JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IMPROVING EMAIL-BASED THREAT DETECTION AND MITIGATION THROUGH EMAIL HEADER ANALYSIS

[1]Deepak Prasad, [1]Meera Parmar, [1]Aastha Patel, [1]Abhi Patel, [2]Nidhi Patel, [3]Milind Purswani
[1,2]Computer Science and Engineering, Parul University Vadodara, India
[1]Student, [2]Assistant Professor
[3]Security Engineer, Amazon San Jose, USA.

ABSTRACT: Email communication has become one of the essential parts of communication, especially in the corporate world, allowing the exchange of crucial information and promoting collaboration. However, email has become a popular target for malicious activities, such as spam emails, which can pose significant threats to individuals and organisations. While email providers use machine learning to identify patterns and classify emails, there is room for improvement. This research aims to increase email security by introducing a simple yet effective verification process for three essential email protocols: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). By analysing over 500 email headers, we aimed to determine how incorporating these protocols could improve the efficiency of spam detection. Our findings provide valuable insights into the behaviour of Gmail's spam detection algorithms and shed light on the complexities of email header analysis. Through empirical data and theoretical considerations, this research contributes to the ongoing discussion on email security and highlights the potential of protocol verification to strengthen defences against email-based threats.

KEYWORDS: Email Header, Analysis, Spam, Potentially Spam, Authentication, SPF, DKIM, DMARC.

I. INTRODUCTION

Email is an integral part of our daily routines, but it's important to remember that it may not always be a secure platform. We all receive a flood of emails, some of which can be annoying and even harmful, such as phishing scams that attempt to steal our personal information. In this research, we are diving into the inner workings of emails, especially their technical side. We want to understand how they prove they are genuine. Think of it like checking someone's ID to make sure they are who they say they are. By doing this, we aim to develop a method to spot fake or dangerous emails, making email safer and more secure.

Within this landscape, our research squarely addresses the pressing issue of identifying harmful emails. Specifically, we delve into the analysis of email header files and the pivotal role of authentication protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance). We aim to answer the fundamental question: “How can these email protocols be leveraged to distinguish genuine emails from fraudulent and harmful emails?”

The main goal of this study is to emphasise the significance of fundamental email protocols as decisive actions for enhancing security. By analysing these protocols, we aim to show how a simple verification process can provide valuable insights to users and organisations. It is about equipping individuals with the ability to discern whether an incoming email is trustworthy or potentially a part of a more significant security threat, ultimately fostering a safer and more informed email experience.

II. LITERATURE REVIEW

2.1 Email Header:

Emails comprise various parts, each serving a specific function. An email has three main components: the header, body, and attachments. The header is the top section of an email that provides essential details about the message. It contains metadata, which comprises different fields, each with its own information set. Knowing how to read an email header is essential for understanding how email communication functions.[16].

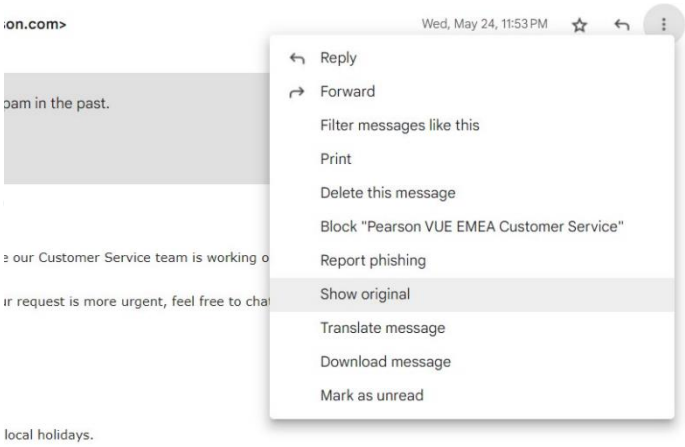

Fig.1. *How to open EMAIL HEADER in* ***Gmail***

2.2 Header Analysis:

Email header analysis is the linchpin of email security. Understanding the intricacies of email header fields is essential for effectively identifying spam messages. These fields contain critical information that cunning spammers manipulate to deceive spam detection systems. Researchers have carefully analysed email header elements to identify features useful for efficiently classifying and combating spam messages [18].

According to [8], different email systems have unique header fields, but common ones include

Fields	Description
From	This field specifies the email address of the sender.
To	This field identifies the email address of the recipient.
Subject	This field provides a summary of the message's contents.
Date	This field indicates the exact time and date that the email was sent.
Message ID	This field is a unique identifier for the email message.
Return-Path	This field specifies the email address to which any bounced messages will be returned.
Received	This field lists the servers through which the email is passed to the recipient.
Reply-To	This field specifies the email address to which replies should be sent.
MIME-Version	This field indicates the version of MIME (Multipurpose Internet Mail Extensions) used to format the message.
Content-Type	This field specifies the type of content in the message, such as text or HTML.
Content-Transfer-Encoding	This field specifies the method used to encode the message.

