SENDER AUTHENTICATION AS A METHOD FOR LEGITIMATE MAIL SERVER DETECTION

Mrs.T. Rathi Devi, Prajwal H.S, Prajwal H.M, Sachin R.M, Srinivas K,

[1]*Mrs.T. Rathi Devi, Information Science & Engineering, RajaRajeswari College of Engineering, Karnataka, India*

[2]*Prajwal H.S, Information Science & Engineering, RajaRajeswari College of Engineering,Karnataka, India*
[3] *Prajwal H.M, Information Science & Engineering, RajaRajeswari College of Engineering,Karnataka, India*
[4]*Sachin R.M, Information Science & Engineering, RajaRajeswari College of Engineering, Karnataka, India*
[5]*Srinivas K, Information Science & Engineering, RajaRajeswari College of Engineering, Karnataka, India*

ABSTRACT

Anti-spam tactics include, for example, ways to distinguish unsolicited Online mail from the email content and ways to make use of sender information. By using email content with a high processing load to assess whether the Online mail should be received based on the sender's Internet Protocol address and Web Address, it is feasible to minimize the amount of time the spam filter spends processing spam. In this inquiry, sender authentication technology is meant to analyze the sender emails that have been forwarded. Since we think the sender of this forwarded email is a legitimate email sender, we suggest using this as an allow list. In this post, we offer a suggestion to improve the approach we previously offered and reduce allow list confusion..We validated the effectiveness of this novel approach using the log data from the emails that were really received..

Keyword:*BEC*- *Buisness email compromise,* ***DNSBL****- Domain Name System-based Black hole List,* ***DNSWL****-DNSbased white list,****SPF****- Sender Policy Framework,* ***DKIM*** *- Domain Keys Identified Mail,* ***DMARC****-Domain-based Message Authentication Reporting & Conformance,****MD5****- message-digest algorithm*

1. INTRODUCTION

Spam problems are not just annoying; they also contribute to a number of security problems. For instance, using tricks like phishing attacks and business email compromise (BEC), email may be exploited to propagate false information for financial advantage. Additionally, dangerous malware that converts PCs into "bots," or externally controllable computers, and steals data is sent through email. On the receiving end, spam filters can be made to protect email users against spam. Innumerable methods have been created for the technology used in spam filters, and they have demonstrated to be largely successful. However, spammers are also seeking to circumvent these spam filters' detection, and as a result, the issue of inaccurate spam filter detection has gotten worse and cannot be avoided. The problem of false positives, which classify valid communications as spam, is quite concerning, especially for users of corporate email. Sender reputation, which uses email sender information, is hence useful for lowering false positives from email filters. DNSBL, which utilises the source IP address as a blocklist, has been used generally for sender reputation. DNSWL is used as an allowlist as well, but it is rarely very well-liked. Because sender authentication technologies like SPF, DKIM, and DMARC have been suggested and made it feasible to prevent sender domain name spoofing, sender reputation utilising these authorised domains is also projected. In this study, we propose a method for locating trustworthy email servers, like a method for boosting sender trustworthiness.Utilising email forwarders allows legal email servers to collect data. This method is superior to the previously suggested techniques.since it aims to reduce false positives. We checked the validity of the obtained valid email server using the judgement results from the spam

filter. This is how this essay is organised. We give a brief overview of sender authentication technology as well as the characteristics of each authentication method. We will also go through relevant research on the process of establishing sender reputation as well as the extraction of the sender of forwarded emails used in our technique. The method we recommended for identifying forwarding emails and the lawful method it employs for email server extraction. Next, we recommend a method to reduce the number of false positives produced by the current method the dataset on which we use our novel approach. We manifest that this novel method has resulted in a decrease in false positives.

1.1 Problem Statement

Spam problems are not just annoying; they also contribute to a quantity of security problems. For instance, through phishing and business email compromise (BEC) schemes, email may be exploited to propagate false information for monetary advantage. Additionally, dangerous malware that converts PCs into "bots," or externally controllable computers, and steals data is sent through email. Users may avoid spam and losing their personal information by using spam filters on the receiving end of email conversations.

