National College of Ireland

Enhancing the security of an E-mail by DMARC and DNS data

MSc Research Project
Cybersecurity

Ravindranath Reddy Kolagotla
Student ID: X19216173

School of Computing
National College of Ireland

Supervisor: Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	RAVINDRANATH REDDY KOLAGOTLA
Student ID:	X19216173
Programme:	MSC CYBERSECURITY **Year:** 2020-2021
Module:	MSc Research Project
Supervisor:	Ross Spelman
Submission Due Date:	23/09/2021
Project Title:	Enhancing the security of an E-mail by DMARC and DNS data
Word Count:	15800 **Page Count:** 30

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: .....

Date: .....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing the security of an E-mail by DMARC and DNS data

RAVINDRANATH REDDY KOLAGOTLA
X19216173

Abstract

Email play's prominent role in our day-to-day life. In general, it communicates between two organisation or two people in and around the world. Now-a-days the use of email has been increased. So, the hackers/attackers are also concentrating to hack an organisation or personal data by using spam, spoofing, phishing and so on but not limited through mails. To overcome from these attacks, Researchers are already proposed various techniques to give more security to emails.

The motivation behind this project is my cousin. My cousin lost around 200 euros (18000 Indian rupees) through an email scam. So, in order to provide more security for emails I have selected this topic. My research project gives more robust to email security by using DMARC and DNS data. DMARC have the capability to diminish the effect of phishing and malware attacks & Logging in domain register for managing the option of DNS setting to configure the further management and also by adding new records to the DNS. These helps to decrease the rate of risk in business.

Introduction:

1.1 Background of the study:

With billions of emails exchanged all over the world at daily basis, these days email is taken into consideration as one of the most extensive forms of digital communication. It has come to notice that because of ease of usage and interoperability, there has been massive use of technology (Ogwu et al., 2020). This beneficial ubiquity of email communication comes at security cost that is often not paid attention at the time maintaining backward compatibility with the versions that have become older. In addition to this, it has been observed that security features are taken in account as optional to make sure that there is high degree of compatibility between the providers. Due to this, there is a consequence, where email communication is not able to safeguard the privacy and authenticity of the information that is exchanged (Ogwu et al., 2020). When the fact is taken into consideration where email is utilized for exchanging private and personal information, it can be said that risk is extremely crucial when it is associated with the latter.

These days, it is noticed that email is taken in account as the most widespread kind of digital communication where more than 100 billion mails are exchanged at daily basis. An email not just account for the most user communication in corporate atmosphere, but it is also used widely in both residential and mobile atmosphere to impart support to the personal communications of the citizens (Stojkovski and Lenzini, 2020). Therefore, notions of security and privacy are extremely crucial and also have gained significant degree of attention because of revelations that are concerned with mass surveillance programs and also due to rise in number of exposed security related threats and vulnerabilities (Stojkovski and Lenzini, 2020).

Email systems are based on Simple mail transfer protocol (SMTP) that was designed 10 years ago around simple but a powerful concept that is interoperability. The ultimate aim was to promote a simple still a trustworthy protocol for email communications. In the early days of internet, email system quickly began to gain high degree of attention that gave birth to rich and ever-growing ecosystem of email providers which are compatible for SMTP (Simpson, 2016). However, with time, it was noticed that simplicity of SMTP came at cost of decreased assistance for purpose of security that was originally taken into consideration as secondary. Unfortunately, Internet has become way more dangerous place than a human would have ever been able to imagine. It has been observed that, as per that the set of standards which are used in email communication has been extended over period of time to deal with the landscape of threat associated with changing security and privacy (Simpson, 2016).

However, the effectual mitigation of security risks that are provided by the present set of standards and executions are very restricted. This comes as a result of the robust requirement to preserve the highest degree of compatibility between email providers so as to make sure that messages are delivered successfully irrespective of the mechanisms of security that are supported by email servicers which are involved in their transmission (Kumar and Somani, 2018). In order to accomplish this goal, till whole community has adopted provided security mechanisms, all the systems have to stay compatible with those which are not secure, which limits the effectual mitigation of security risks. As a result of this, at present email communications are prone to security associated risks that can lead to spoofing of the identity of the users, interception of confidential communications and also modifications of their contents (Kumar and Somani, 2018).