Table 1. Attributes of Email Header

2.3. Information Extraction From Email Header:

2.3.1 Sender and Recipient Analysis:
Sender analysis entails locating the email address and sender's identity by looking at the "From" field in the email header. It aids in determining the sender's credibility and authenticity. To determine who received the email and any extra recipients, recipient analysis concentrates on the "To," "CC," and "BCC" fields. This research makes Understanding the email's dispersion and potential connections between senders and recipients easier.

2.3.2 Date and Time Analysis:
Extraction and interpretation of the "Date" field from the email header constitute Date and Time Analysis. It offers valuable details on the time the email was sent, assisting with timelines, spotting abnormalities, and comprehending the temporal context of the communication.

2.3.3 Subject Line Analysis:
Analysing the subject line entails looking at the email's "Subject" field. It gives context for the content, aids in categorising and organising emails according to their contents, and aids in understanding the objective or topic of the email.

2.3.4 Message-ID and References:
An individual identification given to each message by the email server is contained in the Message-ID field in the email header. Tracking an email conversation's thread and locating replies and forwards are made easier with the help of message-ID analysis. The References field allows for the easy reconstruction of email threads by displaying the Message-IDs of earlier emails in a conversation.

2.3.5 IP Address and Geolocation Analysis:
The "Received" element in the email header, which gives details about the servers the email travelled through, is the IP Address and Geolocation Analysis topic, as shown in [9]. The sender's or the servers' approximate locations can be determined by extracting and analysing the IP addresses, which provide geolocation information.

2.3.6 Email Authentication Protocols:
SPF, DKIM, and DMARC represent indispensable email authentication protocols that play a pivotal role in determining the legitimacy of an email. In the context of this research, these parameters assume a critical significance as they directly influence the research's outcomes and findings.

As mentioned in [18], here is a list of Email Authentication Protocols and Custom Fields in the following:

Fields	Description
Delivered-To	It contains the email address to which the message will be delivered.
SPF	Mail Transfer Agent (MTA) will add this field to the header when the SPF query returns fail.
DKIM-Signature (Domain Key Identified Mail)	This field encompasses the contents of the message body and the headers. It does not necessarily require the e-mail from a specific IP address. Using public key cryptography allows organisations to take responsibility for sent e-mails by verifying that the e-mail came from an authorised source, similar to how secure servers connect over TLS/SSL.
DomainKey-Signature	Combination of the "From" and "Sender" with the private key during the signing process in the email server.

Table.2. Different Fields of Email Header

2.4 The Emergence of SPF and Its Limitations:

In response to the limitations of traditional methods, the Sender Policy Framework (SPF) emerged as a promising email filtering protocol.

2.4.1 How does SPF work?

SPF (Sender Policy Framework) is a protocol used for email authentication to prevent email spoofing and phishing attacks. It allows domain owners to specify which IP addresses or domains are authorised to send emails on behalf of their domain.

- When an email is received, the receiving mail server checks the SPF record of the sender's domain to verify if the sending IP address is authorized to send emails to that domain.
- The email will be considered legitimate if its sending IP address is listed in the Sender Policy Framework (SPF) record. Otherwise, it may be marked as spam or rejected.
- SPF records for a domain are published in DNS as a TXT record.
- The SPF record contains a list of authorized IP addresses or domains, and it can also specify how to handle emails that fail the SPF check. [24]

The robustness of SPF (Sender Policy Framework) as an email authentication protocol has been questioned due to its susceptibility to various spoofing methods employed by malicious actors. One such method involves utilising a compromised or malicious server listed in the SPF record of the impersonated domain, giving the false impression of an authorised sender. Furthermore, attackers can exploit vulnerabilities within the DNS system, allowing them to manipulate SPF records by adding unauthorised IP addresses or domains. Additionally, techniques like email forwarding or relaying enable attackers to bypass SPF checks, sending emails from an authorised server but subsequently rerouting them through unauthorised servers. These vulnerabilities underscore the importance of recognising that SPF alone does not offer foolproof protection against determined attackers.[24]

According to our research, it's best to combine SPF with other email authentication methods, such as DKIM and DMARC, to increase email security and prevent this issue.

2.5 Important role of DKIM and DMARC:

DKIM Verification: DomainKeys Identified Mail (DKIM) constitutes an integral facet of email authentication, bracing the security and integrity of electronic correspondence. Through DKIM, a digital signature is affixed to outgoing emails, serving as an unequivocal seal of authenticity. This cryptographic signature empowers receiving mail servers to

meticulously scrutinize the email's provenance, assuring its origin from a genuine source. Furthermore, DKIM is a sentinel against any malevolent tampering during the email's journey across the digital landscape.

DMARC Verification: Domain-based Message Authentication, Reporting, and Conformance (DMARC) represents a formidable evolution in email security, building upon the foundation laid by SPF and DKIM. DMARC amplifies the protective mantle and furnishes a structured policy framework for email authentication. Domain proprietors wield the authority to delineate explicit directives, dictating how receiving mail servers ought to navigate emails that fail the rigorous litmus tests of SPF or DKIM. This proactive stance in combatting email malevolence is a potent deterrent against pernicious email spoofing and phishing exploits, offering clear-cut guidance on handling potentially nefarious email transmissions.