1.2 Proposed System

- The sender information and the authentication mechanism used.
- Create an electronic signature using the private key using the email's header and content, then add it as a Signature email header to the message..
- It verifies whether or not the server information listed in the record posted on the server corresponds to the sender of the outgoing message.
- It uses the IP address of the email source for authentication. Consequently, an email that was sent by someone other than the sender.
- Sender authentication is used in this system while receiving mail.
- The authentication result is used to assess forwarded messages and identify the sender of the legitimate mail server in order to boost the sender's reputation.

1.3Objectives of theTask

- To determine legitimate mail by looking up the IP address of the sender.
- To recognise flood assaults between sender and recipient, block users based on an incorrect IP.
- Create signatures for the data packets to make sure their contents haven't been changed.

2. LITERATUREREVIEW

Asif Karim, Sami Azam, Bharatidharan Shanmugam, Krishnan Kannoorpatti, Mamoun Alazab, and others noted in this study [1] that whereas emails of the opposite sort are known as ham, or beneficial emails, email spamming is the act of sending unsolicited communications via email, perhaps in mass. When "Shoulder Pork HAM," a precooked pork in a can, was initially offered for sale in 1937, the term "spam" was first used to describe it. It has become common use to use the phrase to describe undesired electronic messages. Spammers disseminate spam emails for fundamental economic purposes in order to disseminate more destructive behaviours like financial disruption and reputational harm on both a personal and institutional level. In other digital communication venues as well, spamming is also gaining ground swiftly.Money is one of the primary drivers of spammers, and it's been calculated that they earn about USD 3.5 million from spam each year.

Kanako Konno, Naoya Kitagawa, Shuji Sakuraba, Nariyoshi Yamai, et al. suggest an Spam problems are not just annoying; they also contribute to a number of security problems. For instance, through phishing and business email compromise (BEC) schemes, email may be exploited to propagate false information for monetary advantage. Additionally, dangerous malware that converts PCs into "bots," or externally controllable computers, and steals data is sent through email. On the receiving end, spam filters can be used to protect email users against spam. Various techniques have been developed for the technology used in spam filters, and they have demonstrated to be largely successful. On the other hand, spammers are trying to avoid being picked up by these spam filters, therefore inaccurate spam filter detection is an issue that must be avoided. The problem of false positives, which classify valid communications as spam, is quite concerning, especially for users of corporate email. The oFsender reputation tool, which makes use of email sender information, is useful for lowering false positives in email filters.

With the current email infrastructure, any server injecting mail into the system is free to use whatever DNS domain name it wishes in any of the various identifiers provided by [RFC5321] and [RFC5322]. This is what S. Kitterman suggests in this article [3]. Although this capability is helpful in some situations, it poses a considerable obstacle to reducing unwanted mass email, generally known as spam. The ease with which other entities might utilise their domain names, usually with malevolent intent, is another reason why ADMDs (as defined in [RFC5598]) would be worried. This document's protocol explains how ADMDs can authorise hosts to use their domain names as "MAIL FROM" or "HELO" identities.During a mail transaction, compliant mail receivers utilise the public Sender Policy Framework (SPF) records to verify that sending Mail Transfer Agents (MTAs) are authorised to use a certain "HELO" or "MAIL FROM" identity. The Sender Policy Framework (SPF) entries that compliant ADMDs broadcast in the DNS describe which hosts are allowed to use their domains. Mail receivers benefit from being able to base local policy judgements concerning the mail on the sender's domain rather than the host's IP address once the usage of an identity has been verified. This is advantageous because reputation of domain names is more likely to be true than reputation of host IP addresses since domain names are more likely to remain steady over a longer period of time.

Additionally, if a stated identity cannot be verified, local policy may take more acute measures against such emails, such as rejecting them.

The Sender Policy Framework ([SPF]) and DomainKeys Identified Mail ([DKIM]) are suggested as a means of providing domain-level authentication in this study [4] by M. Kucherawy and E. Zwicky. Cooperative email receivers can use them to recognise emails that are permitted to use the domain name, which can enable different processing. ([DKIM-dangers] provides a comprehensive summary of the risks that these systems aim to mitigate.]) There hasn't been a single generally accepted or open method to ask for reporting of authentication and mail disposition or to share domain-specific message-handling policies for recipients. Due to the inability to obtain feedback reports, those who have used email authentication find it difficult to assess its success.Thus,attempting to exploit authentication failures as a means of mail filtering is typically futile. Over time, specific senders and receivers established one-on-one connections using privately communicated techniques to enact policies, receive message traffic and authentication disposition information, and enforce those procedures. Despite the fact that these ad hoc solutions have typically been effective, they need a lot of human coordination between players, and this pattern does not scale for widespread Internet use.

