Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

# Legalistic Evaluation of E-Mail Headers Based on Address Spoofing

[1]Ramakant Upadhyay , [2]Chetan Kumar

[1]*MTech Scholar, Dept. of Computer Science & Engineering*
*Kautilya Institute of Technology & Engineering Jaipur-Rajasthan – India*

[2]*Associate Professor, Dept. of Computer Science & Engineering*
*Kautilya Institute of Technology & Engineering Jaipur-Rajasthan – India*

**Abstract—** *in this new era of digital world, E-Mail is a communication medium and extensively used, fast & cheap way of message transfer over the internet world. After all, mail is not completely safe & reliable medium due to technically alternate loopholes in protocols which able to culprits to make mistreat it especially to send spoofed E-Mails which is recently large scale problem to handle for mail systems now days. E-Mail sender address spoofing is malicious action where the origin address are changed and presented as it is coming from expected sender but the real sender is an assaulter. In this paper, we present behavior of several mail applications during receiving the sender address spoofed mails. We recommend sender spoofing analysis algorithm to check sender spoofing in mails through performing comprehensive header evaluation on mail header fields. We generally focused on four fields like R-SPF, DKIM, DKIM Signature and DMARC. This proposed algorithm checks the valid values of the headers. Any non valid value shows towards unauthorized mails. We have also created data values of legitimate and spoofed mails and implemented the evaluations on mail headers for valid and invalid values. Our proposed approach and algorithm is capable to detect sender spoofing especially sender spoofed mails.*

***Keywords—****E-Mail Evaluation, Mail Sender Spoofing, R-SPF, DKIM, DMARC, Header Analysis.*

## I. INTRODUCTION

E-Mail is the communication process and application platform to use widely by user on the internet. Now days it has become a regular part in every corporate, business and organization for message spread fast and cheaply every day. So to send this safely more secure steps are mandatory to make safe and reliable this. E-mail accounts are growing day by day. According to the radicati group study of market, the total 3.7 billion mails account will be in 2017 as both corporate and consumer users. As per the group static executive report 2017-2021, the total emails sent and received per day is 269 billion for both users in 2017 and is expected to grow 4.4 % average annual rate in the next four years and reaching 319.6 billion till 2021. The table is as follows:

| Daily Mail Traffic | **2017** | **2018** | **2019** | **2020** | **2021** |
|---|---|---|---|---|---|
| Total Mail Sent/Received Worldwide | 269.0 | 281.1 | 293.6 | 306.4 | 319.6 |
| Growth (%) | 4.4 | 4.5 | 4.4 | 4.4 | 4.3 |

Table 1 Worldwide Daily E-Mail Traffic over 2017-2021 [9]

Fraud Reports of RSA 2013 says, India arrived as the top country in Asia-pacific region in terms of phishing attack through volume closed followed by China and Australia. Approximated India`s loss from phishing attack stood at $225 Million. Universally, loss due to phishing attacks was $5.9 billion, which is somewhat higher than $1.5 billion loss in the year of 2012. The total number of phishing attacks stood at Rs 448,126 in 2013 and Rs 445,004 in 2012 [8]. According to mcafee report 2017, for the security reasons that evasion approach to ensure that security technologies remain executable.

 

Evasion approach use by malware, anti –sandbox 23.3%, anti security tools 21.2%, code injection 21.1%, anti debugging 16.1%, anti monitoring 18.3% [10]. As per report of Semantic Corporation 2017 ISTR vol. 22, about ransomware number of detection in 2016 is 463841 and ransom amount is $1077 and overall malware are in 1 in 131, Phishing rate 1in 2596, span overall rate is 53% in comparison of previous years [4].

E-Mails are normally encoded in American Standard Code for Information Interchange (ASCII) text format. In spite of, you can also send non-text files, like sound files and graphic images, as attachments sent in binary flow E-Mail is one kind of the protocols comprised with the Transport Control Protocol/Internet Protocol (TCP/IP) suite of protocols. Spoofing is an approach used by spammers and scammers using with phishing to hide the actual source of a Mail Message. By modifying the some properties of the E-Mail, such as the `From`, `Return Path` and `Reply- To` fields (They are presents in E-Mail Header), `Date`, these culprits can make the Mail appear to be from someone other than the real sender. There are so many E-Mail clients software like Microsoft outlook, Gmail inbox, Mozilla thunderbird, windows live mail, eM client, outlook express are used to send the mails to receiver with the message body.