Elevated Email Security: By incorporating DKIM and DMARC into email authentication processes, you can effectively prevent email fraud and misconduct. This powerful combination guarantees the authenticity of emails and provides strong protection against any unauthorized modifications while in transit. As a result, your email security is greatly enhanced, effectively shielding you from the dangers of phishing attacks, email spoofing, and identity theft.

Enhanced Email Deliverability: When DKIM and DMARC verification protocols are implemented, they bring benefits beyond just security. They also improve the chances of emails being delivered successfully. By adhering to these strict authentication standards, legitimate emails are less likely to be marked as spam or rejected by the recipient's mail server. This thorough authentication process builds trust between the sender and recipient, creating a favourable environment for successful email transmission.[16]

Overall, using DKIM and DMARC verification protocols for email security is not just a technical necessity. It's a significant step to make email communication more secure, protect against email spoofing, and ensure that emails are genuinely from the senders in the online world.

III. DEFINITIONS OF TERMS

In this section, we aim to provide clear and formal definitions of essential terms and concepts vital to understanding the research. These definitions are intended to enhance clarity and promote a common understanding of the subject matter. Below, you will find concise explanations of the key terms used throughout this paper:

Spam: In the context of this research, "spam" pertains to unsolicited emails characterized by their intent to gather user information without consent, contain malicious links or attachments, and often take the form of spoofed messages masquerading as legitimate communications.

Absolute Spam (Manually Identified Spams): "Absolute spam" refers to emails subjected to manual investigation to confirm their status as spam.

Gmail Spam: "Gmail spam" denotes the category of emails that are automatically directed to the Gmail Spambox based on the mechanisms and methods employed by Gmail's internal filtering system. This category encompasses emails that Gmail has classified as spam after its automated analysis.

MailFence Spam: "MailFence spam" encompasses emails that the MailFence Tool identifies and labels as spam using its proprietary mechanisms. This category represents emails that the MailFence Tool has autonomously flagged as spam during the analysis process.

Total Emails: "Total emails" signifies the aggregate number of emails drawn from both the Spambox and Inbox for the purposes of research analysis. This total encompasses emails designated as spam as well as those directed to the inbox.

Potentially Spam: "Potentially spam" refers to a category of emails that necessitate user caution and scrutiny. These emails may exhibit characteristics or attributes that raise suspicions about their legitimacy, warranting a closer examination by the recipient.

IV. METHODOLOGY

4.1 Data Collection and Observations:

i) Collecting Email Header Data:
Our data collection involved gathering email header data from a diverse group of individuals, encompassing approximately 15-17 people.
This participant pool covered a broad age range, with some individuals falling within the 19-22-year-old demographic while others were older family members aged approximately 50-53.

ii) Time Frame Limitation For Spam Mails:
Our objective was to acquire a comprehensive compilation of spam emails to conduct a meticulous evaluation. Regrettably, we encountered unforeseen obstacles throughout the data collection procedure. The primary predicament originated from the ephemeral nature of email material, which was exacerbated by Gmail's automatic deletion of spam emails older than 30 days. While this feature undeniably aids in maintaining tidy inboxes and conserving storage capacity, it presented a significant challenge to our investigation.

iii) Data Preprocessing:
To maintain the relevance and quality of our dataset, we undertook rigorous data preprocessing steps as follows:

Manual Analysis: We initiated the data collection process by manually scrutinising each email. Our primary objective was to identify potential spam emails through this manual review.

iv) Ethical Considerations:
All email header data used in our study were collected with explicit permission from the participants. This ethical practice ensured that individuals were aware of and consented to their email header data being used for research purposes.
While we are sharing the results of our research based on test data, it is essential to emphasise that the original email header files used for analysis will not be published or shared in any identifiable form.

4.2 Spam Detection Criteria:

In our research, we implemented a straightforward yet practical approach to detect spam emails based on analysing email headers. This approach was intentionally designed to provide valuable alerts to individuals and help prevent potential email-related losses. Our methodology differed from more complex machine learning algorithms that, despite their sophistication, may still have vulnerabilities.

1. Email Header Parsing:
The initial input to our detection system is the email header file. Given the complexity of email headers, the tool first parses these files to extract relevant data.

2. Header Simplification:
In order to make the analysis easier, we decided to simplify the email header. This involved removing any non-essential information that was not relevant to the study and keeping only critical data elements such as Message-ID, Authentication protocols, and IP address of origin.

3. Verification of Email Authentication Protocols:
We focused on three fundamental email authentication protocols: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance).
For each email, we verified the status of these three protocols. This verification process involved cross-referencing the email's header data with the authentication records associated with the sender's domain.

4. Criteria for Categorization:
Based on the status of each email authentication protocol, we categorised emails into three main groups:

a. **Spam Mail:** If the email failed all three protocols (SPF, DKIM, DMARC), it was classified as a spam email. This designation suggests a high likelihood of malicious intent.

b. **Authenticated Mail:** The email was classified as authenticated if it verified all three protocols. This designation implies a high level of confidence in the email's legitimacy.

c. **Potentially Spam Mail:** If the email's authentication status was mixed (i.e., it verified some protocols but failed others), it was categorised as potentially spam. Users were advised to exercise caution when opening such emails, as they might or might not be malicious.