This study will analyse the present state of art in context of protection of privacy and security of the email communications. In more specific way, it can be said that the investigation will pay attention at the modern ways of security of email with the help of DMARC (Domain based message authentication, reporting and conformance) and DNS (Domain name system) based data. This falls in the category of modern means of email authentication and it helps the end user to make sure that mails which they have are received from authentic senders without enticement. The data of DMARC and DNS helps the firm to be safeguarded from any kind of abuse such as losing money, exposing the crucial data and other matters of privacy.

Emails are extremely easy to spoof. This is loved by the criminals because it is extremely easy to ail and exploit the users by phishing emails when they appear to come from the senders whom an individual trusts the most specifically from the brands that are well known (Derouet, 2016). In the same way, putting logo of well-established brand in email makes it look legal which thereby, raises the likelihood that someone can click at something where they must not. In most of the vases, the end user may not be able to differentiate between real and fake message, and the providers of the mailbox have to make extremely typical choices about which messages are legal and which ones are fake (Derouet, 2016). DMARC helps to solve these issues which thereby, help the senders and receivers of the email to work collectively to secure the emails in better way, safeguard the users and the firms from any kind of abuse.

1.2 Problem Statement:

In context of conducting research, email security faces a lot more issues in context of the factors such as phishing attacks, spoofing on clients, lack of appropriate configurations, inappropriate analysis of gaps in security associated with email, less knowledge in context of

contents of the file, antivirus and so on (Rastenis et al., 2020). Making sure that there is proper security towards the system associated with the computer is taken in account as the effort that is given high degree of consideration. If security is violated or data is misused, then it may be taken in account as harmful or premeditated accident. But there is a way in the procedure of safeguarding it from misuse or accidental part against any kind of misuse associated with malicious nature (Rastenis et al., 2020). Some of the issues of security which are mainly involved in sending emails are inclusive of the factors such as malware lurking in huge part which accounts for 2 and 4 percent of the conflicts associated with complaints, failure at part of imparting adequate specs.

In context of email, it can be said that the most harmful influence of email is that it leads to spamming at greater part by harming communication by clouding the vital communication along with maximum amount of communication which is not much required (Rastenis et al., 2020). One of the most crucial issues faced by the user is that they be afraid that their accounts may be hacked by simply opening their account or they may have changes in their password.

1.3 Significance of the study:

The study holds high degree of significance because emails are highly effective ways of initial infection vector because all the firms make use of email and average employee, get numerous mails in a day. The absolute volume of emails means that the employee just has been left with little amount of time to devote to every single mail and pull them in false sense of security. It is noticed that cybercriminals take complete benefit of this in phishing attacks that has become even more common and effectual with growth of cloud-based email (Mukherjee, 2019). Phishing emails or any other malicious messages are made to give attacker with initial access to the network of the organization. This can take place in numerous ways and attain numerous purposes. It may lead to credential theft means it can steal the username and password of the employee. These credentials can be used to access the service remotely at both on site in cloud to perform theft of data or any other action. In addition to this, it may lead to fraud payment. Business email compromise and some similar kinds of spam are made to imitate high level person in the firm (Mukherjee, 2019). These kinds of email give instruction to the employees for sending payment to certain amount, which pretends that it is for closing deal for making payment of invoice to the vendor. These are some of the potential influences of successful attack of phishing on cyber security of the firm. In any of these cases, only one employee has to fall for attack so as to make sure that it is successful. However, it is noticed that phishers over and over again target numerous employees in the firm to increase their chances of having a successful attack.

1.4 Research Topic:

The entire study is reliant at understanding the manner in which security of email can be enhanced specifically by DMARC and DNS data. This study will be advantageous in enhancing knowledge in context of email security, data of DMARC and DNS. The topic of research is given below:

“Investigating the manner in which security of email can be enhanced by DMARC and DNS data”.

1.5 Research Aim:

The aim of the study is associated with security of email in undertaking the ways to address numerous goals which are taken in consideration as crucial and are inclusive of crucial factors such as safeguarding confidentiality associated with data of the user, steps to preserve

the integrity of the data along with promoting the availability of data only for those users who are authorized.

1.6 Research Objectives:

- To analyse how integrated utilization of DMRC and DNS protocol enhance security of email
- To investigate how DMRC helps in the procedure of reducing phishing on part of user account and report
- To examine what type of IP addresses into domain name and what is length of related file
- To scrutinize how DNS helps in a manner in watching names and numbers associated to the internet

1.7 Research Questions:

- How integrated use of DMARC and DNS protocol enhance security of email?
- How does DMARC help in procedure of reducing phishing on part of user account and report?
- What kinds of IP addresses are transformed by DNS in domain name and what is length of associated file?
- How does DNS help in way of watching names and numbers associated to internet?

