Chapter – 5
Performance Analysis

5.1 Introduction

Performance analysis is a very critical step for deciding the efficiency of any algorithm. We divided our testing process into various scenarios depending on the availability of various anti-spoofing protocols like SPF, DKIM and DMARC for a number of domains. In this way we were able to test almost all the possible situations that may arise in real.

5.2 Testing of Proposed Framework

For testing purposes, we selected the top 10, mostly used email servers around the world for our study to find out whether spoofing of email is still possible or not on these email servers. We also selected some domain names for the experiment based on their DNS entries of SPF, DKIM and DMARC. We then performed our experiment wherein we tried to think as an attacker and tried various techniques to bypass some or all of the anti-spoofing protocols.

We divided our testing experiment into various test cases as follows:

1. **Scenario-I:** Sending normal email from our own domain (mail-server.in) which has all three protocols SPF, DKIM & DMARC
2. **Scenario-II:** Spoofing a domain (gmail.com) which has all three protocols SPF, DKIM and DMARC
3. **Scenario-III:** Spoofing a domain (outlook.com) which has all three protocols SPF, DKIM and DMARC
4. **Scenario-IV:** Spoofing a domain (msubaroda.ac.in) having only DKIM record
5. **Scenario-V:** Spoofing a domain (orthocarehospital.in) having only SPF record
6. **Scenario-VI:** Spoofing a domain (orthocarehospital.in) having both SPF and DKIM records
7. **Scenario-VII:** Spoofing a domain (gujarattourism.com) having none of the authentication records

5.3 Results

From the experiment, we can conclude that our email server can successfully deliver email to the inbox of all major email service providers and the sent email passed all three authentication protocols successfully as shown in *Figure 76.*

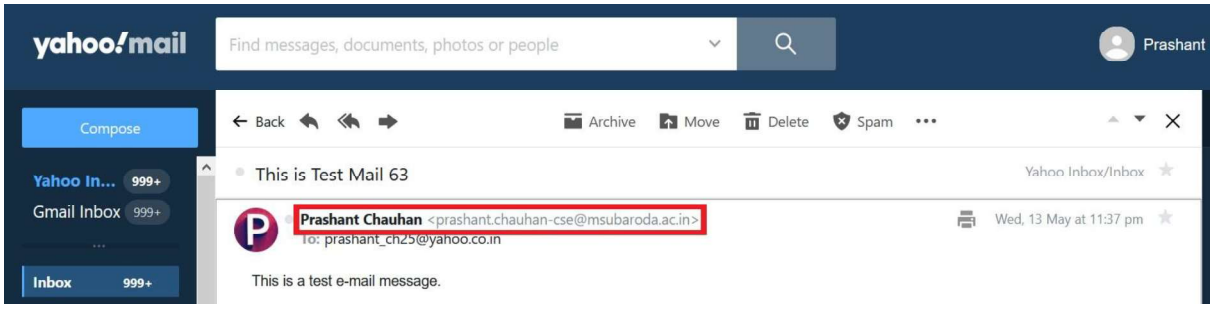

Figure 76: Spoofed email successfully delivered in inbox of recipient

Only in the case of outlook.com, our email was sent to spam instead of inbox despite passing all three protocols. The raw message showing result of SPF, DKIM and DMARC in case of spoofing of email with domain msubaroda.ac.in is shown in *Figure 77*and the result of spoofing of email with domain gmail.com is show in *Figure 78*.

```
 by atlas203.free.mail.sg3.yahoo.com with SMTPs; Mon, 29 Jun 2020 05:07:47 +000
X-Originating-Ip: [209.85.208.53]
Received-SPF: none (domain of msubaroda.ac.in does not designate permitted send
Authentication-Results: atlas203.free.mail.sg3.yahoo.com;
 dkim=pass header.i=@msubaroda-ac-in.20150623.gappssmtp.com header.s=20150623;
 spf=none smtp.mailfrom=msubaroda.ac.in;
 dmarc=unknown
X-Apparently-To: prashant_ch25@yahoo.co.in; Mon, 29 Jun 2020 05:07:48 +0000
X-YMailISG: f4hEagoWLDuOVSAnXuGuF4Eu0eUpyPebtCzTywRGWNHkU4O_
 uXDhZqvLPZlYsA2kGi_bQpBTaYcUDmd6Kr674KvyMkVK591S08NJkgP_mks0
 tCvkT46gdr9BoFXq24Mk_JPLgKT.d_GqWVArNSYMbbmhDBX21Qa8VM70y15i
 Nt1A80u0QuPT9WqTelAYzKq_QWiA5peDVeTNBxibpwTSQY375Myw_vpRZ3we
```