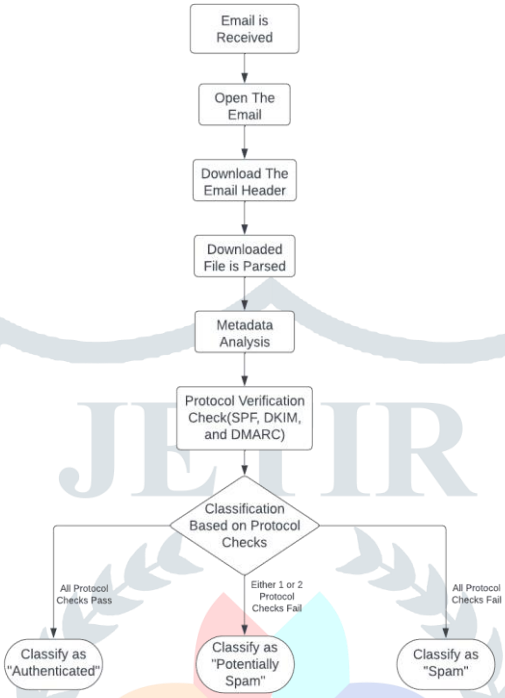

***Fig.2**. MailFence Flowchart*

Our approach is straightforward, prioritising user awareness and preventive action, making it a valuable tool in the fight against email-related threats, particularly for individuals and organisations seeking simple yet effective email security solutions.

Our tool's algorithm uses a python function named email.message_from_file() to read and parse the supplied email header and a class named email.parser.HeaderParser() to extract the email headers. The message ID, authentication outcomes, IP address, sender details, and other email-related metadata are initialised in a meta dictionary.

Libraries	Description
email	This library's classes and functions support email message creation, manipulation, and parsing. It is used to extract the email headers from the raw email file.
re (Regular Expressions)	Regular expressions, which are used for pattern matching and searching within email headers, are supported by this library. Regular expressions assist in locating specific patterns in the header data, such as IP addresses and authentication outcomes.
argparse	This helps parse command line arguments passed by the user. The argparse module defines expected ideas like the email file path and print help messages.

***Table.3**. Few Libraries Used in Our Algorithm*

The algorithm cycles through the email headers, such as determining the message ID and obtaining mail server data. The authentication status is checked by looking at the SPF, DKIM, and DMARC records.

V. ANALYSIS

The study encompassed a comprehensive analysis of 504 header files, comprising emails from both inbox and spambox. The primary objectives were to assess the performance of two different algorithms, the "MF Algorithm" and "Gmail's Algorithm," for identifying spam and potential spam emails within the email dataset.

In this research context, we use two fundamental categories within email management: the 'Inbox' and the 'Spambox.' These categories are critical components of email communication and play a pivotal role in our analysis.

The 'Inbox' represents the repository where safe, legitimate, and desired emails are received and accessible to the user. It serves as the hub for personal and professional correspondence, newsletters, and messages that meet the trust criteria set by the email service provider.

In contrast, the 'Spambox,' also called the 'Spam Folder,' is the designated area for emails flagged as unsafe. These emails are typically identified by algorithms and filtering mechanisms of service providers.

Analysis Results for MailFence:

Metric	Value
Total Email Headers from Inbox	219
Total Email Headers from Spambox	285
Total Email Headers Analysed	504

Table.4. *Total Email Headers Analyzed from Inbox and Spambox*

Inbox and Spam Box Statistics:

Inbox Statistics

Out of 504 total emails, 219 emails landed in our users' inboxes. Among these, an additional 53 emails were identified as spam upon manual verification. We then re-analysed those spam emails with our MailFence tool, identifying 25 out of these 53 emails as absolute spam. Further, 24 emails were marked as potentially spam by MailFence, while 4 were categorised as false positives. This resulted in 49 emails being classified as spam from the inbox emails just by performing SPF DKIM and DMARC verification.

Metric	Value
Total Emails from Inbox	219
Absolute Spams in Inbox	053
MF Verified Spams	025
Potentially Spam Emails by MF	024
False Positives (MF) for Inbox	004

Table.5. *Analysis of Email Headers for Inbox*

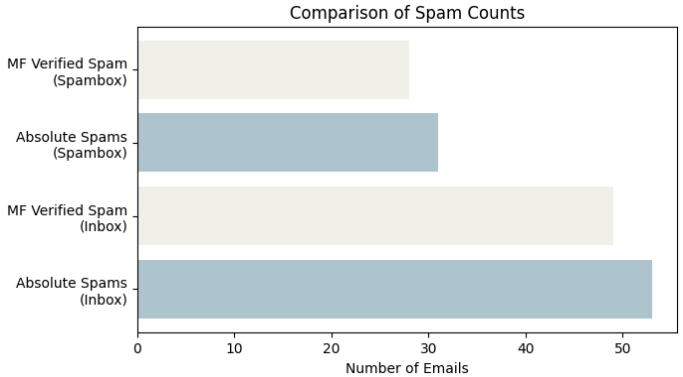

Fig.3. *Bar chart of spam count verified by MailFence and Gmail*

Spam Box Statistics

In the spam box, a total of 285 emails were analysed. Among these, 31 were absolute spam, and 18 emails were verified as spam by the MF Algorithm. Ten emails were marked as potentially spam, and three were identified as false positives. This resulted in 28 emails being classified as spam, including verified and potentially spam ones.