E-Mail spoofing is of two types are as follows. First is Date & Time Spoofing where criminals may change the date which is either before or ahead in the 'Date' field under mail header. An attacker may also modify the time at which the E-Mails were sent. This time field may be few seconds, nano seconds, milliseconds or micro second before or later from the specified time and second is Address spoofing where sender address is completely modified and sent to intended receiver where the receiver will think about the sender that this sender domain is legitimate. In sender address spoofing, attackers may use fake way to attack i.e. friend may send a mail for making joke, one Govt. department employee may send a wrong mail to our colleague for suspension, one student may treat to our faculty. They may also send a mail to reveal information from IB, CBI, NSA, and National Investigation Agencies etc. This paper recommends an algorithm to detect spoofed mails especially address spoofed and real origin of the source. This algorithm coded in java Mail API, Eclipse Tool, which takes few header values as a input like M-ID, RSPF, DKIM, DKIM Signature, and DMARC to investigate further and result out that mail is spoofed or not.

In the reaming part of paper, second part elaborates mail sender address spoofing that how the source address can be spoofed. The Spoofed header is also discussed in deep. After execution, results shows that how the mail is detect as spoofed which is sent by several mail servers. Third part is related work concern. Fourth part discusses about experimental work which result out by proposed detection method and the rest part in totally about conclusion and further scope and future work and enhancement regarding the same.

## II. E-MAIL SENDER ADDRESS SPOOFING

The E-Mail is address spoofed where it is not sent by the corporate/persons or organization while sent by other domain meanwhile the illegal sender is clamming it that E-Mail is genuine and sent by genuine sender. In spoofed mail received field , the displaying name of email sender is not same as the original sender of that email. We have sent few selected mail in our laboratory for forensic analysis and result are given in below figure.


Fig.1 Sender Address Spoofed E-Mail

 

In Fig. 1, this is also a spoofed mail. E-Mail is sent from icrb@isro.gov.in to upadhyay.thesis@aol.com but basically The E-Mail is not sent by icrb@isro.gov.in, it is sent by fake domain mail server, namely www.sharpmail.co.uk where address is going to be spoofed. So finally E- Mail is looking like that it is coming from the original sources of sender meant that coming from icrb@isro.gov.in

Address spoofing may performed using several ways. First is using by fake domain sites where mail can sent by any fake mail ID or by any person name or by organization name or by any domain name whether it exist or does not meant that from field of head may changed by criminals or attackers. In this paper this way is used to send fake mails. Second one is to configure own self SMTP server machine. Third way is to send mails through open relay E-Mail server.

To evaluate the nature and behavior of sender address spoofed E-Mails. We have sent an E-Mail from icrb@isro.gov.in (ISRO Centralized Recruitment Board) to upadhyay.thesis@gmail.com but here it is not sent by icrb@isro.gov.in while sent by http://www.sharpmail.co.uk and its mail server address is pache@main.dannix.co.uk as such in the mail header return path is also pache@main.dannix.co.uk. So in Fig. 2, header fields are extracted and the detailed description of these fields is as follows:

**Delivered-To**: - this header field value is the predetermined receiver E-Mail address.
**Received:** - this field indicates the last server information from where Email is received. Here Email is received by SMTP server having IP address 10.103.115.5 of server machine at Thu, 31 Aug 2017
03:40:17 -0700 (PDT). Clock time is 7(seven) hours behind the GMT (Greenwich Mean Time).

**X-Received:** - meant that mail is received by SMTP server having IP address 10.28.234.2 at Thu, 31
Aug 2017 03:40:17 -0700 (PDT) from main.dannix.co.uk, which is a fake (not genuine) mail server domain in that case and using for sending spoofed mail. Fig 3.2 shows the route traversed by the E- Mail from sender (icrb@isro.gov.in) to receiver (upadhyay.thesis@gmail.com) with a specific path. **Return-Path:** - meant that field must be ISRO Centralized Recruitment Board <icrb@isro.gov.in>
here but fake mailer sender/attacker modified it as pache@main.dannix.co.uk

**Received field:** - means the server name & ID of next server in route, which is receiving the E-Mail. **Received-SPF:** - R-SPF is "pass" here, it means that the domain of apache@main.dannix.co.uk has an IP address 213.171.197.232, is an permitted sender designated by Sender policy Framework (SPF)
based on own security checks.