Figure 77: Raw email message for spoofed email for domain msubaroda.ac.in

```
Received: from 117.240.215.158 (EHLO mail.mail-server.in)
 by atlas116.free.mail.sg3.yahoo.com with SMTPs; Fri, 26 Jun
X-Originating-Ip: [117.240.215.158]
Received-SPF: pass (domain of mail-server.in designates 117.2
Authentication-Results: atlas116.free.mail.sg3.yahoo.com;
 dkim=pass header.i=@mail-server.in header.s=modoboa;
 spf=pass smtp.mailfrom=mail-server.in;
 dmarc=success(p=NONE,sp=QUARANTINE) header.from=gmail.com;
X-Apparently-To: prashant_ch25@yahoo.co.in; Fri, 26 Jun 2020
```

Figure 78: Raw email message for spoofed email for domain gmail.com

We also found that DMARC failed in all the cases due to identifier alignment issue, while both SPF and DKIM were passed by all the email servers used in the experiment for the spoofed email. Gmail and Zoho Mail shows “via” message along with the sender email id. Proton Mail and Rediffmail displays a warning message to the user along with the email and in most cases, the email is successfully delivered to inbox without any kind of warning to the user.

To further try to bypass the authentication protocols, we tried to send the spoofed email with multiple senders, the results of which are shown in *Figure 79*. As seen in the figure all the three protocols SPF, DKIM and DMARC passed for our spoofed email when testing was done on the domain of google.com.