2: Related Work:

DMARC and DNS data:

As per the opinion of Eboibi (2021), DMARC refers to domain-based message authentication reporting and conformance. It is a security protocol that uses the sender policy framework and leverages DNS to verify the sender of the email. Whenever a misalignment is detected between the recipient of the email and the centre of the email, an administered protocol is activated by DMARC for the purpose of telling the receiver server to accept the message or to reject the message in any case. According to Field (2020), a validation process is conducted by DMARC for giving the sender a report on the attempts to use the domain for sending mail. This process of visibility allows the sender to tune their policy relating to the new threats which are emerging. In this manner the company gets necessary help to establishing their brand trust by reducing the threats of fraudulent emails.
As commented by Grilli et al (2020), DMARC is an email validation system which is mainly designed for protecting the business email domains from getting exploited via phishing scams, cybercrimes, email spoofing etc. There are various ways in which domain-based message authentication reporting and conformance helps in handling unauthorized use of email domains. These are by providing security, visibility, identity, and delivery. it plays an essential role in providing security to the email domain by protecting the people from unnecessary fraudulent activities. It is also observed that a great area of visibility can be gathered into the internet at the time of sending email using the email domain. As per the opinion of Hakim et al (2020), with the help of this method it becomes easier to delivered large number of emails of the mega companies for conducting their business operations. However, it enables identification of the email across the growing footprint of DMARC capable receivers.

According to Kagita et al (2020), DNS refers to Domain Name System. It is basically a phone book of the internet. Internet protocol addresses are used by web browsers for interacting purpose. The domain name is translated to internet protocol addresses by the

domain name system so that the browsers can load the internet sources. Each and every device which is connected to the internet has a unique internet protocol address. As commented by Kizza (2020), DNS is a decentralized and hierarchical naming system for services, computers and other resources which are connected to a private network or an internet. All the information relating to the domain name are assigned to each of the participating entities. However, it helps in translating readily memorize domain names to the internet protocol addresses in a numerical manner for identifying and locating computer services with different network protocols.

As per the opinion of Kontinen (2020), a worldwide distributed directory service has been used for identification of different networks. The entire responsibility of delegating and assigning of the domain names to the internet resources are done through the DNS. The administrators of the networks have a right to delegate authority over sub domains of their name space to other name servers. There are a lot of records which are stored in the database of domain name system. These are name servers, internet protocol addresses, start of authority, pointers for reverse DNS lookups, SMTP mail exchanger etc.

Ways in which integrated use of DMARC, and DNS protocol enhances the security of the email

According to Kwak (2020), DMARC is an email validation system which is basically designed for protecting the email of the business from scams and cybercrime activities. There is certain major contribution of this reporting system is to provide security solutions for email. At the time of purchasing a record of DMARC, DNS is used. Both are integrated together for the purpose of preventing the occurrence of cybercrime and scams taking place in the email of the businesses. As commented by Leukfeldt and Roks (2020),one of the major functions is that the centre of the emails can view the mail on behalf of the domain. Hence DMARC is considered to be an important part of email security. It has been agreed by various professional that the emails from the customers and visitors of the websites are very legitimate. For the purpose of implementing security solutions, DMARC email security is very essential. As per the opinion of McAlaney, and Hills (2020), there are more than 4 billion email accounts which are operated daily. Hence email is considered to be one of the most vital communication channels for or effective exchange of ideas and opinions among two or more persons. Hence there are a lot of Cyber-criminal activities which are taking place through email channels. These criminal activities are increasing on a daily basis and it as per the survey it has been observed that a lot of businesses are facing phishing emails on a regular basis.

According to Mugarura, and Ssali (2020), with the help of DMARC security, the number of phishing attacks becomes visible, and the user can gain an insight into the email channels. It is considered to be one of the most powerful tools for reducing the impact of phishing attacks and malware. For the purpose of avoiding the occurrence of email scams for companies, it is observed that it is very essential to prevent spoofing. This will help the business against brand abuse. As commented by Nayyar et al (2020), there are a lot of modern techniques which are being effectively used for providing protection from phishing scams and email spoofing. These techniques are SPF and DKIM.