Metric	Value
Total Email Headers from Spambox	285
Absolute Spam Emails	031
MF Verified Spam	018
Potentially Spam Emails	010
False Positives (MF) Spambox	003

Table.6. *Analysis of Email Headers for Spambox*

5.1 Gmails' Spam Identification Mechanism:

During our rigid testing and detailed analysis of email headers, a fascinating revelation emerged about the Gmail Spam Filtration Algorithm. It became evident that Gmail's sophisticated spam filtration mechanism leverages advanced machine-learning techniques underpinned by intricate pattern recognition algorithms. This cutting-edge approach exhibits several distinct characteristics in its operation:

User Engagement-Based Filtering: Gmail's algorithm employs a user-centric strategy, prominently featuring the propensity of email recipients to interact with their incoming messages. Specifically, the algorithm appears to scrutinize the historical engagement patterns of users with their emails. Consequently, emails the recipient has yet to open or engage with frequently may be more prone to classification as spam.

Categorization of Promotional Content: Our analysis revealed that Gmail's algorithm tends to categorize a substantial portion of promotional emails as spam despite having a distinct section within Gmail for such promotional content. This observation highlights a noteworthy dimension of Gmail's filtration logic, where promotional emails are consistently rerouted to the spam box, potentially due to specific common attributes or patterns shared by these emails.

Prevalence of Non-Spam Categories: A substantial proportion of emails in the spam box were identified as non-spam during manual verification. These included legitimate emails such as newsletters, announcements, and other non-spam emails. This observation raises pertinent questions regarding the algorithm's classification criteria and the potential need for fine-tuning to reduce the occurrence of false positives, where genuine emails are inaccurately marked as spam.

Gmail's spam filtration system is advanced, using machine learning and pattern recognition techniques. However, our analysis highlights certain aspects of its functionality that warrant further investigation and refinement. The proactive classification of promotional emails and the occasional misclassification of non-spam content underscores the complex nature of email filtering algorithms, calling for a nuanced approach to enhance their precision and effectiveness.

5.2 Results:

Gmails' Success Rate for Email Classification:

Total number of emails analysed: 504
Let's assume this as "A"

Total emails in spambox: 285
Absolute spam in spambox: 31
Successfully Identified Spambox emails = 31
Let's assume this as "B"

Total emails in Inbox: 219
Absolute Spams in Inbox: 53
Successfully Identified Inbox emails = 219 -53 = 166
Let's assume this as "C"

Success Rate for Email Classification by Gmail
= ((B+C) / A) * 100

= ((31+166) / 504) * 100
= 197/504 * 100
= 0.3908 * 100
= **39.08%**

Result: The Gmail's Success Rate for Email Classification is 39.08%.

Gmails' Overall Spam Detection Rate:

Total Absolute Spams = Inbox spams + Spambox spams
= 53 + 31
= 84

Gmail Identified spams = 31(Spambox)

Spam Detection Rate
= (Gmail Identified Spams / Total Absolute Spam)*100
= (31 / 84) * 100
= 0.3690 * 100
= **36.90%**

Result: During our research, Gmails' Overall Spam Detection Rate came out to be 36.90%.

Metric	Value
Total Emails in Spambox	285
Absolute Spam	31
Non-spam Emails	254

Table.7. Spambox Statistics

Accuracy of Google's Spam Detection for Spam box:

Total Absolute Spam: 31
Total Emails in Spambox: 285
Accuracy Calculation: (Total Absolute Spam/Total Emails in Spambox)

Accuracy = (31 / 285) * 100
= 0.108 * 100
= 10.8%

Result: Google's accuracy for identifying spam in the spam folder is 10.8%.

Accuracy of MailFence for Spam Detection in Inbox:

Spams Identified by MF from Inbox: 77
Absolute Spams in Inbox: 84
Accuracy Calculation: (MF Identified Spams from Inbox / Absolute Spams in Inbox) * 100

Accuracy = (77 / 84) * 100
= 0.916 * 100
= **91.6%**

Result: The tool's accuracy for identifying spam in the inbox is 91.6%.

Accuracy of the Tool for Spam Detection in Spambox:

Total Tool-Identified Spams in Spambox: 49
Total Absolute Spam Mails in Spambox: 53

Accuracy Calculation: (Tool-Identified Spams in Spambox / Absolute Spam Mails in Spambox)
Accuracy = (49 / 53) * 100
= 0.9245 * 100
= **92.45%**

Result: The tool's accuracy for identifying inbox emails in the Spambox is 92.4%.