**Authentication-Results:** - meant that the field SPF is "pass" with IP allocated as 213.171.197.232 which is the indication of authentic and **DMARC** field value is "Fail" which showing that the server machine is not genuine.
**DKIM:** - this field is absent which indicate that sent mail is spoofed E-Mail, as such given in the above example.
**DKIM-Signature:** - in that case this field is absent meant that this mail may be spoofed and send by fake mail server machine.

**From:** - meant that this field is spoofed here in this case; basically E-Mail is sent by pache@main.dannix.co.uk while not dent by ISRO Centralized Recruitment Board <icrb@isro.gov.in>
**M-ID:** - known as Message ID, meant that this is the server name of sending E-Mail that is pache@main.dannix.co.uk .MID is an combinations of alphabets & numeric characters
**MIME-Version, Content-Type, Content-Transfer-Encoding** meant that these values show the MIME version number i.e. 1.0, type of contents and type of content encoding for transfer. Further, Mail can be properly decoded at receiver end by Mail User Agent.

**X-COMPLAINTS:** - meant that it shows message fixed by fake mailer and fake URL domain. it is trying to make fool to the user that after to show the message " to report abuse please mail" at abuse@sharpmail.co.uk meant that it wants to show that this is real mail domain.
**Subject:** - it displays the content which is used to make as title for particular E-Mail i.e. ISRO Head Quarter for Joining as a Scientist.

**ARC Seal, ARC Message Signature, ARC Authentication result:** - meant that these are the authentication parameters used to validate the E-Mails with their separate properties.

 

```
Delivered-To: upadhyay.thesis@gmail.com
Received:     by 10.103.115.5 with SMTP id o5csp2363225vsc;Thu, 31 Aug 2017 03:40:17 -0700
              (PDT) X-Received: by 10.28.234.2 with SMTP id i2mr243120wmh.80.1504176017145;
              Thu, 31 Aug 2017 03:40:17 -0700 (PDT)
ARC-Seal:     i=1; a=rsa-sha256; t=1504176017; cv=none;d=google.com; s=arc-20160816;
              b=Vk0if2+W7oXnUZ3rKxq8uYwm3tuhtUYP0R8lkWNfJyCSE6uRfbrpEWN7aX
              wb9TsFp2NYaGep5mr0XRMetS4bh7h7JlrG96pxiSXiB72hxjnkH2YkmxrAdJ/4P6
              ZyJiXqVqmck6wcKXWR/Ayvm4/ROaIA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
              h=date:message-id:content-transfer-encoding:subject:from:to:mime-version:content-
              transfer-encoding:arc-authentication-results;
              bh=PrP7xSJ9KdTZhnY9s9cHOpqzv9d00uvgaJPJY+RYCJQ=;
              b=LdloCBm2v8CHqrEDV3B2n7oyUrjTr2X6fHvn5MMNP0OP0G0hH8vp3YEouuv1u4
ARC-Authentication-Results: i=1; mx.google.com;
              spf=pass (google.com: best guess record for domain of apache@main.dannix.co.uk_designates
              213.171.197.232 as permitted sender) smtp.mailfrom=apache@main.dannix.co.uk;
              dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=gmail.com
Return-Path: <pache@main.dannix.co.uk>
Received: from main.dannix.co.uk (main.dannix.co.uk. [213.171.197.232])
              by mx.google.com with ESMTPS id v63si4796634wme.202.2017.08.31.03.40.16
              for <upadhyay.thesis@gmail.com>
              (version=TLS1 cipher=AES128-SHA bits=128/128);
Received-SPF: pass (google.com: best guess record for domain of apache@main.dannix.co.uk
              Designates 213.171.197.232 as permitted sender) client-ip=213.171.197.232;
Authentication-Results: mx.google.com;
              spf=pass (google.com: best guess record for domain of apache@main.dannix.co.uk designates
              213.171.197.232 as permitted sender) smtp.mailfrom=apache@main.dannix.co.uk;
              dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=gmail.com
              Received: from main.dannix.co.uk (unknown [213.171.197.232]) by main.dannix.co.uk (Postfix)
              with ESMTPS id 99A609C668 for <upadhyay.thesis@gmail.com>; Thu, 31 Aug 2017 11:40:16
              +0100 (BST)
Content-Transfer-Encoding: 7bit
MIME-Version: 1.0
To: upadhyay.thesis@gmail.com
From: ISRO Centralised Recruitment Board <icrb@isro.gov.in>
Subject: ISRO Head Quarter for Joining as a Scientist
X-COMPLAINTS: To report abuse please email
X-COMPLAINTS: abuse@sharpmail.co.uk
Content-Transfer-Encoding: binary
Content-Type: text/plain; charset="utf-8"
Message-Id: 20170831104016.8D4DE9C6CB@main.dannix.co.uk

Dear Ramakant,

 Congratulations!!! You are selected in ISRO in your Final round.
 Your name has been shortlisted for the post of scientist so come with your all
 Testimonials certificates and verify your all details on 18th September 2017
 At sharp 10.00 AM at Delhi head quarter.
 ISRO -HQ-Delhi
```

