Improvement of Legitimate Mail Server Detection Method using Sender Authentication

Asst. Prof. Kavya R[1], Pooja P[2], Jayant PB[3], Jayanth kowshik[4], Sushmitha MH[5]

[1]Assistant Professor, Dept. of CSE, Vidya Vikas Institute of Engineering and Technology, Mysore, Karnataka, India.
[2,3,4,5] Student, Dept. of CSE, Vidya Vikas Institute of Engineering and Technology, Mysore, Karnataka, India.

---***---

Abstract *- The anti-spam measures include ways to detect unsolicited email from email content and ways to use sender information. If it cannot be determined from the sender's IP address of the sender information and the sender's domain name whether the email should be received, it is possible to reduce the processing of spam filter by email content which has a heavy load of processing to determine. This study uses sender authentication technology to identify the sender of the forwarded email. We think the sender of this forwarded email is the official email sender to receive, and we suggest using them as a checklist. In this paper, we propose a way to further improve the approach we have proposed and reduce the misinterpretation of the approval list. We have verified that this new method works using login details for emails that are not actually accepted.*

Key Words**: Unsolicited emails, legitimated email,** ***Authentication technology, Ip address, AntiSpam.***

1. INTRODUCTION

Spam issues are not only annoying but also cause various security issues. For example, email is used as a way to pass on false information for the purposes of money exploitation, such as phishing and business email interception (BEC). Additionally, email is misused as a means of sending malware for information theft and creating externally controllable PCs called bots. To protect email users from spam, it is effective to apply spam filters on the receiving end. Various methods have been developed for the technology used in spam filters and have been effective to some extent. On the other hand, spammers are also trying to avoid being detected by these spam filters, and misperception of spam filters has become an inevitable problem. The problem of false positives identifying legitimate emails as spam is a major concern, especially for business email users.

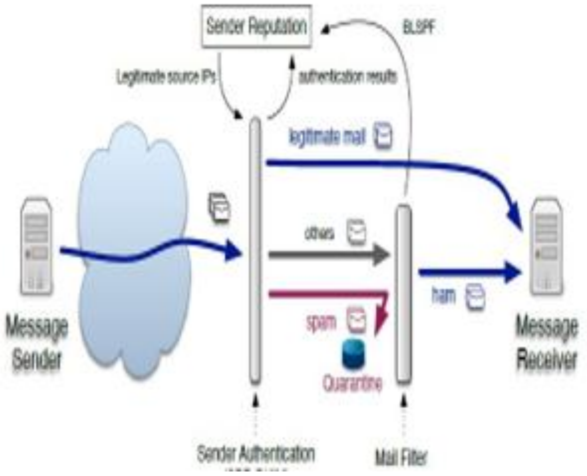

Fig1: Architecture of the System.

2. LITERATURE SURVEY

• Legitimate mail server detection

The problem of phishing email, also known as spam, including targeted phishing or spam-derived malware, has necessitated the need for reliable intelligent anti-spam email filters. This survey report describes a focused literature search on Artificial Intelligence (AI) and Machine Learning (ML) methods for intelligent spam email detection, which we believe can help develop appropriate countermeasures.

• IP address and protocol

In this article, we propose a method of collecting legitimate email servers as a method of building sender reputation. Legitimate e-mail servers collect the forwarded e-mail using their senders. This method is an improvement over the previously proposed method [7] in order to reduce false positives. We verified using the spam filter's evaluation result to evaluate whether the legitimate email server collected was correct.

3. REQUIREMENT ANALYSIS

To achieve the aim of this system, the system requirements need to be determined. In this part the detail of the requirements will be determined in the following steps:

System Requirements

- **The software requirements are:**

1. Database: MongoDB
2. Tools: JDK 8, NetBeans IDE 8.0, Heidisql
3. Backend Language: MySQL 5.0 Server
4. Frontend Language: Java AWT and Java Swing.