3. METHODOLOGY

We start by explaining our recommended approach for locating genuine mail servers. One method to find a trustworthy email server is to ascertain the sender's authentication result for the forwarded email using the sender's IP address and the sender's authentication result for the received email.

In this project, we offer a technique to improve our system further and reduce the likelihood that the allow list would be incorrectly interpreted. We were able to verify the success of this novel strategy by using the log information from the Online mails that were really received.

The source IP address is used as a blacklist in DNSBL Domain Name System Blacklists, which have historically been used to manage sender reputation. The DNSWL DNS-based white list, albeit not widely used, may also be used as an allow list. Because sender authentication technologies like SPF Sender Policy Framework, DKIM Domain Keys Identified Mail, and DMARC demarcation point have been suggested and may currently prevent sender domain name spoofing, sender reputation utilising these permitted domains is also projected.

3.1 DATA FLOW

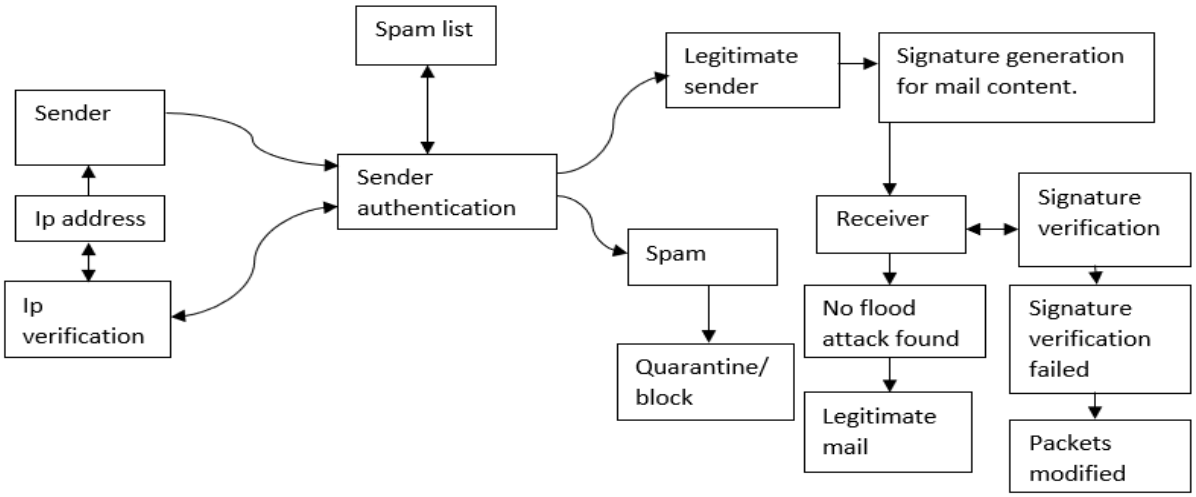

Fig-1:Data Flow of project

3.2 ARCHITECTUREOFTHESYSTEM

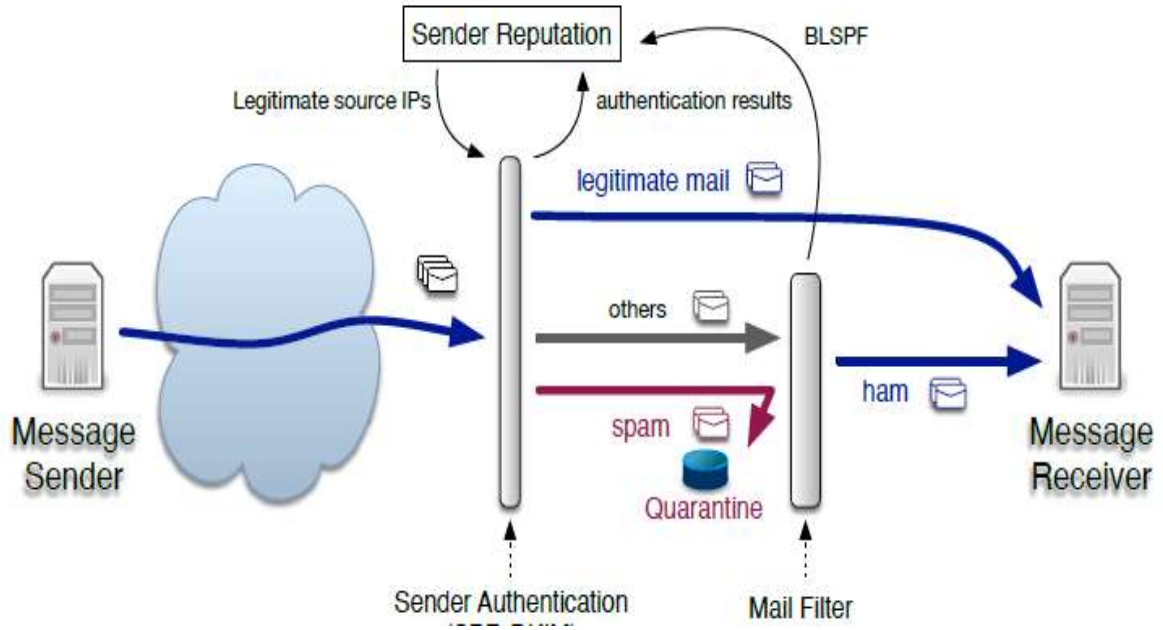

Fig-2: ArchitectureofSystem

4. RESULTSANDANALYSIS

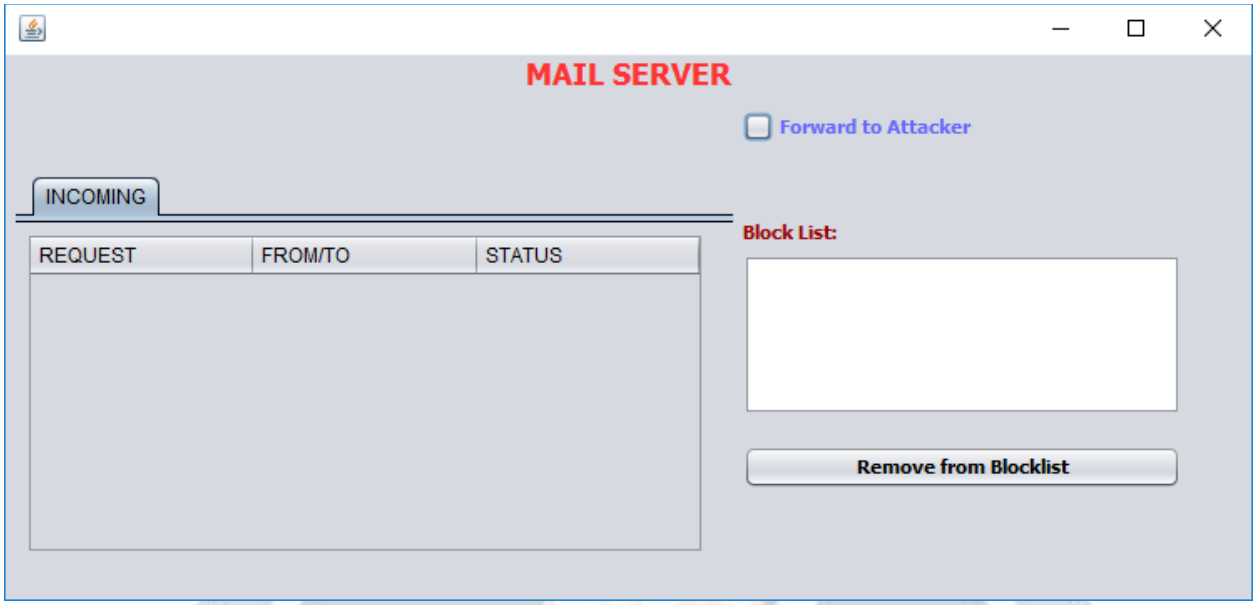

Fig-3: Mail server

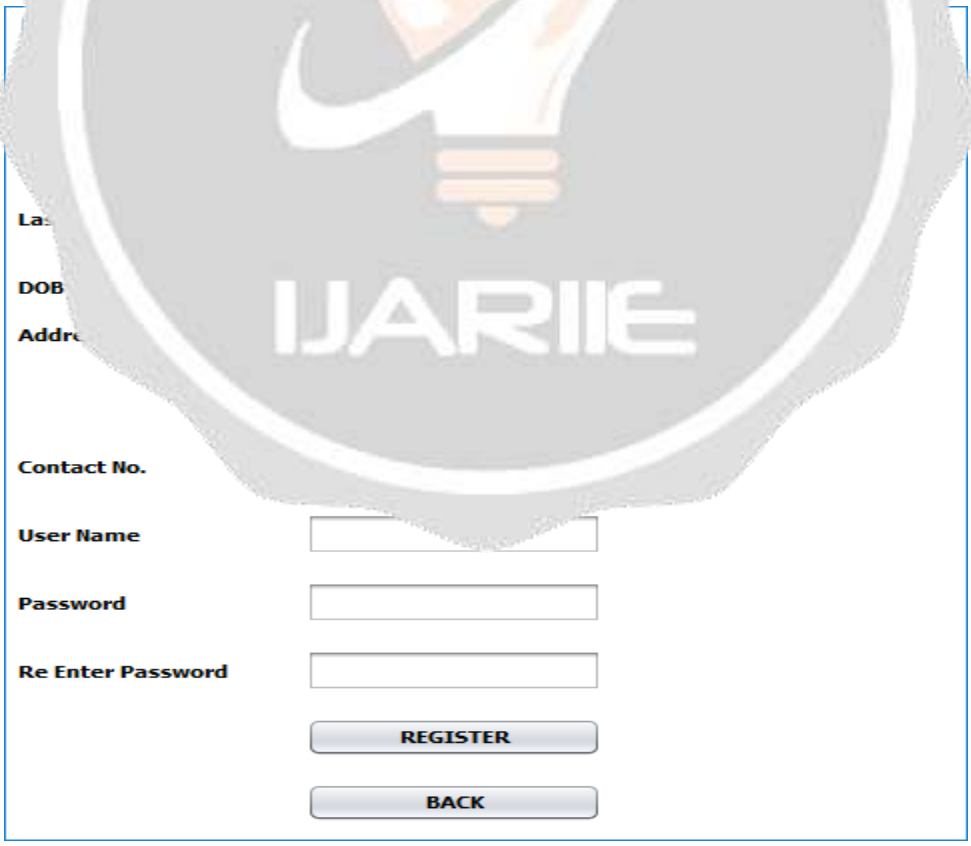

Fig-4: User registration form

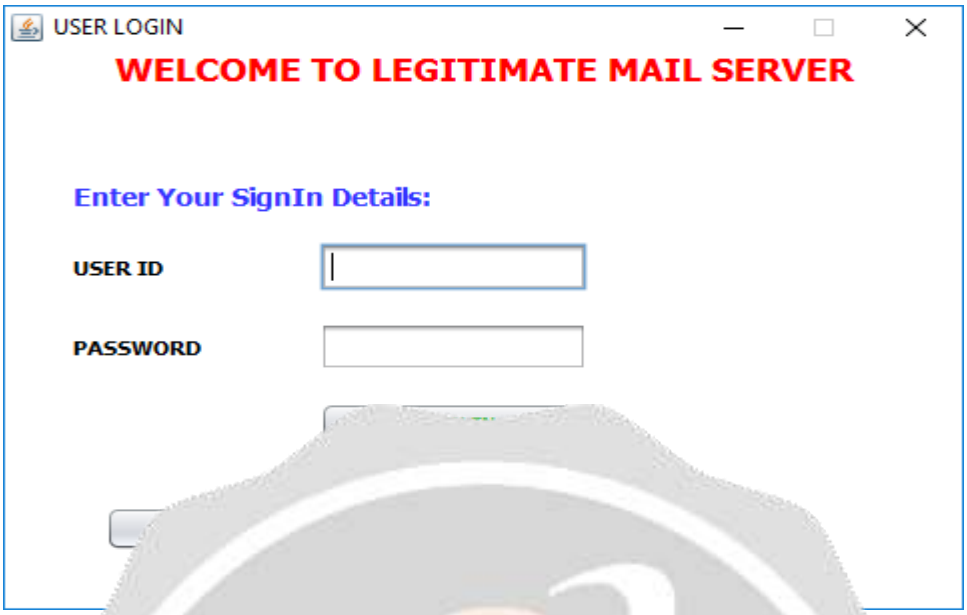