But however, the level of Cyber-criminal is activities bypassing these security measures. For the purpose of achieving high security business email, one should make the best use of DMARC. This helps in creating a beneficial in between SPF and DKIM.As per the opinion of Pajankar (2020),a validation process is conducted by DMARC for giving the sender a report on the attempts to use the domain for sending mail. These are by providing security,

visibility, identity, and delivery. it plays an essential role in providing security to the email domain by protecting the people from unnecessary fraudulent activities. The process of implementation of DMARC is very simple and easier. For this purpose, a domain name system (DNS) server administrator is required. The DNS server administrator is added to your DMARC record. This meets the entire monitoring process of the domain much easier.

According to Särökaari (2020), with the help of domain name system and DMARC it becomes possible to ensure maximum safety and security to the emails. A hierarchical decentralized naming system is used for the computers in order to identify the private as well as public networks. Certain specific information's are attached with each of the domain name in order to determine their entities with the help of information protocol addresses. A proper connection is prevailing between the reporting system and the domain name. The domain name system is a type of computer server which possesses different database is related to the IP addresses. With the help of this system, it becomes easier to determine the computer system. As commented by Sharma, and Bashir (2020), the entire workings of the domain name system can be discussed as follows. It is seen that when a user searches in the unique resource locator, a request is immediately sent to the DNS server rather than sending the request to the Google server. A series of lookup tables are used by DNS servers to determine whether the answer is stored inside the cache memory of the computer or not. In case it is not stored in the cache memory of the computer, this request is now sent to the relevant server so that correct display of information is possible on the web browser of a user.

As per the opinion of Tatang et al (2021),it is observed that there are two different types of DNS servers which are used. These are known as primary DNS servers and secondary DNS servers. A lot of beneficial uses adopting with the help of DNS servers. It becomes easier to connect to the search engine without typing any internet protocol addresses. A large number of beneficial characteristics are possessed by DNS which is used by the web masters. A lot of major vulnerabilities are to be considered by the users so that the attackers don't exploit the benefits of obtained by using DNS. According to Wash (2020), there are certain advantages which are borne by DNS. One of the major advantages of DNS is internet dependency. Over the years it has been observed that internet has played a very essential part for various companies and individuals to conduct their operations. With the help of DNS, it becomes easier to use the internet and remember all the IP addresses. Highest internet speed can be enjoyed with the help of DNS. These are some of the most vital benefits which are utilized by companies and individuals with the help of DNS.As per the opinion of Eboibi (2021),a lot of security purposes of the companies and individuals are also served with the help of DNS. Over the years it has been observed that the number of cyber-criminal activities and increasing at a higher place.

According to Field (2020), for the purpose of protecting the emails from scams, DNS has played the very essential role. Use of proper DNS servers has prevented the hackers in gaining maximum information from the server of the companies. However, for a larger organization it is very essential to implement certain security measures along with a DNS server. With the help of the DNS, it becomes easier to remember various IP addresses. Proper stability can be maintained within the system by using DNS effectively.

Ways in which DMRC help in reducing phishing on behalf of the user account and report
As commented by Grilli et al (2020), DMARC is an authentication and reporting process which is based on both DKIM and SPF. The record for DNS is mainly used for publishing information that the domain email authentication is majorly supported by the policies as

defined by SPF and DKIM. All the major procedures for authentication are mainly handled by this process. It is observed that there are various ways which are used by DMRC for the purpose of reducing the occurrence of phishing on behalf of the user account and report. It is observed that phishing scams are one of the most common methods for attacking the email of big business houses. These are considered to be one of the most profitable attack methods used by cyber criminals every year. Due to the common place, it is observed that phishing scams are becoming avoidable if they are identified on time. As per the opinion of McAlaney, and Hills (2020),proper identification of phishing scam helps in taking virus preventive measures against them. There are various ways in which the phishing scams can be easily prevented. These tips play an essential role in minimizing the scams of cybercriminals which are associated with the emails. There are a lot of phishing attack methods which are used every day. Hence identification of the phishing scam please a very essential role in undertaking potential preventive measures. It is always advised not to click any link in a particular email.