- **The Hardware requirements are:**

1. System processor: 1.8GHz or more.
2. System RAM: 2GB or more.
3. Processor bit: 32bit or 64bit.
4. Hard disk space: 20GB or more

4. DESIGN

The two main components of systems development are system analysis and system design. The system architecture is created during the system design phase. Maps the requirement to the architecture. Components, their interfaces and behaviors are defined in the architecture. The design document describes an email authentication database.

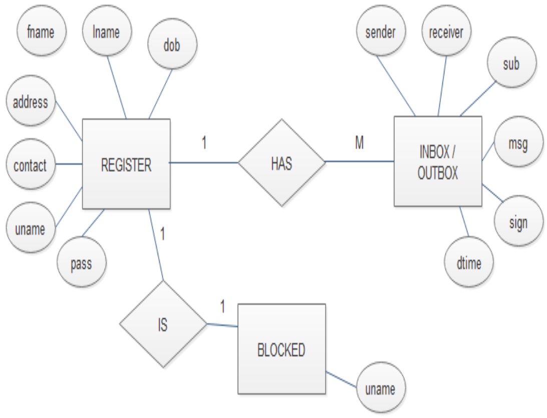

Fig2: Data Flow diagram showing communicationbetween sender and authentication.

Fig2 depicts the high-level design of the proposed system, where the broker or the main node, is the intermediation between the two ends i.e. Register and inbox/outbox, where the each module can how to register and send messages through sender to receiver that time how hacker can hack messages that messages to avoid through detection and digital signature that will be showed in this data flow diagram.

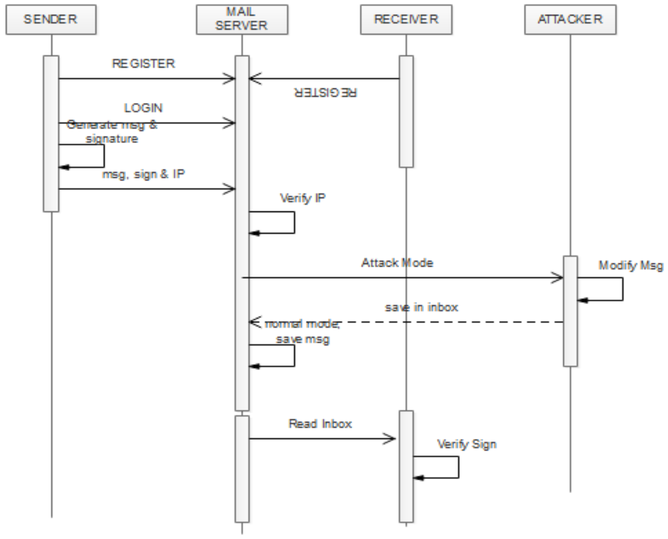

Fig3: sequence diagram of sender and attacker

Fig3 shows the Sequence diagram of the proposed system where initially, sender and receiver communication that time how attacker can change the messages how flood attack will be happened in mail server and how this project is helpful to avoid the flood attacks that will be showed in the figure.

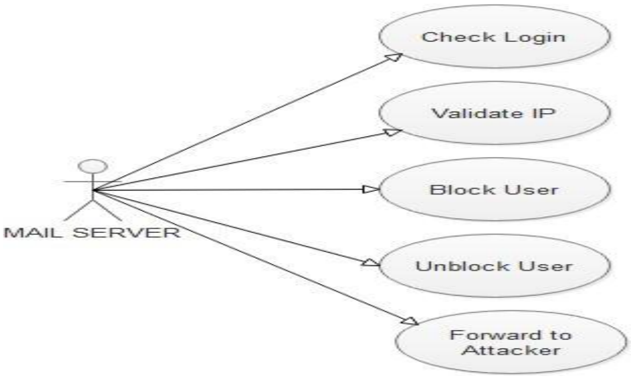

Fig4: Sequence diagram of Mail User

Fig 4: A Mail User is **for receiving email**. Since a Mail User is for redirecting email to an external address, that external address is usually where they would send email from.

