ISSN 2278-3091
Volume 10, No.2, March - April 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse271022021.pdf
https://doi.org/10.30534/ijatcse/2021/271022021

A Secure Methodology for Filtering Spam & Malware in E-mail System and Secure E-mail Testbed Setup

Sanjay Adiwal, Akanksha Gupta, Balaji Rajendran, B S Bindhumadhava
Centre for Development of Advanced Computing (C-DAC)
Bangalore, INDIA, {sanjayadiwal, akankshag, balaji, bindhu}@cdac.in

ABSTRACT

E-mail system is one of the critical infrastructures of any organization. It is necessary to ensure that the mail servers in use should be secured in such a way that no security properties like confidentiality, integrity, and authenticity are compromised. To achieve these security properties we have setup a secure e-mail server testbed that provides security against malware and spam, and guaranties secure e-mail delivery.

This paper proposes a secure methodology for filtering spam and malware in the e-mail system, comprising standard layers of protocols and policies. An experimental testbed is established to evaluate the effectiveness of our methodology and was tested with spam and malware e-mails. Our results showed an accuracy of 95 percent, against a typical configuration of an e-mail system.

Key words : E-Mail Security, E-Mail Testbed Setup, Proxmox, DNS, SMTP.

1. INTRODUCTION

Traditional e-mail server works on the Simple Mail Transfer Protocol, a broadly deployed and primitive protocol that authenticates and directs the transfer of e-mail, which does not characterize any privacy and security policy. As a result, in e-mail inward threats come in the shape of malware, spam, spyware and phishing e-mail that redirect users to malicious websites, e-mail exploits, phishing scams and so on [3]. Outward threats are Eavesdropping, spoofing, replying & forwarding issues, carbon copy (cc) & blind carbon copy (bcc) issues and malicious e-mail attachments. Although several add-on protocols like S-MIME, TLS, SSL, and other protocols have been evolved to make e-mail transactions more secure and private [8], still the compromise rate is not greatly reduced.

The typical e-mail threats are viruses, malware, spyware, spam e-mail that redirect users to phony websites, e-mail exploits, phishing scams, and so on. To make the communication more secure, a secure e-mail server testbed was implemented which includes all open source software's like postfix & sendmail for mail servers, squirrelmail & rainloop for mail user agent, dovecot for mail delivery agent. We have also used proxmox mail gateway, clamav open-source antivirus and anti-spam software like spamassassin / amavisd to address viruses, worms, spam, and other malwares.

The remainder of this paper is organized as follows: The next section illustrates related work and publications in-person recognition, detailing the various methodologies implemented to secure e-mail infrastructure. Section 3 covers the basic introduction to the e-mail system. The implementation part of the testbed is listed in section 4, this section also details the testbed setup for two different domains and Proxmox deployment. Section 5 explains the experimental results obtained and section 6 concludes our paper with future work.

2. RELATED WORK

SMTP is the most widely deployed and tested in different organizations across the world and is a primary protocol for e-mail transfer [7]. SMTP servers usually communicate through TCP port 25. The main objective of SMTP is to exchange e-mail messages efficiently, easily and reliably. The traditional SMTP protocol doesn't authenticate the user's identity which makes it vulnerable to spoofing attacks [11]. It does not define any security features like privacy (i.e. sniffing), authentication of sending party (i.e. spamming), the integrity of e-mail message (i.e. man in the middle), non - repudiation and consistency of e-mail envelope (i.e. e-mail spoofing).

To make e-mail conversations more secure and private, several add-on protocols and procedures have been developed. For e-mail security, several solutions are proposed in recent past years.

In his research paper titled "Designing secure e-mail infrastructure" [1], Dharmerndara Choukse explained inherent weakness in e-mail infrastructure and methodologies to improve the security of the e-mail infrastructure and also highlighted good and weak practices in varying aspects of

e-mail infrastructure design.

In his research work titled "Secure Email Gateway" [2], Khandu Om presented a methodology to implement a secure e-mail gateway for incoming e-mail, which checks filtering of URL and defends against spam, malware, and phishing. He focused on mainly three components i.e. e-mail security and content control, URL verification and filtering, e-mail content and attachment access rights management. The challenges and ethical issues were also highlighted.

