Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., & Adetunmbi, A. O. (2019, June 11). *Heliyon*. Machine learning for email spam filtering: review, approaches and open research problems. Retrieved February 12, 2021, from https://www.cell.com/heliyon/fulltext/S2405-8440(18)35340-4?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2405844018353404%3Fshowall%3Dtrue

Delany, S. J., & Bridge, D. (2006, January 1). *Feature based and feature free textual CBR: a comparison in spam filtering*. Citeseerx. Retrieved December 14, 2020, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.359.4722&rep=rep1&type=pdf

Diao, Y., Lu, H., & Wu, D. (2003, March 24). *A comparative study of classification based personal e-mail filtering*. SpringerLink. Retrieved February 6, 2021, from https://link.springer.com/chapter/10.1007/3-540-45571-X_48

E-mail. (2021, November 6). Computer Hope. Retrieved December 19, 2021, from https://www.computerhope.com/jargon/e/email.htm

Fallows, D. (2003, October 22). *Spam: How it is hurting email and degrading life on the internet*. Pew Research Center: Internet, Science & Tech. Retrieved February 11, 2021, from https://www.pewresearch.org/internet/2003/10/22/spam-how-it-is-hurting-email-and-degrading-life-on-the-internet/

Fruhlinger, J. (2020, April 7). *Phishing*. CSO. Retrieved November 11, 2020, from https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Greve, G. (2019, June 7). *Security, spam and the future of email*. Security Boulevard. Retrieved October 17, 2020, from https://securityboulevard.com/2019/06/security-spam-and-the-future-of-email/

Gudkova, D., & Vergelis, M. (2017, February 20). *Spam and phishing in 2016*. Kaspersky. Retrieved September 26, 2020, from https://securelist.com/kaspersky-security-bulletin-spam-and-phishing-in-2016/77483/

Guntrip, M. (2018, July 18). *FBI reports $12.5 billion in global financial losses due to business email compromise and email account compromise*. Proofpoint. Retrieved October 12, 2020, from https://www.proofpoint.com/us/corporate-blog/post/fbi-reports-125-billion-global-financial-losses-due-business-email-compromise

Guzella, T. S., & Caminhas, W. M. (2009, February 20). *A review of machine learning approaches to spam filtering*. ScienceDirect. Retrieved November 17, 2020, from https://www.sciencedirect.com/science/article/abs/pii/S095741740900181X?via%3Dihub

Hoffman, C. (2016, September 22). *Why is email spam still a problem*? How-To Geek. Retrieved December 15, 2020, from https://www.howtogeek.com/180604/htg-explains-why-is-spam-still-a-problem/

Jameel, N. G. M., & Mohammed, E. Z. (2017, June). *An online content-based email attachments retrieval system*. ResearchGate. Retrieved December 21, 2020, from https://www.researchgate.net/publication/319182999_An_Online_Content_Based_Email_Attachments_Retrieval_System#pf2

Jamkatel, N., & Gupta, R. (2018, January 25). *Spam email identification*. PowerPoint Courses by LinkedIn Learning. Retrieved November 26, 2020, from https://www.slideshare.net/nabinsjamkatel/spam-email-identification

Kanaris, I., & Kanaris, K. (2006). *Words Vs. Character n-grams for anti-spam filtering*. Mafiadoc. Retrieved October 14, 2020, from https://mafiadoc.com/words-vs-character-n-grams-for-anti-spam-filtering-1-_598d41e31723ddcc692f0614.html

Kumar, N. (2019, January 9). *Naive Bayes: Text classifier for spam detection.* Medium. Retrieved January 7, 2021, from https://medium.com/@naveeen.kumar.k/naive-bayes-spam-detection-7d087cc96d9d

Lackey, K. (2017, July 12). *Do I need an email spam filtering service?* Beacon IT Services (bITs). Retrieved January 21, 2021, from https://www.beaconitservices.com/blog/2017/07/do-i-need-an-email-spam-filtering-service/

Lessard, T. (2013, July 31). *5 ways to stop spam email today*. Online Privacy | Abine. Retrieved February 4, 2021, from https://www.abine.com/blog/2013/stop-spam-email-today/

M´Endez, J. R., & Fdez-Riverola, F. (2006). *A comparative performance study of feature selection methods for the anti-spam filtering Domain.* Springer Link. Retrieved March 17, 2021, from https://link.springer.com/chapter/10.1007/11790853_9

Phishing | Revealing the most vulnerable targets. (2019, June 27). SentinelOne. Retrieved December 11, 2020, from https://www.sentinelone.com/blog/phishing-revealing-vulnerable-targets/

Pitkar, T. (2020, January 16). *Evolution of Gmail spam filters | An email deliverability perspective*. Pepipost. Retrieved January 29, 2021, from https://pepipost.com/blog/gmail-spam-filters-evolution/

Rao, J. M., & Reiley, D. H. (2012). The economics of spam. *Journal of Economic Perspectives*, 89–90.

Saleh, A. J., & Karim, A. (2019, June 12). *An intelligent spam detection model based on artificial immune system*. MDPI. Retrieved December 24, 2020, from https://www.mdpi.com/2078-2489/10/6/209/htm

Satterfield, B. (2006, November 30). *Ten Spam-Filtering methods explained*. Techsoup Canada. Retrieved November 28, 2020, from https://www.techsoupcanada.ca/en/learning_center/10_sfm_explained

Sharma, M., & Sharma, P. S. (2018). *A survey of email spam filtering methods*. IISTE. Retrieved February 24, 2021, from https://iiste.org/Journals/index.php/CTI/article/download/43672/45005

Sorkin, D. E. (2020, April). *Spam statistics and facts*. Spam Laws. Retrieved January 16, 2021, from https://www.spamlaws.com/spam-stats.html

Spector, L. (2016, June 7). *Ways to stop spam from invading your email*. PCWorld. Retrieved August 10, 2020, from https://www.pcworld.com/article/3072435/5-ways-to-stop-spam-from-invading-your-email.html

Tretyakov, K. (2004, May 3). *Machine learning techniques in spam filtering*. Quretec. Retrieved July 19, 2020, from http://www.quretec.com/u/vilo/edu/2003-04/Problem_2004k/Final/P06/P06.pdf

Understanding DNSBL filtering. (1998). Spamhaus. Retrieved December 17, 2020, from https://www.spamhaus.org/whitepapers/dnsbl_function/

Varnsen, K. (2020, April 1). *Types of spam e-mails*. Ranker. Retrieved August 7, 2020, from https://www.ranker.com/list/types-of-spam-e-mails/kel-varnsen

Vijayasekaran, G., & Rosi, S. (2018, April). *Spam and email detection in big data platform using naives bayesian classifier*. IJCSMC. Retrieved August 6, 2020, from https://ijcsmc.com/docs/papers/April2018/V7I4201813.pdf

Wang, D., & Irani, D. (2013, November 12). *A study on evolution of email spam over fifteen years*. European Union Digital Library (EUDL). Retrieved September 19, 2020, from https://eudl.eu/doi/10.4108/icst.collaboratecom.2013.254082

Yeh, C.-Y., & Wu, C.-H. (2005, October 12). *Effective spam classification based on meta-heuristics*. IEEE Xplore. Retrieved October 17, 2020, from https://ieeexplore.ieee.org/abstract/document/1571750/authors#authors

Zhang, L., & Zhu, J. (2004, December). *An evaluation of statistical spam filtering techniques*. ACM Digital Library. Retrieved July 8, 2020, from https://dl.acm.org/doi/10.1145/1039621.1039625