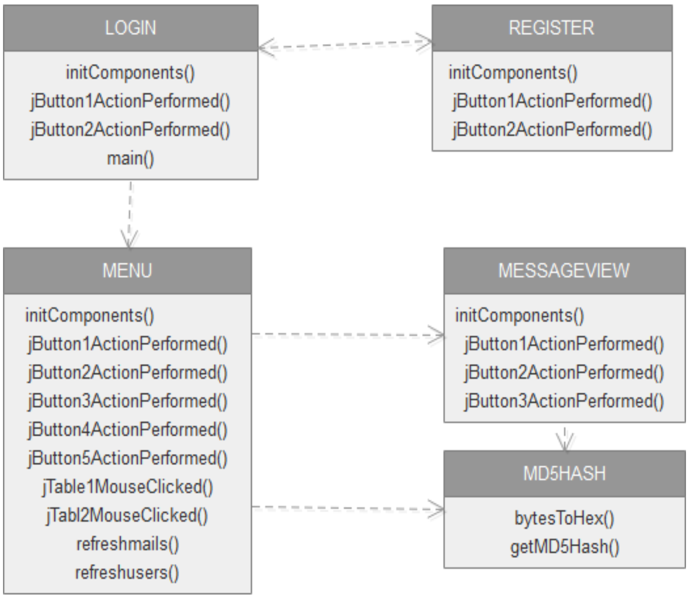
LOGIN
initComponents()
jButton1ActionPerformed()
jButton2ActionPerformed()
main()
REGISTER
initComponents()
jButton1ActionPerformed()
jButton2ActionPerformed()
MENU
initComponents()
jButton1ActionPerformed()
jButton2ActionPerformed()
jButton3ActionPerformed()
jButton4ActionPerformed()
jButton5ActionPerformed()
jTable1MouseClicked()
jTabl2MouseClicked()
refreshmails()
refreshusers()
MESSAGEVIEW
initComponents()
jButton1ActionPerformed()
jButton2ActionPerformed()
jButton3ActionPerformed()
MD5HASH
bytesToHex()
getMD5Hash()

Fig 5:Class diagram of Mail Server

Fig 5: A Communication between Mail server and the Register and Menu part in the Project.

4. CONCLUSIONS

In this article, we have described the development of a allow list generation method by detecting forwarded mail using sender authentication technology and extracting legitimate mail servers from this forwarding source.

This method focused on forwarded emails, assumed the sender was a legitimate email sender to receive, and offered a method to collect legitimate email senders. Also, in this improvement method, we have introduced a procedure to exclude spam sources that should not be included from legitimate email sources. It has been shown that erroneous judgments can be reduced by applying this optimization method to actually received e-mails, whether it is effective or not. From these results, we were able to show that our improvement method was effective..

REFERENCES

[1] Nidhi Tomar, Amit Kumar Manjhvar, "An improved optimized clustering technique for crime detection", in symposium on colossal data analysis and networking(CDAN) 2016.

[2] Peng Chen, Justin Kurland, "Time, place and modusoperandi:A simple apriori algorithm for crime patterndetection",2018.

[3] Shyam Varan Nath, "Crime pattern detection using data mining", oracle corporation 2017.

[4] Chung-Hsien Yu1, Max W. Ward1, Melissa Morabito2, and Wei Ding, " crime forecasting using data mining technique", Department of Computer Science, 2Department of Sociology, University of Massachusetts Boston, 100 Morrissey Blvd., Boston, MA 02125-2018.

BIOGRAPHIES

KAVYA R
ASSISTANT PROFESSOR
VVIET CLG
MYSORE-570028

JAYANTH PB
VVIET CLG
MYSORE-570028

POOJA P
VVIET CLG
MYSORE-570028

JAYANTH KOWSHIK
VVIET CLG
MYSORE-570028

SUSHMITHA MH
VVIET CLG
MYSORE-570028