Suresh Kumar Balakrishnan [4] presented a practical oriented secure e-mail system that uses certificateless public key cryptography and DNS as the mechanism to publish a user's public key server address. DNS is used for infrastructure for public key exchange and a secure key token/fingerprint authentication system for user authentication.

In their survey paper titled "A Survey of Email Service; Attacks, Security Methods and Protocols", Haider M Al Mashhadi [9] discussed and presented various e-mail threats, vulnerabilities, and different approaches to secure e-mail service. E-mail threat includes eavesdropping, identity theft, message modification, false messages, unprotected backups, repudiation, e-mail spoofing, spamming, e-mail bombing, etc.

3. ELECTRONIC MAIL SYSTEM

Electronic mail (e-mail) allows exchanges of messages between electronic devices over global network i.e. Internet. In traditional early e-mail systems both the sender and the receiver were required to be online at the same time, in common with instant messaging [6]. The current e-mail scheme is using a store-and-forward model i.e. the e-mail servers forwards, accepts, delivers, and stores e-mail. The users of the e-mail need not be online always; they typically connect to an e-mail server through the web interface and receives or send messages.

3.1 COMPONENTS OF E-MAIL SYSTEM

There are three basic components in the working of an e-mail system as shown in Figure1.

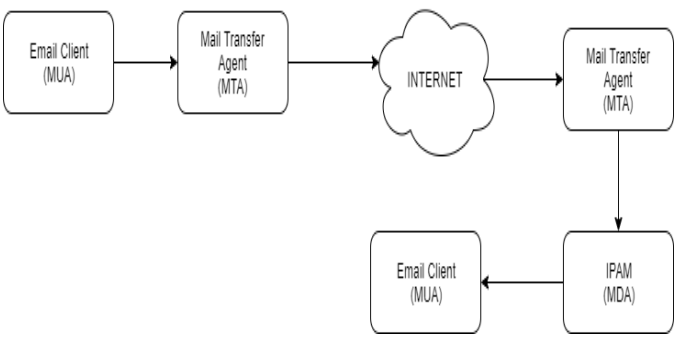

Figure 1: Basic components of an e-mail system

3.1.1 MAIL USER AGENT

Mail user agent (MUA) is an interface between the user and the SMTP server. It helps the user to read and write e-mail messages. MUA is also called as e-mail client software. The examples of MUA are: Mozilla Thunderbird and Microsoft Outlook. The webmail interface can also be treated as an MUA e.g. www.gmail.com, mail.yahoo.com. MUA software transforms a simple text message into the appropriate Internet format for the message to reach its destination.

3.1.2 MAIL TRANSFER AGENT

Broadly and historically, any program that exchanges e-mail between electronic devices is a mail transfer agent (MTA). Typically MTA is responsible for transferring e-mail messages from the source to destination. Any application which runs SMTP is an MTA. Postfix and Sendmail are examples of MTA.

3.1.3 MAIL DELIVERY AGENT

Mail delivery agent (MDA) is an application that receives messages from MTAs and delivers them to the mailbox of the recipient at the SMTP server. The recipient accesses the e-mail in their mailbox using a MUA. IMAP (Internet Message Access Protocol specified in RFC 3501) and POP3 (Post Office Protocol - Version 3 specified in RFC 1939) are the common protocols for MDA.

3.2 WORKING OF E-MAIL

The e-mail system follows client server architecture, where client is the mailer typically a MUA and server is running a SMTP service. The basic steps involved in sending and receiving e-mails are as follows:

1. The MUA (client on the sender side) creates the properly formatted mail which is sent to an MTA in the background.
2. MTA's can vary in number so it will be routed until the e-mail is on a 'boundary MTA' on the receiver end.
3. The boundary MTA performs a query using DNS to identify the MX (Mail Exchanger Record) for the domain the e-mail is intended for.
4. The MTA connects to the MX and transfers the e-mail.
5. The MX transfers the e-mail to the inbox of the user.
6. At this point, the e-mail is transferred to the appropriate internal mail server and stored until the MDA connects to it and retrieves the e-mail on behalf of the user usually using the POP or IMAP protocols.