Fig. 2 Spoofed E-Mail Header Information Detected

**III. Related work**

S Gupta [1] discussed about the forensic analysis of E-Mails headers data values. In this paper algorithm made to catch the spoofed mail based on address spoofing, address means domain name of server. She implemented an approach by which fake mail identified using the comparison of few header values and several domains with its real permission code, like PASS etc.

this comparison is made among SPF, DKIM, DMARC etc .if all parameters are passing as "PASS" then based on the code it is easy to identify that an E-Mail is not address spoofed which meant that mail comes to appear from legitimate sender or in simple way say that valid sender server domain.

The author also made a java API program to perform the detailed information of mail header. They given an approach to evaluate address spoofing if any one of these parameters are fail/neutral fail/soft fail then mail is address spoofed meant that mail may send from third party domains. but in the data set we found that in DKIM Signature field not talk about if it`s d`s value when this is pass and d`s value having the address of fake domain.

P. Mishra [2] proposed an algorithm for the forensic evaluation of E-Mail date and time spoofing. The author updated as extended style the algorithm given by the T. Banday. Date and Time field is extracted from the E-Mail header and then done the experimental analysis of the sending and receiving date and time variation.

If the difference is greater than a given specific margin, then we can easily say that E-Mail is Date or Time or Date and Time spoofed. The author created also spoofed E-Mail dataset values by using Java Mail API classes and performed the expanded header analysis on the E-Mails. They have given approach to check sent and received date and time field of each and every E-Mail, if they vary from a predefined margin, then E-Mail is date spoofed.

DK Tayal [3], author develop an algorithm to detect all spam E-Mails through linear techniques and method through N Bayes and modified K-means strategy. To identify sapm mail, author used Machine Learning (ML) or rule based classification and content based methods (CBM). ML is used a set of rules to classify that incoming mails are spam or not. In CBM, computer machine takes intelligent decisions based on data sets.

T. Banday [5] presents how an E-Mail message can be detected and prevented from date spoofing method. It also describes the mechanisms to send and receive date spoofed E-Mail. Furthermore, it has the lists of solutions to the problem of date spoofing and recommends a model, which includes necessary algorithms to detect and stop transmission and reception of date spoofed E- mail messages.

Date spoofed E-Mails can be sent from any E-Mail client program either through directly modifying the send `date` header field or by altering the clock of the computer system running the E-Mail client program. The programs such as Office Outlook, Outlook Express and Eudora etc. can be used to send date spoofed E-Mail by temporarily adjusting the clock of the client computer system before sending the mail.

M.T. Banday [6] talked about the E-Mail`s header in detail. He also describes the sender spoofing approaches, but not provided any method to check and find the sender spoofing in presumption E- Mails.
M.T. Banday [7] has recommended solutions to avoid date spoofing. He did not given any practical implementation. Some of the drawbacks of the solutions are as follows: The date`s alteration can be verified or validated if all the server machines and clients are time synchronized. The E-Mails are required to be fetched or retrieved from the trusted third party server, will raise overhead only in terms of cost and time. Repeatedly sender server domain and receiver machine must trust same type server.

## IV. Proposed Technique

It checks four conditions for E-Mail legalistic detection:

(1) Message-ID (at last portion) should same as the domain address of FROM field

(2) DMARC and R-SPF both must be PASS

(3) DKIM,R-SPF values must PASS & R-SPF value must contains "domain name same as is in the From field" or "FROM field ID" & string shows as "authentic as permitted sender"

(4) If DKIM and R-SPF are not present then D`s value, under DKIM-signature, must be the domain name of the FROM field.