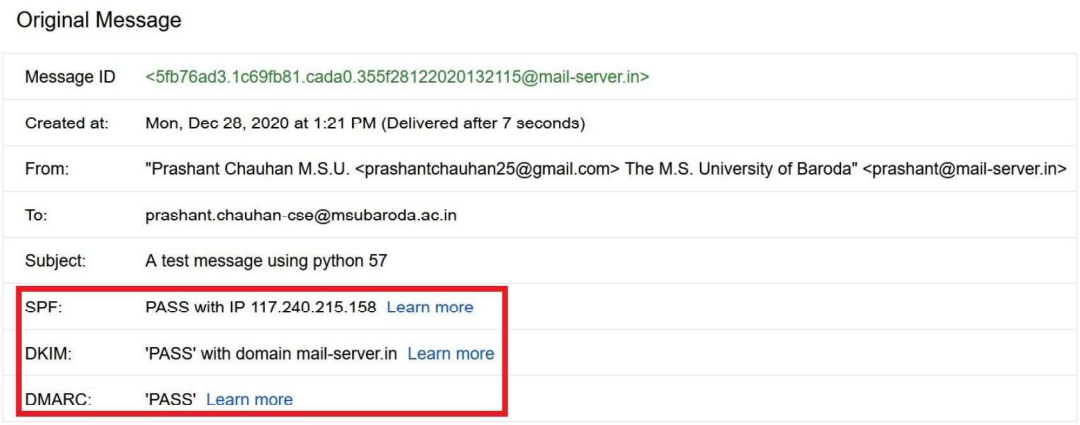

Figure 79: Test results for spoofed email for domain gmail.com having multiple senders

```
Authentication-Results: mx.google.com;
       dkim=pass header.i=@mail-server.in header.s=modoboa header.b=Np+w1mam;
       spf=pass (google.com: domain of prashant@msubaroda.ac.in designates 117.240.215.158 as permitted sender)
smtp.mailfrom=prashant@msubaroda.ac.in
Message-ID: <60f67234.1c69fb81.a9e7d.58c0SMTPIN_ADDED_MISSING@mx.google.com>
Received: from localhost (localhost [127.0.0.1]) by mail-server.in (Postfix) with ESMTP id 3C9F0140381 for
<prashantchauhan25@gmail.com>; Tue, 20 Jul 2021 12:20:25 +0530 (IST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mail-server.in; s=modoboa; t=1626763825;
bh=8YWeKVa184g6uHoI5gIx2a8eNvx3uAaf9+uUysf1iRU=; h=From:To:Date:Subject:From; b=Np+w1mam/
C4P18k6sq3pSQu7hK2e49g+lvtSysJGnNK4bQbZnuQhEqmFB1bLtijco
        X1VEWFzums4k2+yC9US6rNsAokszOLO/9j7U4haQOOZgHsd2eAUiQkEhyWivQXoUY4
        TRaFag4I3Vfpx5gCB/c5TtIOMbZfQEhmJup7mY7I=
X-Virus-Scanned: Debian amavisd-new at mail.mail-server.in
Received: from mail-server.in ([127.0.0.1]) by localhost (mail.mail-server.in [127.0.0.1]) (amavisd-new, port 1
ESMTP id qoVQ6e6ZxL_3 for <prashantchauhan25@gmail.com>; Tue, 20 Jul 2021 12:20:23 +0530 (IST)
Received: from DESKTOP-H6GUK6H (mail-server.in [117.240.215.158]) (using TLSv1.2 with cipher ECDHE-RSA-AES256-G
(256/256 bits)) (No client certificate requested) by mail-server.in (Postfix) with ESMTPSA for <prashantchauhan
Tue, 20 Jul 2021 12:20:23 +0530 (IST)
EAIC: 7978104763042458
MIME-Version: 1.0
From: prashant@msubaroda.ac.in
To: prashantchauhan25@gmail.com
Date: 20 Jul 2021 12:20:23 +0530
```

Figure 80: Spoofed email message header displaying EAIC code

The raw message displaying the headers of the received email including the EAIC code as one of the headers can be seen in *Figure 80*. The received EAIC code will then be used by our proposed Adaptive Authentication Framework for Email (AAFE). And depending on the value of EAIC code the proposed framework will detect whether the received email is authentic or spoofed.

5.4 Scenario – 1: Email with SPF, DKIM & DMARC (mail-server.in)

In this case, we selected our own email server domain as the sending email domain i.e., **mail-server.in.** The selected sending domain has implemented all three authentication protocols i.e. Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC). We selected **prashant@mail-server.in** as the spoofed sending email id in this case. The result of our experiment when trying to send email from our own domain having published all three anti-spoofing protocols SPF, DKIM and DMARC is shown in *Table 4*.

From the table, we can conclude that our email server can successfully deliver email to the inbox of all major email service providers and the sent email passed all 3 protocols successfully. Only in the case of outlook.com, our email was sent to spam instead of inbox.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC
Gmail	Inbox	Pass	Pass	Pass
Outlook	Spam	Pass	Pass	Pass
Proton Mail	Inbox	Pass	Pass	Pass
AOL Mail	Inbox	Pass	Pass	Pass
Yahoo! Mail	Inbox	Pass	Pass	Pass
Zoho Mail	Inbox	Pass	Pass	Pass
iCloud Mail	Inbox	Pass	Pass	Pass
Rediffmail.com	Inbox	Pass	Pass	Pass
Mail.com	Inbox	Pass	Pass	Pass
Yandex Mail	Inbox	Pass	Pass	Pass

Table 4: Experiment results for mail-server.in

5.5 Scenario – 2.1: Spoofing with SPF, DKIM & DMARC (gmail.com)

In this case, we selected **gmail.com** as the sending email domain which uses all three authentication protocols SPF, DKIM and DMARC. We selected **prashant@gmail.com** as the spoofed sending email id in this case. The result of our experiment in this case is shown in *Table 5*.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Fail	via shown
Outlook	Spam	Pass	Pass	Fail	-
Proton Mail	Inbox	Pass	Pass	Fail	warning
AOL Mail	Inbox	Pass	Pass	Fail	-
Yahoo! Mail	Inbox	Pass	Pass	Fail	-
Zoho Mail	Spam	Pass	Pass	Fail	via shown
iCloud Mail	Inbox	Pass	Pass	Fail	-
Rediffmail.com	Inbox	Pass	Fail	Fail	warning
Mail.com	Inbox	Pass	Pass	Fail	-
Yandex Mail	Spam	Pass	Pass	Fail	-