4. EXPERIMENT SETUP OF SECURE E-MAIL TEDBED

The secure e-mail testbed setup is implemented for two different domains i.e. "coe.in" and "dnscoe.in". Figure 2 illustrates the implementation architecture of secure e-mail communication setup using Proxmox [13] and other open-source software.

Centos7.6 is used as a platform for implementation for DNS server and E-mail Server applications.

The secure e-mail testbed setup comprises of different open source applications as shown in Table 1, i.e. Sendmail and Postfix for SMTP server, Squirrelmail and Rain-loop as e-mail client and Dovecot for delivery of an e-mail to the mail clients. On top of the MTA, antivirus and anti-spam software are installed to detect malware infected e-mail and spam. To secure e-mail communication between two domains “coe.in” and “dnscoe.in”, a Proxmox mail gateway is hosted between the two MTA.

Table 1 : List of open source applications used in secure e-mail testbed.

Domain Name	Mail Server	MUA Application	Antivirus	Antispam
coe.in	Sendmail [14]	SquirrealMail [21]	ClamAV [16]	Spamassassion [17]
dnscoe.in	Postfix [19]	RainLoop [15]	ClamAV	Amavisd [18]

4.1 DNS SERVER SETUP FOR SECURE E-MAIL (“COE.IN” AND “DNSCOE.IN”)

Domain Name System - DNS is the critical infrastructure of the e-mail echo system. All devices that are connected to the Internet are identified by a unique number called IP address. Humans can easily remember domain names as compared to the IP addresses. Prior to DNS, computers used a simple text file called a “hosts” file, located in /etc directory that mapped hostnames to IP addresses. As the host file is local to a single computer, in order to maintain a centralized hosts list and their corresponding domains, DNS came into existence.

For secure e-mail testbed setup, an authoritative DNS server for two domains “coe.in” and “dnscoe.in” has configured. Two zones “coe.in and “dnscoe.in” are declared in the main configuration file (named.conf) of bind DNS Server.

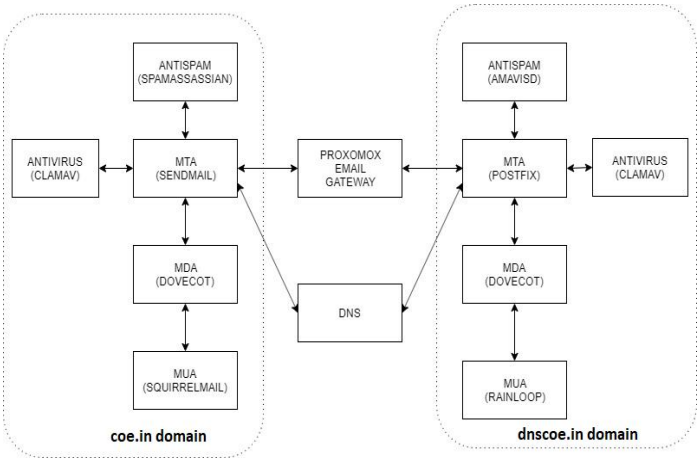

Figure 2 : The architecture of a secure e-mail testbed.

/etc/named.conf

```
zone "coe.in" IN {
        type master;
        file "coe.in.zone";};

zone "dnscoe.in" IN {
        type master;
        file "dnscoe.in.zone";};
```

To configure zone for “coe.in” domain, the zone file is created as follows:

/var/named/coe.in.zone

```
coe.in.    3600  IN   SOA   coe.in.   root.coe.in.
(20191231 86400 900 691200 86400);
coe.in.          3600 IN   NS    ns.coe.in.
www.coe.in.      3600  IN   A     10.182.0.11
coe.in.          3600 IN   MX    10  mail.coe.in.
mail.coe.in.     3600  IN   A     10.182.1.216
ns.coe.in.       3600  IN   A     10.182.0.11
```

The zone file for “dnscoe.in” zone is as follows:

