# Chapter – 6
# Conclusion and Future Enhancement

## 6.1 Summary

From our experiment, we found that our proposed protocol can detected an email to be spoofed in all the types of attacks found and tested earlier, which was not possible using only the DMARC, DKIM and SPF protocols. Comparison of our proposed framework with the existing methods used for prevention and detection of spoofing of email is shown is *Table 1*.

It can be said that identifier alignment used in DMARC is quite helpful in marking an email as DMARC fail. It checks if the email id in "From" field of the email body is same as the one in email header. If both these email ids are not similar, DMARC test is failed, and decision is made by the recipient email server based on the DMARC policy established by the sending email domain owner. It is found that even when DMARC test is failed, none of the email servers rejected our spoofed email because of their selected DMARC policy. The liberal DMARC policy of allowing email even in case of failure of DMARC, leads the email to the inbox of the user which might be dangerous for the recipient user.

Also, with our experiment we can say that using multiple email ids in the "From" field of email body, identifier alignment test can be passed, if one of the email ids in the "From" field of email body is kept same as the one in email header. There must be some techniques to ensure identifier alignment is checked and passed before any email is received at the receiving email server which will ensure prevention of email spoofing.

Also, it is found that some of the email service providers like Gmail and Zoho Mail show a "via" message along with the sender email id which is quite helpful in detecting the source of the email and warn the user for possibility of spoofing. And, in few cases of spoofing of email, only Proton Mail and Rediffmail displayed a warning message to the user to warn them of possibility of spoofing of email, while rest others displayed no

warning to the user regarding possibility of spoofing. A normal user is not expected to go to email details and see the raw email message to check the status of SPF, DKIM and DMARC tests.

In such cases, where users are not very tech-savvy, they will only see whatever is displayed on their main screen of the inbox and won't in detail to check the authenticity of the received email and may get in the trap of the attacker. In some cases, and by few of the email servers, this kind of warning message is displayed to the user but not by majority of them.

We suggest the email receivers to provide such warning message to the user in all cases where any of the tests are failed or in case spoofing of email is presumed by the receiving email server. The ideal threshold value used to check the authenticity of an email in Adaptive Authentication Framework for Email (AAFE) is kept to be 60 so an email can be assumed to be authentic even if it passes the EAIC test and if it came from a single sender email id, irrespective of the other checks.

Thus, our framework will work even if the authentication protocols like SPF, DKIM and DMARC are not used by any domain owner. Also, the threshold value can be adjusted by the email server as per their needs.

In present scenario the only options for preventing spoofing of email are authentication protocols namely DMARC, DKIM and SPF which are not sufficient to prevent email spoofing completely. We also found that there are multiple ways by which we may bypass all the three authentication protocols and make way for the spoofed email to the inbox of the recipient user instead of marking the email as spam or rejecting the email all together.

As a conclusion of this experimental study, we propose our Adaptive Protocol to be used by all the email servers to ensure prevention and detection of email spoofing in addition to the existing protocols like SPF, DKIM and DMARC.

## 6.2 Limitation of the Proposed System

After a lot of brainstorming and experimentation under variable situations, we can think of following limitations in our proposed framework:

1. **Issue 1:** One major drawback of the proposed framework may be that the system starts working only after receiving at least 2 emails from the same Sending Mail User (SMU). It may be possible that an attacker sends the first few emails and sets the EAIC code as per its need. In that case the emails will be bypassed from our proposed framework.

   **Discussion:** This won't be a major concern considering the fact that attackers normally spoof only the famous or well-known email ids and not a new email id. Thus, for any well-known email id the genuine EAIC code will exist at the receiving email server side which will not be possible for any attacker to bypass.