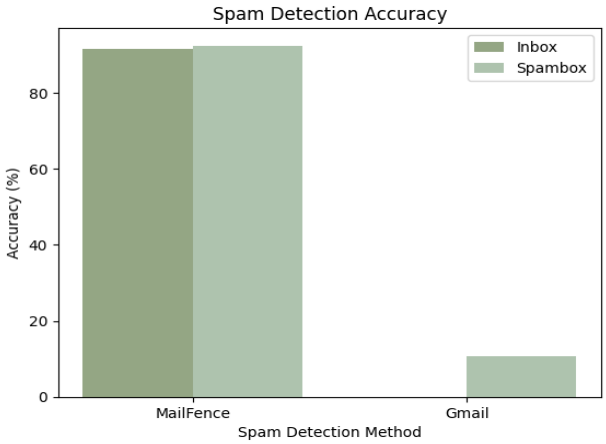

Fig.4. *Spam Detection Accuracy Comparison Between MailFence and Gmail*

5.3 Caution Rate:

Here, "Potentially Spam Mails" refer to emails that exhibit characteristics or behaviours that may raise suspicion but do not conclusively indicate malicious intent. These emails do not outright fail all authentication checks but may display mixed results or specific indicators that warrant caution when handling them. They fall into a grey area where users must be vigilant while assessing their legitimacy.

Here's an analysis of the provided data related to potential spam emails of the research:

Total Potentially Spam Mails: 134

This represents our analysis's overall count of potentially spam emails.

Potentially Spam Mails in Inbox:

Potentially Spam Mails in Inbox: 42
Total Inbox Emails: 219
Percentage of Potentially Spam Mails in Inbox:
Percentage = (42 / 219) * 100% ≈ **19.17%**

Potentially Spam Mails in Spambox:

Potentially Spam Mails in Spambox: 92
Total Spambox Emails: 285
Percentage of Potentially Spam Mails in Spambox:
Percentage = (92 / 285) * 100% ≈ **32.28%**

Caution Rate:

Total Mails Requiring Caution: 134
Total Mails Analyzed: 504

Caution Rate Calculation:

Caution Rate = (Mails Requiring Caution / Total Mails Analyzed) * 100

Caution Rate = (134 / 504) * 100
= 0.265 * 100
= **26.5%**

Result: Approximately 26.5% of the analysed emails require extra user caution when opening.

Confirmation Rate of Potentially Spam Mails:

Total Potentially spam Mails (potentially spam): 134
Total Confirmed Spam among potential spam Emails: 34

Confirmation Rate Calculation:

Confirmation Rate = (Confirmed Spam among Potentially spam Mails / Total Potentially spam Mails) * 100

Confirmation Rate = (34 / 134) * 100
= 0.25 * 100
= **25%**

Result: Approximately 25% of the emails categorised as potentially spam emails were confirmed as actual spam.

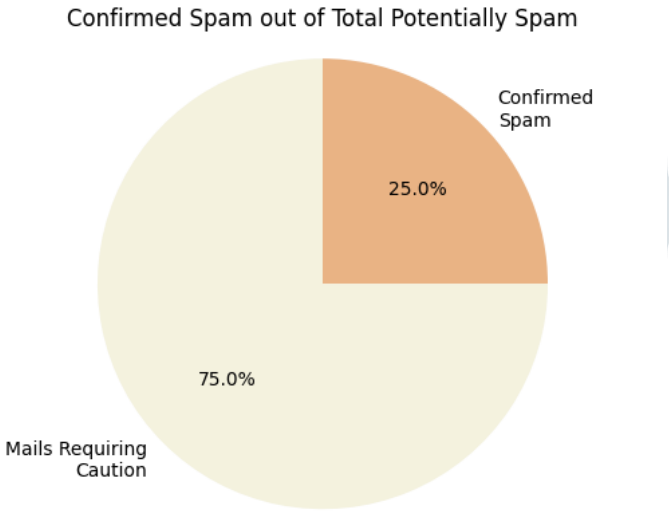

Fig.5. *Proportion of Confirmed Spam in Potentially Spam Emails*

VI. DISCUSSION

During the course of our research, several significant findings emerged that shed light on the intricacies of email security and spam detection. These findings not only contribute to our understanding of email filtering but also reveal areas where improvements and increased awareness are needed.

Age and Email Habits:

One noteworthy discovery from our research is the correlation between age and susceptibility to spam emails. It became evident that older individuals tend to receive more spam emails compared to their younger counterparts. This phenomenon can be attributed to the online behaviours of different age groups. Older individuals often use their email addresses on various websites without thoroughly verifying their authenticity, making them more vulnerable to spam. In contrast, younger individuals exhibit a greater degree of caution when sharing their email addresses, thus experiencing fewer spam emails. This finding underscores the importance of raising awareness about email security

practices, particularly among older populations. Implementing educational initiatives and providing guidance on safe email practices could substantially reduce the incidence of spam among this demographic.