/var/named/dnscoe.in.zone

```
dnscoe.in.  3600  IN   SOA   dnscoe.in. root.dnscoe.in.
(20191231 86400 900 691200 86400);
dnscoe.in.       3600 IN   NS    ns.dnscoe.in.
www.coe.in.      3600 IN   A     192.168.100.2
dnscoe.in.       3600 IN   MX    10  mail.dnscoe.in.
mail.dnscoe.in.  3600  IN   A     192.168.100.1
ns.coe.in.       3600  IN   A     10.182.0.11
```

4.2 SECURE E-MAIL SETUP FOR “COE.IN” DOMAIN

The first part of the testbed is to configure and deploy secure e-mail setup for “coe.in” domain. The deployment includes installation and configuration of sendmail server, dovecot, squirrelmail webmail client, clamav antivirus and spmassassion. To resolve the MX records of “coe.in” and “dnscoe.in” domains a DNS server is implemented locally as in section 4.1. Centos-7 is the base operating system used for “coe.in”.

4.2.1 SENDMAIL INSTALLATION AND CONFIGURATION FOR “COE.IN” DOMAIN

Sendmail is an MTA, which is the most popular and powerful mail server on the Internet that delivers almost 70 percent of all e-mail messages on the Internet [12]. Most of its configuration files can be found under the /etc/mail/ directory.

The following changes were made in sendmail macro configuration file (sednmail.mc) for "coe.in" domain:

/etc/mail/sendmail.mc

```
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1,
Name=MTA')dnl
   FEATURE(`relay_hosts_only')dnl
```

The commands used to generate main configuration file (sendmail.cf) is:

```
#cd /etc/mail
#m4 sendmail.mc > sendmail.cf
```

4.2.2 DOVECOT INSTALLATION AND CONFIGURATION FOR "COE.IN" DOMAIN

Dovecot is the most popular IMAP and POP3 server for Linux/UNIX-like systems. Mail is delivered to the server using a MDA or Dovecot itself can act as MDA and stored for later access with MUA. The dovecot is installed for "coe.in" domain and following changes are made in dovecot configuration files:

/etc/dovecot/dovecot.conf

```
protocols = imap pop3 lmtp
```

/etc/dovecot/conf.d/10-auth.conf

```
disable_plaintext_auth = no
```

/etc/dovecot/conf.d/10-mail.conf

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

4.2.3 SQUIRRELMAIL INSTALLATION AND CONFIGURATION FOR "COE.IN" DOMAIN

Squirrelmail is written in PHP that provides both a web-based e-mail client and a proxy server for the IMAP protocol. The web server needs access to the IMAP server hosting the e-mail and to an SMTP server to be able to send mails. The prerequisite for squireelmail is the apache web server. After installation of apache, squirrelmail is installed and configured using the following commands:

```
#cd /usr/share/squirrelmail/config/
# ./conf.pl
```

The configuration of squirrelmail asks organization details, imap server and smtp server details.

4.2.4 ANTIVIRUS(CLAMAV) INSTALLATION AND CONFIGURATION FOR "COE.IN" DOMAIN

Clamav is an open-source antivirus application, which can detect almost all types of malware. The clamav antivirus is available in the epel repository for centos 7. The main configuration file is freshclam.conf, and has to be modified as follows:

/etc/freshclam.conf

```
UpdateLogFile /var/log/freshclam.log
LogTime yes
```

Installed clamav and updated fresh pattern files using following commands.

```
#freshclam
#clamscan --infected --remove --recursive /home
```

Modified scan.conf file as follows and started clamav antivirus service.

/etc/clamd.d/scan.conf

```
PidFile /var/run/clamd.scan/clamd.pid
TemporaryDirectory /var/tmp
LocalSocket /var/run/clamd.scan/clamd.sock
```

4.2.5 ANTI-SPAM (SPAMASSASSIN) INSTALLATION AND CONFIGURATION FOR "COE.IN" DOMAIN

Spamassassin is an anti-spam application for filtering spam from an incoming e-mail. Spamassasain has been installed for "coe.in" and the following changes have been made in the main configuration file where e-mail will be identified as spam with a score is 6 and above and then the header of the e-mail will be rewritten as "IdentifiedasSPAM".