(5) Otherwise sent E-Mail is fake means that mail is sender spoofed.

```
While (Complete Header`s Information are extracted & ready for access)
Read ---Message-ID/R-SPF/ DMARC /DKIM/DKIM-Signature
If (R-SPF==Pass && DMARC==Pass) //Both SPF & DMARC Checked by && operator
{
Sender Address is Genuine
}                                                    // nested If else Loop
Else if (R-SPF ==Pass && DKIM==Pass && ((R-SPF.value == "Domain name of From
field authentic as permitted sender") | |(R-SPF.value== "From field authentic as permitted
sender")))
{
Sender Address is Genuine
}                                                    // nested If else Loop
Else if (R-SPF== null && DKIM== null | | pass && DKIM SIGNATURE.d==domain
name same as From fileld)
{
Sender Address is Genuine
}
Else                                                 // Spoofed Identification Section
{
Sender is Fake and It`s Email address is Spoofed
S_name= extract_MESSAGE_ID.value
Spoofed_Server_Identity/Name= S_Name
Sub_name=extract_Subject.value
Subject of Spoofed Mail is= Sub_name
}
}
```

Fig. 3 Algorithm for E-Mail Sender Address Spoofing

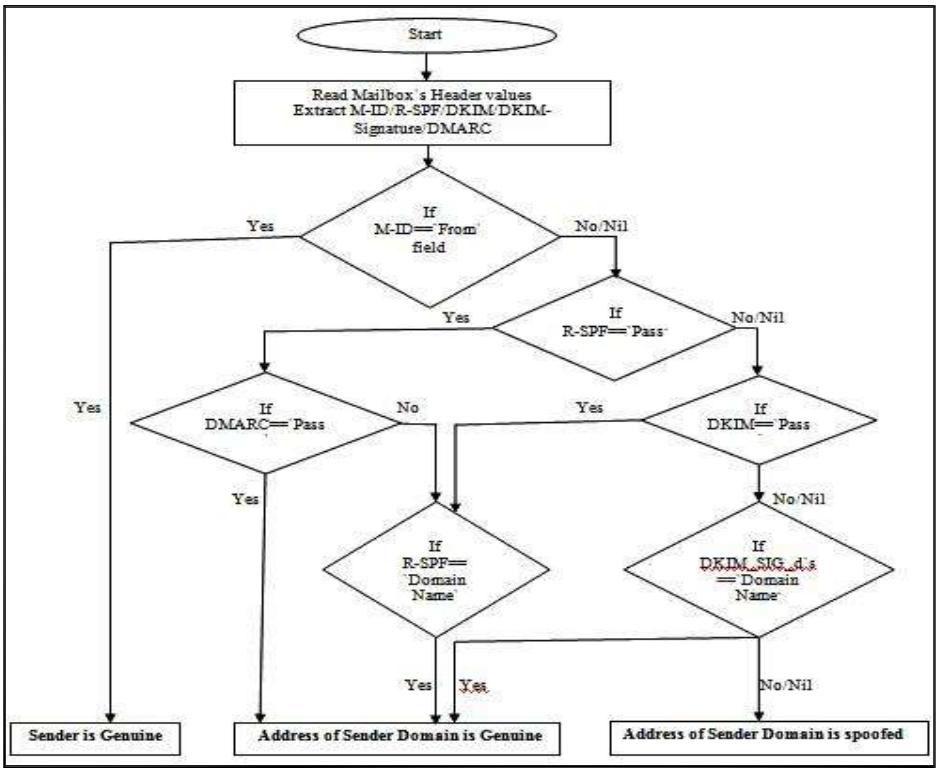


Fig. 4 Flowchart for E-Mail Address Spoofing Detection

## V. Experiments

The following number of exercise and experiments are used to perform to detect sender address spoofing in all E-Mails domains. The steps are as follows as:

- Creation of original E-Mail header data sets using java API
- Creation of Spoofed E-Mail header datasets using java API

 

- Recognition and classification of E-Mails using java API
- Evaluation and equivalence of several original and spoofed header fields
- Automatically generated text file for header analysis output using java API