Table 5: Experiment results for gmail.com with single sender

From the table we found that DMARC failed in all the cases due to identified alignment issue while both SPF and DKIM were passed by all the email servers used in experiment for the spoofed email. Gmail and Zoho Mail shows “via” message along with the sender email id. Proton Mail and Rediffmail displays a warning message to the user along with the email and in most cases the email is successfully delivered to inbox without any kind of warning to the user. To further try to bypass the authentication protocols, we tried to send the spoofed email with multiple senders whose results are shown in *Table 6*. From the table, we can see that by using multiple sender ids we were able to pass all three protocols in the case of Gmail and Proton Mail which was not possible with single sender id. Even no “via” message was shown in case of Gmail for the spoofed email with multiple sender email ids which was displayed in case of spoofed email with single sender email id. Also, in the case of mail.com the email was completely rejected and not delivered to the recipient user when multiple sender email ids were used.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Spam	Pass	Pass	Fail	-
Proton Mail	Inbox	Pass	Pass	Pass	warning
AOL Mail	Inbox	Pass	Pass	Fail	-
Yahoo! Mail	Inbox	Pass	Pass	Fail	-
Zoho Mail	Spam	Pass	Pass	Fail	via shown
iCloud Mail	Inbox	Pass	Pass	Fail	-
Rediffmail.com	Inbox	Pass	Fail	Fail	warning
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	Fail	-

Table 6: Experiment results for gmail.com with multiple senders

5.6 Scenario – 2.2: Spoofing with SPF, DKIM & DMARC (outlook.com)

In this case, we selected **outlook.com** as the sending email domain which uses all authentication protocols SPF, DKIM and DMARC. We selected **prashant@outlook.com** as the spoofed sending email id in this case. The result of our experiment in this case is shown in *Table 7*.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Fail	via shown
Outlook	spam	Pass	Pass	Fail	-
Proton Mail	Inbox	Pass	Pass	Fail	warning
AOL Mail	Inbox	Pass	Pass	Fail	-
Yahoo! Mail	Inbox	Pass	Pass	Fail	-
Zoho Mail	Spam	Pass	Pass	Fail	via shown
iCloud Mail	Inbox	Pass	Pass	Fail	-
Rediffmail.com	Inbox	Pass	Fail	Fail	-
Mail.com	Inbox	Pass	Pass	Fail	-
Yandex Mail	Spam	Pass	Pass	Fail	-

Table 7: Experiment results for outlook.com with single sender

To further try to bypass the authentication protocols, we tried to send the spoofed email with multiple senders, the result of which is shown in *Table 8*.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	spam	Pass	Pass	Fail	-
Proton Mail	Inbox	Pass	Pass	Pass	warning
AOL Mail	Inbox	Pass	Pass	Fail	-
Yahoo! Mail	Inbox	Pass	Pass	Fail	-
Zoho Mail	Spam	Pass	Pass	Fail	via shown
iCloud Mail	Inbox	Pass	Pass	Fail	-
Rediffmail.com	Inbox	Pass	Pass	Fail	-
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	Fail	-

Table 8: Experiment results for outlook.com with multiple senders

From the table, we can see that by using multiple sender ids we were able to pass all three protocols in the case of Gmail and Proton Mail which was not possible with single sender id. Unlike the case with single sender email id, even no “via” message was shown in case of Gmail for the spoofed email with multiple sender email ids. Also, in the case of Mail.com the email was completely rejected and not delivered to the recipient user when multiple sender email ids were used.

5.7 Scenario – 3: Spoofing with only DKIM (msubaroda.ac.in)

In this case, we selected **msubaroda.ac.in** as the sending email domain which uses only DKIM protocol. We selected **prashant@msubaroda.ac.in** as the spoofed sending email id in this case. The result of our experiment in this case is shown in *Table 9*. From the table, we can see that result of DMARC is shown as “none” as the selected domain has not published DMARC record. It is to be noted that in all the cases SFP was passed even though the selected domain has not published any SPF record. Also, Gmail and Zoho Mail shows “via” message along with the sender email id.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	none	via shown
Outlook	Spam	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	none	-
AOL Mail	Inbox	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Spam	Pass	Pass	none	-
Rediffmail.com	Inbox	Pass	Fail	none	-
Mail.com	Inbox	Pass	Pass	none	-
Yandex Mail	Spam	Pass	Pass	none	-

Table 9: Experiment results for msubaroda.ac.in with single sender having only DKIM

To further try to bypass the authentication protocols, we tried to send the spoofed email with multiple senders, the result of which is shown in *Table 10*. From the table, we can see that by using multiple sender ids we were able to pass all three protocols in the case of Gmail and Proton Mail which was not possible with single sender id. Also "via" message was shown in case of Zoho Mail and warning was shown only in Proton Mail.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Spam	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	Pass	warning
AOL Mail	Inbox	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Spam	Pass	Pass	none	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Not delivered				
Yandex Mail	Inbox	Pass	Pass	none	-