/etc/mail/spamassassin/local.cf

```
required_hits 6
rewrite_header Subject [IdentifiedasSPAM]
```

To run spamassassin for inbound e-mail, the following changes have been added in sendmail.mc file and sendmail service restarted.

/etc/mail/sendmail.mc

```
INPUT_MAIL_FILTER( `spamassassin', `
S=unix:/var/run/spamass.sock, F=,
T=C:15m;S:4m;R:4m;E:10m ')dnl
```

4.3 SECURE E-MAIL SETUP FOR "DNSCOE.IN" DOMAIN

The second part of the testbed is to configure and deploy secure e-mail setup for "dnscoe.in" domain. The deployment includes installation and configuration of the postfix mail server, dovecot, rainloop webmail client, clamav antivirus and amavisd applications.

4.3.1 POSTFIX INSTALLATION AND CONFIGURATIONS FOR "DNSCOE.IN" DOMAIN

Postfix is widely deployed most popular among the other SMTP server. The postfix is installed and configured for "dnscoe.in" domain, most of its configuration files can be found under the /etc/postfix/ directory. The postfix configuration file (main.cf) for "dnscoe.in" domain is as follows:

/etc/postfix/main.cf

```
myhostname = mail.dnscoe.in
mydomain = dnscoe.in
myorigin = $mydomain
inet_protocols = all
mydestination = $mydomain
mynetworks = 192.168.100.0/24,
home_mailbox = Maildir
```

4.3.2 DOVECOT INSTALLATION AND CONFIGURATIONS FOR "DNSCOE.IN" DOMAIN

The dovecot is installed for "dnscoe.in" and made following changes in dovecot configuration files:

/etc/dovcot/dovecot.conf

```
protocols = imap pop3 lmtp
```

/etc/dovecot/conf.d/10-auth.conf

```
disable_plaintext_auth = no
```

/etc/dovecot/conf.d/10-mail.conf

```
mail_location = maildir:~/Maildir
disable_plaintext_auth = yes
auth_mechanisms = plain login
```

4.3.3 RAINLOOP INSTALLATION AND CONFIGURATIONS FOR "DNSCOE.IN" DOMAIN

Rainloop is a modern web-based e-mail client software. It was mainly designed for low-end web servers. It also allows for working in secure mode with mail servers using SSL and STARTTLS protocols which includes client-side OpenPGP and two-factor Authentication. Apache webserver is needed for rainloop. After installation of apache, rainloop e-mail client is installed and configured with the following configuration settings:

IMAP Settings

```
IMAP Server: coe.in
Port: 143
```

SMTP Settings

```
SMTP Server: mail.dnscoe.in
Port: 25
```

4.3.4 ANTIVIRUS(CLAMAV) INSTALLATION FOR "DNSCOE.IN" DOMAIN

The clamav antivirus application is installed for "dnscoe.in" domain as mentioned in section 4.2.4.

4.3.5 AMAVISD INSTALLATION AND CONFIGURATION FOR "DNSCOE.IN" DOMAIN

Amavisd is an interface between SMTP servers and content filters like malware applications and anti-spam applications which protects against malware and spam threats. Amavisd is installed for "dnscoe.in" with the following modifications in the main configuration file (amavisd.conf) of amavisd.

/etc/amavisd/amavisd.conf

```
$mydomain = 'dnscoe.in';
$myhostname = 'mail.dnscoe.in';
```

main.cf file of postfix has modified as follows.

/etc/postfix/main.cf

```
content_filter=smtp-amavis:[127.0.0.1]:10024
```

postfix configuration file (master.cf) has modified as follows:

/etc/postfix/master.cf

```
smtp-amavis unix -    -    n    -    2 smtp
127.0.0.1:10025 inet n    -    n    -    - smtpd
```

4.4 PROXMOX MAIL GATEWAY DEPLOYMENT FOR "DNSCOE.IN"

The proxmox mail gateway is a single application that provides defense against malware and spam. It is the leading and well-known open-source email security software serving organization to protect their e-mail server against all email

threats including RAT, Trojans, viruses, phishing and spam. It is easy to configure with its user-friendly web interface, which allows user to manage all inbound and outbound e-mails to protect from malware, spam, phishing, and trojans.