**A. Creation of original E-Mail header data set**

| E-Mail sent from AOL to AOL ID | | |
|---|---|---|
| **Header Fields** | **Header Fields Value** | **Description** |
| **Subject** | Greetings for Gold Medal | Subject`s Name |
| **R-SPF** | NIL | Sender Permitted None |
| **Return Path** | ramakant.thesis@aol.com | AOL Sender |
| **DKIM** | NIL | Authentic None |
| **DKIM Signature** | v=1; a=rsa-sha256; c=relaxed/relaxed; d=mx.aol.com;s=20150623; s=20150623 t= 1503032287; bh=fNevakGnS0b | Authentic |
| **DMARC** | pass (p=REJECT sp=REJECT dis=NONE) header.from=aol.com | Authentic |
| **Message -ID** | 15df3b49b69-c0a-82e@webjas-vad081.srv.aolmail.net | AOL Domain |

Table 2 Legitimate E-Mail header dataset mails sent from AOL to other AOL Domain

In table 2, mail sent from AOL ID to AOL ID where subject RSPF in Nil means that no checking of received sender policy framework phase. Return path is same as from (sender) field. DKIM is also Nil which shows that its value header.d= sender domain name not generated and identified. DKIM- signature d`s value is same domain name. DMARC field is pass and Message-ID field having the domain at the last portion of M-ID. Finally table data sets are matching with third condition of algorithm, so therefore it is legitimate mail.

**B. Creation of Spoofed E-Mail header dataset**

In table 3, indicates the header fields of E-Mail sent from AOL to AOL using fake mail domain. Return path is nil which should be same as from field value, i.e. aol.com, but here this data value has changed and indicates as Nil. R-SPF is Nil so not able to check from field because here no return path so not possible to check with aol.com domain as in this case. DKIM is pass but DKIM-signature d`s value is not as domain name which is showing fake mailer domain. M-Id is also showing the fake mail server name. Here we detected sender address spoofing approach. This data is not meeting any of the above three conditions of algorithm, so sent E-Mail is sender address spoofed E-Mail.

| E-Mail sent from AOL to AOL | | |
|---|---|---|
| **Header Fields** | **Header Fields Value** | **Description** |
| **Subject** | Congrats! You Won 50000000 Billion Thousand Dollar | Subject`s Name |
| **R-SPF** | NIL | None |
| **Return Path** | NIL | AOL Sender None |
| **DKIM** | Pass header.i=@bplaced.de | Authentic but I`s value is differ |
| **DKIM Signature** | v=1; a=rsa-sha256; c=relaxed/relaxed; d=bplaced.mail.de; s=dkim; t=87358754; | Unauthentic because d`s value is differ from Domain |
| **DMARC** | fail (p=NONE) header.from=aolmail.net | Authentication Fail |
| **M-ID** | 2745HDTYBVigsek dhh_5438io@bplaced.net | Domain of Fake Mailer with Message ID |

Table 3 Spoofed E-Mail header mail sent from AOL to Other AOL Domain using fake mailer 1

 

### C. Recognition and classification of E-Mails

Our mail detection algorithm is implemented on mail servers and coded in java mail API. This java program checks about spoofed and legitimate mail on the basis of five header fields security standards and header filed parameters like R-SPF, DKIM, DKIM Signature, and M-ID. Our program read particular mail inbox messages one by one and extracts their headers and especially these five fields in side header. So based on the value of these fields, the program decides that the E-Mail is address spoofed or legitimate mail. We will see this effect further in next section.