Fig -5 : Welcome page

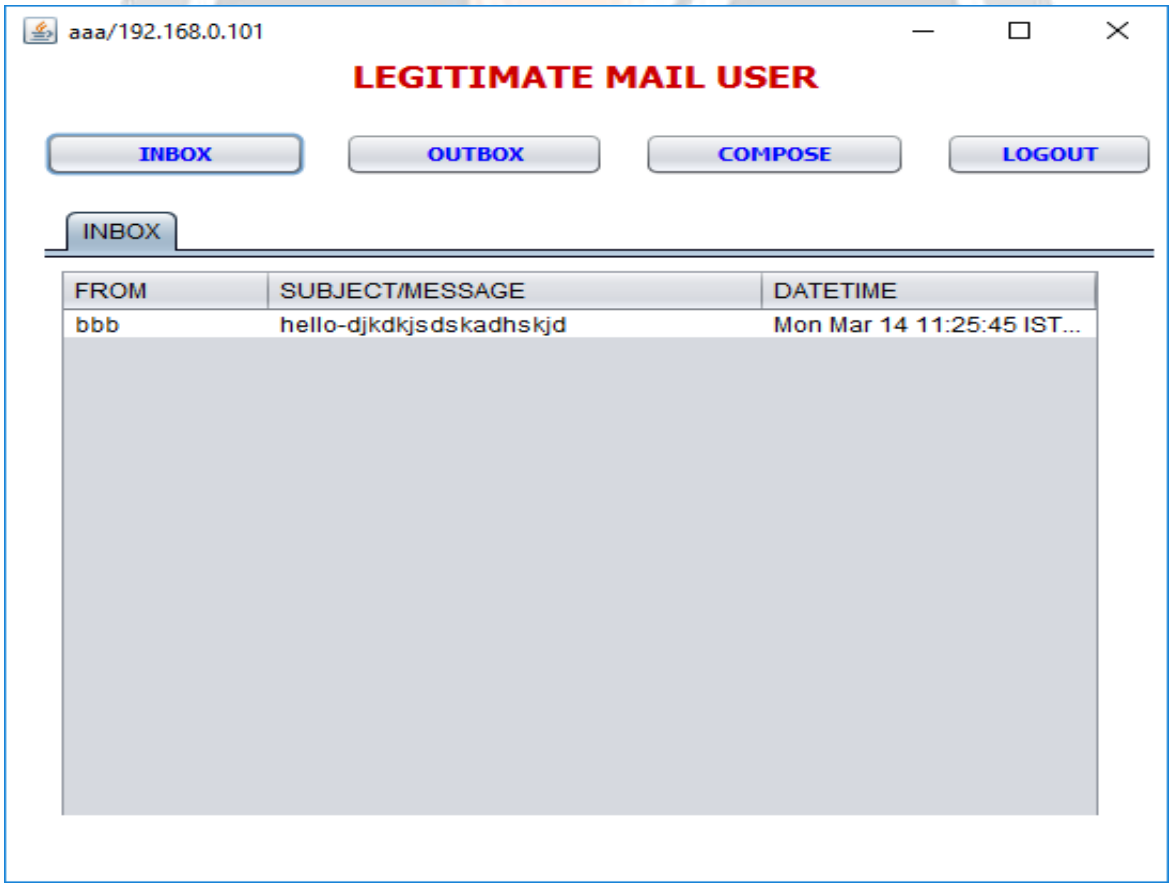

Fig-6 : Inbox

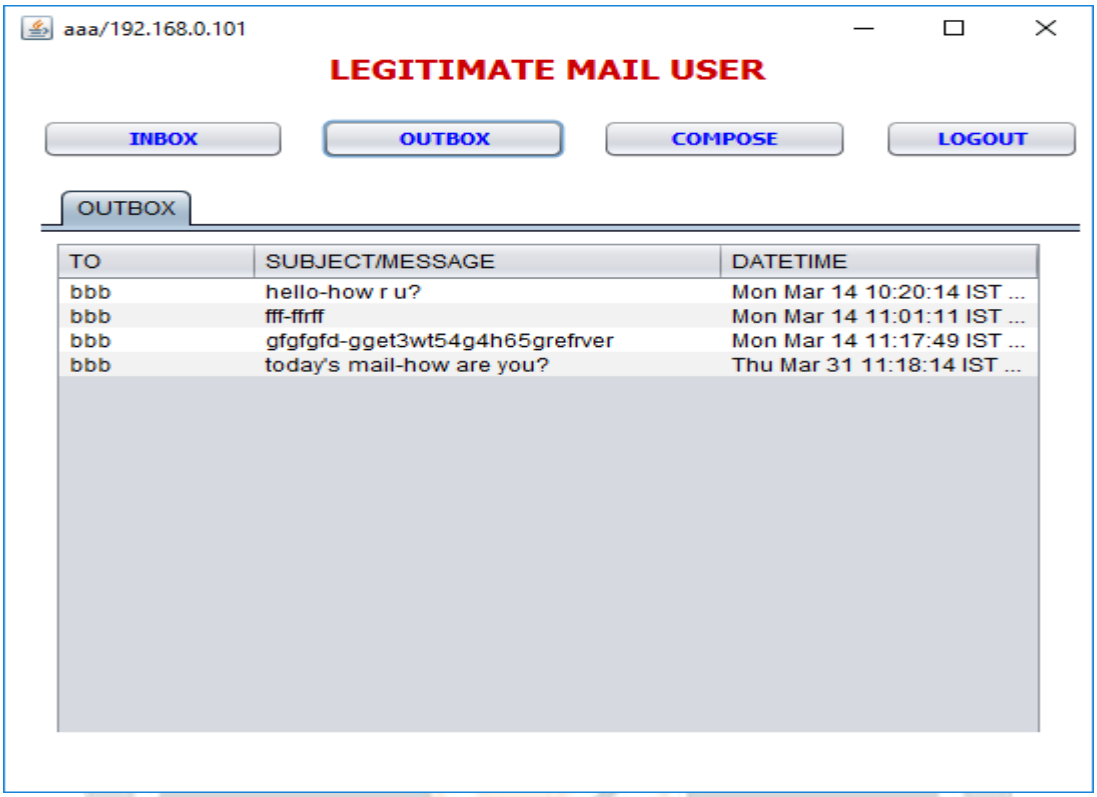

Fig-7 : Outbox

Fig-8 : Compose mail

Fig-9 : Attacker page

5. EXPECTED OUTCOMES

- Using IP address verification, one may ascertain if a sender is a human, a spambot, or a computer.
- Packets are verified using the signature generation mechanism. Planning flood defences will benefit from this.
- Sender of spam is blocked.
- Receiver doesn't get any spam or false information.

6. REFERENCES

[1] "Sender reputation construction method using sender authentication technologies," IPSJ Journal, Vol. 62, No. 5, pp. 11731183, 2021. S. Sakuraba, M. Yoda, Y. Sei, Y. Tahara, and A. Ohsuga.