The proxmox gateway is installed for “dnscoe.in” for incoming as well as outgoing e-mail. E-mail traffic for “dnscoe.in” domain is forwarded to the proxmox gateway which filters the entire e-mail traffic and removes e-mails threats. The IP address of proxmox is announced as an e-mail exchanger (MX record) for “dnscoe.in”. All incoming mail for “dnscoe.in” will reach to proxmox first and then it will forward to SMTP server of “dnscoe.in”. The same is applied for an outgoing e-mail from “dnscoe.in”. The proxmox runs on TCP port numbers 25 and 26, 25 is used for all incoming e-mails and 26 used for an outgoing e-mail as shown in Figure 3.

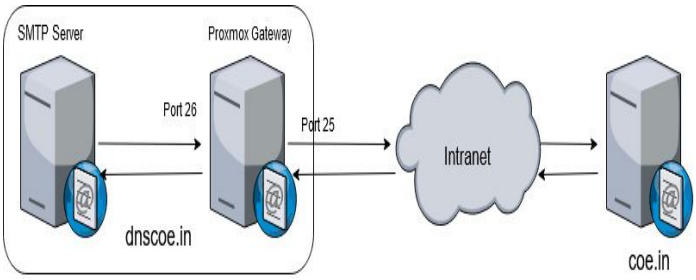

Figure 3 : Proxmox mail gateway deployment for secure e-mail testbed

5. TESBED EVALUATION AND RESULT

The secure e-mail testbed implemented in section 4, is tested by sending malware and spam e-mails between “coe.in” and “dnscoe.in” domains. The experiment is conducted by sending approximately 1000 spam e-mail using various command-line tools (mail, mailx etc.) [10] and over 100 malware attached e-mails, the malware was created by the metasploit framework (msfvenom) [20] and some malware was downloaded from various known sources [22] [23].

The proxmox mail gateway was able to detect approximately 90% of spam e-mail and 95% of malware e-mail. Approximately 50% spam e-mail among 10% false positive by proxmox, was detected by amavisd.

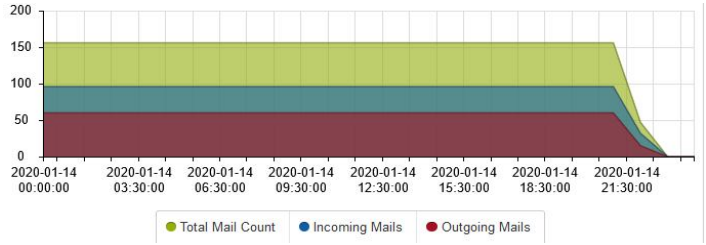

Figure 4 : Plot showing malware detected e-mail from all incoming e-mail on a single day

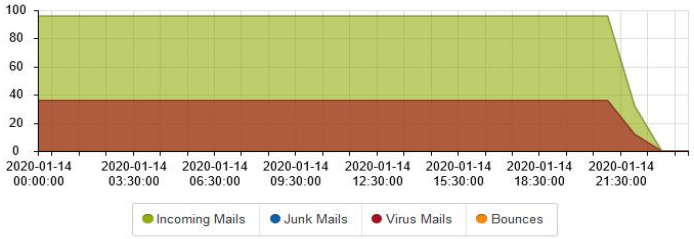

Figure 5 : Plot showing total e-mail count including incoming and outgoing e-mail on a single day

Proxmox mail gateway detected malware attached e-mails sent from an internal host as well as from incoming e-mail for “dnscoe.in” domain as shown in Figure 4. The incoming, outgoing and total e-mail count is shown in Figure 5.

6. CONCLUSION AND FUTURE WORK

The main objective and primary outcome of this paper is to protect e-mail infrastructure from being exploited in e-mail compromise attacks, phishing e-mails, e-mail scams, and other cyber threat activities. It also gives the ability to protect a domain from unauthorized use, commonly known as e-mail spoofing, thus to provide a complete e-mail server protection. This paper presented a secure methodology for filtering spam and malware in an e-mail system through a testbed setup that includes all open source software’s to address viruses, worms, spam, and e-mail threats. Our results showed better accuracy, against a typical configuration of an e-mail system.