### D. Evaluation and equivalence of several original and spoofed header fields

| Header / Mail | Values of Genuine Mail Header ( Mail Sent via AOL) | | Values of Fake Mail Header ( Mail sent via several Fake Mailers) | | |
|---|---|---|---|---|---|
| | AOL to AOL (Mail 1) | AOL to Hotmail (Mail 2) | AOL to AOL (Mail 3) | AOL to Hotmail (Mail 4) | AOL to Rediff (Mail 5) |
| **Header Information** | ramakant.thesis@aol.com to upadhyay.thesis@aol.com | ramakant.thesis@aol.com to upadhyay.thesis@hotmail.com | ramakant.thesis@aol.com to upadhyay.thesis@aol.com | ramakant.thesis@aol.com to upadhyay.thesis@hotmail.com | ramakant.thesis@aol.com to upadhyay.thesis @rediffmail.com |
| **Return Path** | ramakant.thesis@aol.com | ramakant.thesis@aol.com | NIL | upadhyay.thesis@aol.aol mail.com | fakesend@fakemail.com |
| **R-SPF** | NIL | Pass protection.outlook.com : domain of hotmail.com designates 40.92.254.33 as permitted sender | NIL | Softfail (aol.net: domain ramakant.thesis@aol.co m does not designated 145.165.122.189 as permitted sender | NIL |
| **DKIM** | NIL | Pass header.d=hotmail.com, x-hmca=pass header.id= upadhyay.thesis @hotmail.com | Pass header.i=@bplaced.de | fail (from bplaced.de) | Pass header .i=@semdfakenail.co m |
| **DKIM Signature** | v=1; a=rsa-sha256; c=relaxed/relaxed d=mx.aol.com | v=1; a=rsa-sha256; c=relaxed/relaxed;d=hotmail.com | v=1; a=rsa-sha256; c=relaxed/relaxed; d=bplaced.mail.de; s=dkim; t=87358754; | v=1; a=rsa-sha256; c=relaxed/relaxed; d=bplaced.mail.de; s=mail; t=34986436; | =1; a=rsa-sha256; c=relaxed/relaxed; =sendfakemail.com |
| **DMARC** | pass(p=REJECTsp=REJECT is=NONE) header.from=aol.com | pass action=none header.from=hotmail.c om | Fail(p=NONE) header.from=aolmail.n et | NIL | fail(p=NONE,dis-NONE) header.from=sendfakemail.com |
| **M-ID** | 15d9-c0a-2e@wbjas-va081.srv.aolmail.net | MAX15F30@M1B0121.INDPRD01.PROD.OUTLOOK.COM | 2745HDTYBVigsekdhh_5438io@bplaced.net | 8645364HFDRUJNGF_Uiecfgfhh0@bplaced.net | 64346HDDCUKINCytv_fdsfadgj423566 @Sendfakemail.com |

Table 4 Header values of Genuine and sender Spoofed E-Mails from AOL

In the table 4, it presents distinct header values while sender and receiver are same but domain address will different.When E-Mail sent from same Mail ID but sender domain address are different. Here in this case when mail sent from ramakant.thesis@aol.com to upadhyay.thesis@aol.com. In mail 1, return path is same as from field but in mail 3 this field is Nil. In mail 3 R-SPS is Nil and DKIM is pass but header.i is spoofed address which indicates that fake domain

 

**E. Automatically generated text file for header analysis output**

Figure V showing the final result of E-Mail evaluation where our proposed algorithm is used to detect them as legitimate or spoofed. When it executed successfully then the new notepad file is created namely as in text file.