2. **Issue 2:** If Receiving Mail Server (RMS) doesn't receive an email sent from Sending Mail Server (SMS) and the email is lost in between, in this situation the SMS has a value of EAIC code stored in its database. But since the RMS never received this email, the same value of EAIC code will never be received by the RMS and this might create a major synchronization issue between the SMS and the RMS. If such situation arises then any further emails sent from SMU to RMS will not be authenticated by the RMS as the EAIC code expected will never match in this scenario for any of the emails sent after a missing email.

   **Discussion:** The possibility of an email server not receiving an email is very rare as the email is sent only after the handshake between the Sending Mail Server (SMS) and the Receiving Mail Server (RMS) is successful. Also, in case of a disconnection of the network the email servers always keep a waiting queue of emails received from its users which will resume once the connection is reestablished and deliver it to the concerned RMS.

   Apart from all this even if we consider the possibility of an email being completely lost in between, still we can have a modification in our proposed framework to also check the EAIC code considering addition of the RIN multiple times. If the received EAIC code matches with any of the EAIC codes generated by adding the RIN for multiple times, it can still work and authenticate the sender as always.

## 6.3 Outcome of Research Work

With this research work we are supposed to achieve the following outcomes

1. We studied the existing process of email system comprising of SMTP protocol at its core and various anti-spoofing protocols like SPF, DKIM and DMARC to prevent and detect spoofing of email. We also researched the techniques proposed by other researchers to countermeasure the problem of email spoofing. And at the end we were able to find the gaps available in the existing system which makes the spoofing of email possible by the attackers.
2. With this research we successfully studied and tested the currently available anti-spoofing protocols SPF, DKIM and DMARC and found the possible ways to bypass each one of them. By knowing the ways to bypass the existing system, we and other researchers too can propose possible solutions to the problem of email spoofing.
3. With this research we designed and developed our proposed framework namely Adaptive Authentication Framework for Email (AAFE) which can effectively provide solution to the existing problem of email spoofing.
4. If our proposed framework is adopted my majority of the email servers, the problem of email spoofing can be prevented completely which will not only save people who are victims of email spoofing from mental stress but also save billions of moneys lost by the victims of spoofed email.
5. Due to the large amount of spoofed email received daily by the majority of the users, there is a loss of confidence in considering email to be an authentic way of communication. With our proposed framework we may bring back the lost confidence of people on email due to spoofing of emails.
6. A lot of effort is made by email service providers daily so as to detect or prevent spoofed email from reaching its users. With our proposed framework we will be able to decrease these unnecessary efforts made by the employees of the well-known email servers.

## 6.4 Future Scope of Work

The proposed system is well equipped to countermeasure the problem of authentication of email. To further increase the security of the system and to prevent attackers from finding a way to bypass the proposed system following enhancements could be made:

1. Provision of change of Initial Random Number and Random Increment Number used for generation of EAIC code after every 100$^{th}$ or any other number of emails sent by a specific user to a specific email server domain.
2. At present, the EAIC code is sent as a header along with the email body. To further increase security, the receiving email server could remove the EAIC code after its purpose of authentication is served. So, no user can see the EAIC code used for the authentication of emails received by him or her.
3. Provision of addition of the RIN multiple times at the Receiving Mail Server (RMS) side to find the expected EAIC code. If the received EAIC code matches with any of the EAIC codes generated by adding the RIN for multiple times, it can still work and authenticate the sender as always even in case of a missed email which was sent by the SMS but never received by the RMS.

## 6.5 Conclusion

With this research we were able to achieve the predefined objectives of finding a possible solution to counter measure the problem of email authentication. Because of the lack of proper mechanism to authenticate the sender of an email, spoofing of email is still possible. With time many anti-spoofing protocols were developed to stop the spoofing of email like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC) but none is found to provide complete protection from email spoofing. To fill up the gaps of the existing system we designed and proposed Adaptive Authentication Framework for Email (AAFE) which can solve the problem of email spoofing altogether if adopted by the email servers. With our proposed framework we expect the possibility of spoofing of emails to become negligible and thus save billions of moneys lost due to email spoofing.