Table 10: Experiment results for msubaroda.ac.in with multiple senders having only DKIM

5.8 Scenario – 4: Spoofing with only SPF (orthocarehospital.in)

In this case, we selected **orthocarehospital.in** as the sending email domain and we published only SPF records for this domain for the purpose of our experiment. We selected **prashant@orthocarehospital.in** as the spoofed sending email id in this case. The result of our experiment in this case is shown in *Table 11*.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	none	via shown
Outlook	Inbox	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	none	-
AOL Mail	Inbox	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Inbox	Pass	Pass	none	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Inbox	Pass	Pass	Pass	-
Yandex Mail	Spam	Pass	Pass	none	-

Table 11: Experiment results for orthocarehospital.in with single sender having only SPF

From the table, we can see that result of DMARC is shown as “none” as the selected domain has not published DMARC record. It is to be noted that in all the cases both SFP and DKIM were passed even though the selected domain has only published its own SPF record and all the email were delivered to the inbox except Yandex Mail which delivered the spoofed email in spam folder. Also, Gmail and Zoho Mail shows “via” message along with the sender email id except which warning was shown in none of the selected email servers. The results for multiple sender ids in spoofed email are shown in *Table 12*. From this table, we can see that by using multiple sender ids we were able to pass all three protocols in the case of Gmail and iCloud Mail which was not possible with single sender id. The “via” message was shown only in case of Zoho Mail and email was delivered to spam folder for AOL Mail, Yahoo Mail, iCloud Mail and Yandex Mail. For the rest, all the email were successfully delivered to the inbox of the recipient user.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Inbox	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	none	-
AOL Mail	Spam	Pass	Pass	none	-
Yahoo! Mail	Spam	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Spam	Pass	Pass	Pass	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	none	-

Table 12: Experiment results for orthocarehospital.in with multiple senders having only SPF

5.9 Scenario – 5: Spoofing with SPF and DKIM (orthocarehospital.in)

In this case, we selected **orthocarehospital.in** as the sending email domain and published both SPF and DKIM records in the DNS for this domain. Then, we selected **prashant@orthocarehospital.in** as the spoofed sending email id for this case. The result of our experiment for this case is shown in *Table 13*.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	none	via shown
Outlook	Inbox	Pass	Pass	none	_
Proton Mail	Inbox	Pass	Pass	none	_
AOL Mail	Inbox	Pass	Pass	none	_
Yahoo! Mail	Inbox	Pass	Pass	none	_
Zoho Mail	Inbox	Pass	Pass	none	-
iCloud Mail	Inbox	Pass	Pass	none	_
Rediffmail.com	Inbox	Pass	Pass	none	_
Mail.com	Inbox	Pass	Pass	Pass	_
Yandex Mail	Spam	Pass	Pass	none	_

Table 13: Experiment results for orthocarehospital.in with single sender having SPF and DKIM

From the table, we can see that result of DMARC is shown as “none” as the selected domain has not published DMARC record. It is to be noted that in all the cases both SFP and DKIM were passed even though the selected domain has published its own SPF and DKIM records and all the email were delivered to the inbox except for Yandex Mail where the email was delivered in the spam folder. Also, only Gmail shows “via” message along with the sender email id rest all others just delivers the spoofed email without any kind of warning to the end user.

Then we performed the same experiment by sending multiple sender ids in spoofed email whose results can be seen in *Table 14*.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Inbox	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	Pass	-
AOL Mail	Spam	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	Pass	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Inbox	Pass	Pass	Pass	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	none	-

Table 14: Experiment results for orthocarehospital.in with multiple senders having SPF and DKIM

From the table, we can see that by using multiple sender ids we were able to pass all three protocols in the case of Gmail, Proton Mail and iCloud Mail which was not possible with single sender id.

Also “via” message was shown only in case of Zoho Mail and email was delivered to spam folder only for AOL mail and Yandex mail, for rest all the email was successfully delivered to the inbox of the recipient user.