The future work can be implementing DMARC authentication protocol which is a combination of two existing technologies namely as SPF and DKIM which prevents SMTP servers from being abused [5].

ACKNOWLEDGEMENT

We thank “Internet Governance Division of Ministry of Electronics & Information Technology (MeitY)” and “National Internet Exchange of India (NIXI)” for their support in this research work.

REFERENCES

1. D. Choukse, U. K. Singh, L. Laddhani and R. Shahapurkar. **Designing secure e-mail infrastructure,** in *Proc. 2012 Ninth International Conference on Wireless and Optical Communi-cations Networks (WOCN)*, Indore, pp. 1-9, 2012.
2. K. Om. **Secure e-mail gateway**, in *Proc. IEEE International Conference on Smart Tech-nologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, Chennai, pp. 49-53, 2017.
3. Fatima Aziz Rawdhan, Mahmood KhalelIbrahim. **Enhancement of E-mail Security Services**,

International Journal of Scientific & Engineering Research, Volume 8, Issue 1, 2017.

4. Suresh Kumar, Balakrishnan and V. P. Jagathy Raj. **Practical Implementation of a Secure Email System Using Certificate less Cryptography and Domain Name System**, *International Journal of Network Security*, Vol.18, No.1, PP.99-107, 2016.
5. M. H. Jalalzai, W. B. Shahid and M. M. W. Iqbal. **DNS security challenges and best practices to deploy secure DNS with digital signatures.** in *Proc. 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, Islamabad, pp. 280-285, 2015.
6. G. Liyanage and S. Fernando. **A comprehensive secure email transfer model**, in *Proc. IEEE International Conference on Industrial and Information Systems (ICIIS)*, Peradeniya, pp. 1-5, 2017.
7. Klensin, J., Ed. **Simple Mail Transfer Protocol**, *RFC 2821*, DOI 10.17487/RFC2821, https://www.rfc-editor.org/info/rfc2821(2001).
8. T. Ayodele, C. A. Shoniregun and G. A. Akmayeva. **Security review of email summarization systems**, in *Proc. World Congress on Internet Security (WorldCIS-2011)*, London, pp. 269-271, 2011.
9. Haider M Al-Mashhadi, Mohammed H.Alabiech. **Survey of Email Service; Attacks, Security Methods and Protocols**, in *Proc. International Journal of Computer Applications (0975 –8887)* Volume 162 –No 11, 2017.
10. SPAM Archive Homepage, http://untroubled.org/spam/, last accessed 2021/02/28.
11. Afnan S. Babrahem, Eman T. Alharbi, Aisha M. Alshiky, Saja S. Alqurashi and Jayapra-kash Kar. **Study of the Security Enhancements in Various E-Mail Systems**, *Journal of Information Security*,6,1-11, 2015.
12. C. Partridge. **The Technical Development of Internet Email**, *IEEE Annals of the History of Computing*, vol. 30, no. 02, pp. 3-29,2008.
13. Proxmox Homepage, https://www.proxmox.com/en/, last accessed 2021/01/29
14. Sendmail Homepage, https://www.proofpoint.com/us/products/open-source-email-solution, last accessed 2021/01/30.
15. Rainloop Homepage, https://www.rainloop.net, last accessed 2021/02/22
16. Clamav Homepage, https://www.clamav.net, last accessed 2021/02/23
17. Spamassassin Homepage https://spamassassin.apache.org/, last accessed 2021/02/24
18. Amavisd Homepage, https://www.ijs.si/software/amavisd/, last accessed 2021/02/26
19. Postfix Homepage, http://www.postfix.org/, last accessed 2021/02/21
20. Msfvemon Homepage, https://www.offensive-security.com/metasploit-unleashed/msfvenom/, last accessed 2021/02/11
21. Squirrelmail Homepage, https://squirrelmail.org/, last accessed 2021/02/11
22. Lenny Zeltser, Free Malware Sample Sources for Researchers Homepage https://zeltser.com/malware-sample-sources/, last accessed 2021/02/11
23. Contagio malware dump Homepage, http://contagiodump.blogspot.com/, last accessed 2021/02/28