Challenges in Parsing Obfuscated Headers:

Throughout our testing phase, we encountered a significant challenge related to certain email headers that proved difficult to read and parse. Upon closer examination, we discovered that spammers had deliberately obfuscated these email headers. This deliberate obfuscation rendered these headers indecipherable by our algorithms, resulting in their classification as spam. This revelation underscores the sophistication of modern spamming techniques and the need for continuous improvement in email filtering algorithms to detect and handle such obfuscation effectively. Addressing this issue could further enhance the accuracy of spam detection and reduce the chances of false positives.

DMARC Verification Limitations:

Another notable observation pertains to the verification of emails using the Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocol. Our research revealed a substantial failure rate in DMARC verification, primarily because many organisations have not undergone DMARC authentication. Consequently, emails from such organisations often end up being categorised as potentially spam due to their failure to pass DMARC checks. While DMARC is a powerful tool for enhancing email security, its effectiveness relies on widespread adoption and proper configuration by organisations. Encouraging more entities to adopt and configure DMARC correctly is essential to mitigate this limitation in email filtering systems.

Content Analysis for Enhanced Detection:

In our analysis of spam emails, we also uncovered a category of spam domains that successfully passed all the established email security protocols, making them appear authenticated. However, a manual examination of these emails unveiled telltale signs of their deceptive nature. These emails exhibited numerous grammatical errors and lengthy subject lines devoid of meaningful content—characteristics rarely found in communications from genuine organisations. This insight suggests that incorporating content analysis into our spam detection algorithms can be a valuable addition to address this limitation effectively. By considering the actual content of emails in addition to technical verification protocols, we can refine our spam detection methods and better identify malicious messages.

This research has illuminated various facets of email security and spam detection. The age-related susceptibility to spam, challenges posed by obfuscated email headers, DMARC verification limitations, and the importance of content analysis collectively underscore the complexity of email security. These findings provide valuable insights into the ongoing efforts to enhance email filtering systems, emphasising the need for continuous education, algorithmic improvements, and comprehensive email security practices to combat the ever-evolving landscape of email-based threats.

VII. EMAIL HEADER ANALYSIS IN CYBERSECURITY

7.1 Email Spoofing and Phishing Detection:

Cybercriminals frequently use email spoofing and phishing to fool receivers and trick them into disclosing critical information. Inconsistencies in the sender information, strange reply-to addresses, or mismatched domains are some indicators of spoofing and phishing attempts that can be found with practical email header analysis [14,21]. Advanced algorithms and machine learning models are used to analyse email headers, scan email content, and find patterns suggestive of fraudulent activity. This enables prompt detection and mitigation of these risks.

7.2 Email Threat Intelligence:

Email threat intelligence gathers and examines data from various sources to find new email-based risks. Security researchers can learn important details about the origin, purpose, and strategies threat actors use by looking at email headers. To stop upcoming attacks, this intelligence can be used to create proactive defence mechanisms, improve security standards, and spot trends or signs of compromise.

7.3 Email Authentication (SPF, DKIM, DMARC):

Email header analysis heavily relies on email authentication protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance),

as studied in [16,18]. While DKIM adds digital signatures to emails to verify message integrity and SPF and DKIM are combined in DMARC to give a complete authentication framework, SPF checks that the sending server is authorised to send emails on behalf of a specific domain. By examining these authentication measures in email headers, you may prevent spoofing and phishing attacks and confirm the reliability of email sources.

Standards are rules that ensure different parts of a system work together correctly. However, these standards can sometimes be unclear and open to different interpretations. Let's take an example to understand this better:

According to [16], imagine we have two components, DMARC and SPF, which are used to prevent email spoofing (a type of email fraud). DMARC relies on SPF to authenticate the sender's email address. However, there is a problem. The DMARC component assumes that if the sender's email address is not empty, the SPF component will always verify it. But SPF does not guarantee this.

In this situation, the SPF component might verify a different identifier called "HELO," which is a part of the email protocol. Then, it leaves it up to the DMARC component to determine which identity is verified. This mismatch in authentication can lead to an email authentication bypass, which means that fraudulent emails may still get through the system.[16]

To summarise, the issue is that the standards need to be more apparent, and each component interprets them differently. This misinterpretation leads to a mismatch in authenticating the email identifiers, resulting in a potential security vulnerability. Due to this, Email Header Analysis is essential to use, especially by enormous organisations.

7.4 Malware and Spam Detection:

Malware and spam detection in cybersecurity depend heavily on email header analysis. According to [15,23], security systems can locate suspicious indicators by carefully examining email headers, such as attachments or links to harmful information, odd email routing patterns, or specific header data linked to spam operations. Advanced heuristics, behaviour-based analysis, and machine learning algorithms are used to identify and filter out potentially hazardous emails. This lowers the risk of malware infections and lessens the impact of spam on email users and organisations.

VIII. CONCLUSION

We delved into the intricate world of email header analysis, specifically focusing on the efficacy of authentication protocols such as SPF, DKIM, and DMARC. Our findings underscore these protocols' pivotal role in bolstering email security by establishing trust in email communication. Through meticulous analysis, our developed tool showcased impressive accuracy rates of 91.6% for identifying spam within inboxes and 92.4% for recognising genuine spam emails in the spambox, offering users a valuable defence against email-related threats.