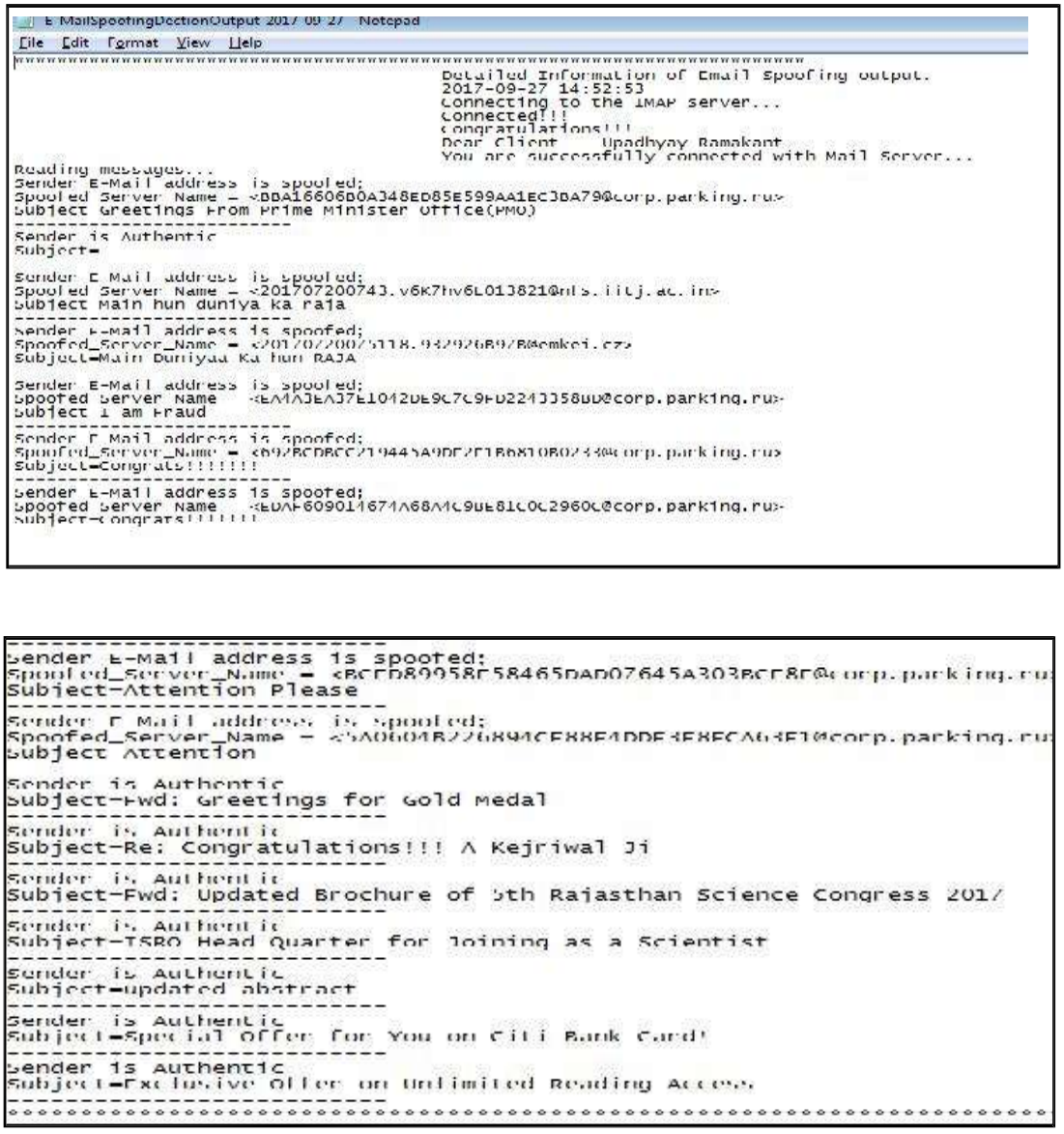





Fig. V Automated Text File Generated

## VI. CONCLUSION AND FUTURE WORK

Any mail ID may misuse by anyone easily to send fake E-Mails. These sender address spoofed mails may identify and detected through given algorithm, which is proposed algorithm & implemented on over the dataset, and it is implemented in Java mail API eclipse tool. We sent fake mail by fake mailers and made its datasets using headers fields. The few headers field, we have considered and perform extensive evaluation on them. Using proposed algorithm, check specific header field values. If they lie we can say sender is legitimate otherwise E-Mail sender address is spoofed. Future work of this paper is to use more mature tools to do complicated header analysis, to now IP address of machine then find log files of it, and more challenging task is to know geographical location of server machine only to detect the sender address spoofing.

 

**REFERENCES**

[1] Surekha G, E.S Pilli, P Mishra, S. Sundar, R.C Joshi, " Forensic Analysis of E-Mail Sender Address Spoofing", in International Conference Confluence 2014- ieeexplore.ieee.org- The Next Generation Information Technology Summit, Noida, India.

[2] P. Mishra, E.S Pilli and R.C Joshi, "Forensic Analysis of E-Mail date and time spoofing", 3rd International Conference on Computer and Communication Technology (ICCCT), Allahabad, UP, India, 2012, pp. 309-314.

[3] DK Tayal, A Jain, K Meena, "Development of Anti- Spam techniques using modified K-means and N Bayes algorithm, Computing for sustainable global Development (INDIAcom) summit 3rd International Conference-ieeexpore.ieee.org. [March 2016]

[4] Internet Security Threat Report and a case study of 2017, ISTR volume No. 22, "Semantic Corporation Inc" [US]

[5] M.T Banday, F.A Mir, J.A Qadir and N.A Shah, "Analyzing Internet E-Mail date spoofing", Digital Investigation , vol 7, pp. 145-153, 2011

[6] M.T Banday, "Analyzing Email headers for forensic Investigation", Journal of Digital Forensic, Security & law, V6,No 2, PP. 49-64, 2011

[7] M.T Banday, "On the Authentication of date in E-Mail using Trusted Time Stamping Services", International Journal of Computer Applications, pp. 36-42, 2011

[8] 2014 A Year in review, 2015. Available:https://www.emc.com/collatral/fraud-report/rsa-online- fraud-report12014.pdf

[9] https://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021- Executive-Summary.pdf

[10] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf

 