[2] S. Sakurab, "Messaging technology," IIJ Internet Infrastructure Review (IIR), Vol. 47, 2020, pp. 4–9, available at: http://www.iij.ad.jp/en/dev/iir/pdf/iir vol47 EN.pdf.

[3] "Legitimate email forwarding server detection method by X-means clustering utilising DMARC reports," Eleventh International Conference on Evolving Internet (INTERNET 2019), pp. 24-29, 2019. K. Konno, N. Kitagawa, S. Sakuraba, and N. Yamai.14

[4] S. Azam, B. Shanmugam, K. Kannoorpatti, M. Alazab, and A. Karim: "A comprehensive survey for intelligent spam email detection," IEEE Access, Vol. 7, pp. 168261–168295, 2019..

[5] "Domain-based message authentication, reporting, and conformance (DMARC)," by M. Kucherawy and E. Zwicky. RFC7489, 2015.

[6] D. Sipahi, G. Dalk, and M. H. O'zcanhan, "Detecting spam through their sender policy framework records," in Security and Communication Networks, Vol. 8, No. 18, 2015, pp. 3555–3563.

[7] D. Sipahi, G. Dalk, and M. H. Ozcanhan, "Detecting spam through their sender policy framework records," in

Security and Communication Networks, Vol. 8, No. 18, 2015, pp. 3555–3563.

[8] "Sender policy framework (SPF) for authorising use of domains in email, version 1," S. Kitterman, RFC7208, 2014.

[9] "DomainKeys identified mail (DKIM) signature," by D. Crocker, T. Hansen, and M. Kucherawy. 2011's STD 76, RFC 6376.

[10]"On the effectiveness of IP reputation for spam filtering," 2010 Second International Conference on COMmunication Systems and NETworks (COMSNETS 2010), pp. 1–10, by H. Esquivel, A. Akella, and T. Mori.