Moreover, we introduced the concept of "potentially spam emails," representing emails with suspicious attributes that necessitate user caution. Approximately 19.17% of inbox emails and 32.28% of spambox content fell into this category, underscoring the importance of user vigilance when handling such messages. Our research also revealed a confirmation rate of 25% among potentially spam emails, emphasising the need for thorough scrutiny to mitigate security risks.

As we progress, our research is leading the way for future advancements in email security. One potential area for future exploration involves incorporating advanced grammatical analysis utilizing large language models(LLM). This innovative approach has the potential to overcome the limitations encountered during manual spam mail observation, which could enhance our tool’s efficiency.

In conclusion, this project contributes to a deeper understanding of email authentication protocols and equips users with a powerful tool for spam detection. It emphasises the critical role of user diligence in safeguarding against potentially malicious emails. It provides valuable insights to enhance digital communication security in an ever-evolving cyber landscape.

REFERENCES

[1] Basit, A.W., Zafar, M., Liu, X., Javed, A.R., Jalil, Z., & Kifayat, K. (2020). A comprehensive survey of AI-enabled phishing attack detection techniques. Telecommunication Systems, 76, 139 - 154.

[2] Alotaibi, R.M., Al-Turaiki, I.M., & Alakeel, F. (2020). We are mitigating Email Phishing Attacks using Convolutional Neural Networks. 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), 1-6.

[3] Wongwatkit, R., Raktham, M., & Phawananthaphuti, T. (2022). Intelligent Blacklist Security System for Protecting Spammer in Corporate Email Solution: A Case of Corporate Email Service Provider in Thailand. 2022 24th International Conference on Advanced Communication Technology (ICACT), 387-391.

[4] Gordon, W.J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R.J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M.A., Sanford, B., Scheib, P., & Landman, A.B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. JAMA Network Open, 2.

[5] Ahmad, M. A., & Ismail, N. (2020). Digital Forensic on Email Fraud Investigation Using Design Science Research Methodology. International Journal of Software Engineering and Its Applications, 14(2), 37-50

[6] Guo, H., Jin, B., & Qian, W. (2013). Analysis of Email Header for Forensics Purposes. 2013 International Conference on Communication Systems and Network Technologies, 340-344.

[7] Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. Int. J. Hum. Comput. Stud., 82, 69-82.

[8] Banday, M.T. (2011). Technology Corner: Analysing E-mail Headers For Forensic Investigation. J. Digit. Forensics Secur. Law, 6, 49-64.

[9] Lin, E., Aycock, J., & Mannan, M. (2012). Lightweight Client-Side Methods for Detecting Email Forgery. Web Information System and Application Conference.

[10] Gupta, S., Pilli, E.S., Mishra, P., Pundir, S., & Joshi, R.C. (2014). Forensic analysis of E-mail address spoofing. 2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), 898-904.

[11] Babu, P.R., & Bhaskari, D.L. (2010). A Comprehensive Analysis of Spoofing. International Journal of Advanced Computer Science and Applications, 1.

[12] Rastenis, J., Ramanauskaitė, S., Janulevicius, J., Cenys, A., Slotkienė, A., & Pakrijauskas, K. (2020). E-mail-Based Phishing Attack Taxonomy. Applied Sciences.

[13] Wijayanto, A.W., & Takdir (2014). Fighting cybercrime in email spamming: An evaluation of fuzzy clustering approach to classifying spam messages. 2014 International Conference on Information Technology Systems and Innovation (ICITSI), 19-24.

[14] Mistry N., Bhati R., Jain H., Parmar M. (2016). Email Spoofing Analysis. International Journal of Computer Science & Information Technology (IJCSIT), Volume 8, Issue 5

[15] Hoonakker, P.L.T. & Carayon, Pascale & Bornø, Nis. (2009). Spamming, spoofing and phishing E-mail security: A survey among end-users.

[16] Chen, J., Paxson, V., & Jiang, J. (2020). Composition Kills A Case Study of Email Sender Authentication. USENIX Security Symposium.

[17] Charalambou, E., Bratskas, R., Karkas, G., & Anastasiades, A. (2016). Email forensic tools: A roadmap to email header analysis through a cybercrime use case.

[18] Razak, S.B., & Mohamad, A.F. (2013). Identification of spam email based on information from email header. 2013 13th International Conference on Intelligent Systems Design and Applications, 347-353

[19] Jakobsson, M. (2005). Modelling and Preventing Phishing Attacks. Financial Cryptography.

[20] Alam, M.N., Sarma, D., Lima, F.F., Saha, I., Ulfath, R.E., & Hossain, S. (2020). Phishing Attacks Detection using Machine Learning Approach. 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 1173-1179.

[21] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

[22] Salloum, S., Gaber, T., Vadera, S., & Sharan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. IEEE Access.

[23] Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K., & Alazab, M. (2019). A comprehensive survey for intelligent spam email detection. IEEE Access, 7, 168261-168295.

[24] Dalkılıç, G., Sipahi, D., & Özcanhan, M.H. (2009). A simple yet effective spam blocking method. International Conference on Security of Information and Networks.