5.10 Scenario – 6: Spoofing with no authentication (gujarattourism.in)

In this case, we selected **gujarattourism.com** as the sending email domain which uses none of the authentication protocols. We selected **prashant@gujarattourism.com** as the spoofed sending email id in this case. The result of our experiment in this case is shown in *Table 15*.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	none	via shown
Outlook	Spam	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	none	-
AOL Mail	Inbox	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	none	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Inbox	Pass	Pass	none	-
Rediffmail.com	Inbox	Pass	Fail	none	-
Mail.com	Inbox	Pass	Pass	none	-
Yandex Mail	Spam	Pass	Pass	none	-

Table 15: Experiment results for gujarattourism.com with single sender

From the table, we can see that result of DMARC is shown as “none” as the selected domain has not published DMARC record. It is to be noted that in all the cases both SFP and DKIM were passed even though the selected domain has not published its own SPF and DKIM records and all the emails were delivered to the inbox except for Yandex Mail and Outlook. Also, only Gmail and Zoho Mail shows “via” message along with the sender email id.

Then, we performed the same experiment by sending multiple sender ids in spoofed email whose results are displayed in *Table 16*.

From the table, we can see that by using multiple sender ids we were able to pass all three protocols in the case of Gmail, Proton Mail and iCloud Mail which was not possible with single sender id.

Also “via” message was shown only in case of Zoho Mail and email was delivered to spam folder only for AOL Mail and Yandex Mail, for rest all, the email was successfully delivered to the inbox of the recipient user. Also, the email was completely rejected by Mail.com server, when multiple sender email ids were used in the spoofed email.

Receiving Server Name	Delivery Location	SPF	DKIM	DMARC	Remarks
Gmail	Inbox	Pass	Pass	Pass	-
Outlook	Inbox	Pass	Pass	none	-
Proton Mail	Inbox	Pass	Pass	Pass	-
AOL Mail	Spam	Pass	Pass	none	-
Yahoo! Mail	Inbox	Pass	Pass	Pass	-
Zoho Mail	Inbox	Pass	Pass	none	via shown
iCloud Mail	Inbox	Pass	Pass	Pass	-
Rediffmail.com	Inbox	Pass	Pass	none	-
Mail.com	Not delivered				
Yandex Mail	Spam	Pass	Pass	none	-

Table 16: Experiment results for gujarattourism.in with multiple senders

5.11 Performance Analysis with Existing System

From our testing, we found that our proposed Framework can detect an email to be spoofed in all of the types of attacks found and tested earlier, which was not possible using only the SPF, DKIM and DMARC protocols. As we could test the delivery of an email using our proposed Adaptive Authentication Framework for Email (AAFE) only on our own email server, which can be modified as per our requirements, we could test the AAFE on our own domain but not on any of the other email servers as they are not in our control and are currently not using our proposed framework. A brief comparison of performance analysis of our proposed system (AAFE) with the existing system comprising of SPF, DKIM & DMARC is shown in *Table 17*.

Sr. No.	Existing Method (SPF, DKIM, DMARC)	Adaptive Authentication Framework for Email (AAFE)
1.	The solution is at individual domain level	The solution is at email server level
2.	Individual domain owners need to publish their DMARC, DKIM and SPF records in DNS for the current system to prevent spoofing of their domain	Individual domain owners need not to do anything. Only the email server needs to adopt our proposed framework
3.	Even after publishing DMARC, DKIM and SPF, a domain owner is not protected from email spoofing. Users of this domain can still receive spoofed email from other domains not using anti-spoofing protocols	All users of an email server will get benefited and will be protected to spoofed email if only the email server adopts our proposed framework.
4.	Successful only if all the domain owners publish their DMARC, DKIM and SPF records	Can be successful by implementation of proposed framework only by major email servers
5.	Even after successful implementation, spoofing is still possible till date	With proposed model rate of spoofing is expected to become negligible
6.	SPF, DKIM and DMARC can be bypassed by specific type of attacks	Proposed model is resistant towards such attacks

Table 17: Comparison of proposed framework with existing methods

5.12 Conclusion and Summary

In this chapter, we discussed the results of our experiment of spoofing of email under various scenarios. We found that by applying certain tricks we can easily bypass all the three anti-spoofing protocols SPF, DKIM and DMARC which will successfully deliver a spoofed email to the inbox of the recipient victim user. We selected top 10 mostly used email servers and performed our experiment on these email servers and found which email servers are susceptible to what kind of spoofing attacks. Few of the email servers rejected the email altogether on detecting a possibility of spoofing of email while majority of the email servers successfully delivered even a spoofed email to the recipient user. At the end we described the major advantages of our proposed framework (AAFE) over the existing system using DMARC, DKIM and SPF.