A lot of links is leading to phishing scams. As commented by Leukfeldt and Roks (2020), there are certain anti-phishing add-ons which are provided by most of the browsers to determine the malicious attack on the website. These can be used as a preventive measure for reducing phishing scams. It is also advised not to give any information to an unsecured site. A site which does not consist of any security certificates are an indication that the can be used for phishing scams. It is also requested to the users that password should be rotated regularly. This helps in preventing the attacker from gaining unlimited access. Addition of extra layer of protection by using password rotation helps in preventing phishing scams. As per the opinion of McAlaney, and Hills (2020), it is also determined that ignoring regular updates can be a signal of cyber attacking methods. It is very essential to update your browsers in order to reduce the risk of phishing scams. Through these easy steps it is observed that the occurrence of phishing scams and attacks in the email can be easily reduced by the user account. However, the installation of firewalls is an effective measure to prevent attack from external sources by providing a sheet between the computer and the hacker. As commented by Sharma, and Bashir (2020), when both the network firewall and text of firewalls are used together it acts as a great source of security and reduces the chances of attack by the hacker. Often it is observed that a lot of popup takes place at the time of browsing a particular website. These are also most effective sources of attempts for making phishing attacks. It is advised to click on the close option of these ads in order to reduce the attack of phishing scams. As per the opinion of Hakim et al (2020), the users should try to have a data security platform in order to spot the signs of phishing attacks. The security platforms please an essential role in preventing the user from further damage.

IP addresses which are transformed by DNS in domain name and length of associated file
As commented by Leukfeldt and Roks (2020),DNS server is an integral part of the domain name system. It is one of the major parts of the database and computers which are connected to the internet and is responsible for discharging to main responsibilities. The first most essential responsibility is to translate the domain name into an IP address. With the help of this responsibility, it becomes easier to remember a large bunch of numbers. The second most essential responsibility of a domain name server is to specify the mail servers were responsible for distribution of information for the domain name. As per the opinion of McAlaney, and Hills (2020), IP address is unique set of numbers which are allocated for the purpose of detecting a particular computer network. A domain name helps in determining a series of numbers which are known as internet protocol addresses. It is one of the most essential communication protocols which is used for the purpose of exchanging data over two

or three computer networks. As commented by Sharma, and Bashir (2020), with the help IP addresses it becomes easier to allow geographic and networks of computers to communicate among themselves within a very short span of time. A lot of links is required for determining the connection prevailing between the computers. With the help of an IP address, it becomes easier to address the location of the internet. There are generally four sets of numbers ranging from 0 to 225 which are used for setting up the IP address. There are various ways in which the domain name server information can be obtained.

As per the opinion of Hakim et al (2020), the domain name server ensures that the entire data which is sent to a particular address is received by that addressed and no other address. For the purpose of sending a particular data to a particular web address it is essential to determine the unique IP address. Hence with the help of DNS it becomes easier to determine the association prevailing between IP address and the domain name. There are various ways by which the domain name server can be modified. This is mainly done by selecting the manage domain menu option. All possible modifications relating to DNS are made with the help of this option. With the help of a domain name system, it becomes easier to convert the domain name into a particular internet protocol address. Hence there are a lot of Cyber-criminal activities which are taking place through email channels. But however, the level of Cyber-criminal activities is by passing these security measures. As per the opinion of McAlaney, and Hills (2020), for the purpose of achieving high security business email one should make the best use of DMARC. In case it is not stored in the cache memory of the computer, this request is now sent to the relevant server so that correct display of information is possible on the web browser of a user.

Ways in which DNS helps watching names and numbers associated to internet
As per the opinion of Tatang et al (2021), Domain name system (DNS) is a process which involves converting a hostname into a computer friendly IP address. Each device has a unique IP address for the purpose of determining the appropriateness of the internet device. Whenever a user tries to load a webpage translation occur which converts the hostname into IP address. There are various hardware components which are to be studied in order to determine the working process behind DNS. It is observed that there are mainly 4 types of DNS servers at the time of loading a web page. These are DNS recursor, root name server, authoritative name server and TLD name server. The DNS recursor acts as a librarian which receives the queries from the client machine use through web browsers. The entire request relating to the query of the clients are dealt in this stage. The first step in translating the human-readable host name into internet protocol address is through root server. It acts as a reference to different specific locations. As per the opinion of McAlaney, and Hills (2020), the TLD name server searches the specific IP address, and it hosts the last position of a hostname. The final name servers are the last stop in the name server query. There are various ways in which the DNS helps in watching the names and numbers which are associated to internet. These names and numbers are basically the IP address. The first step is to transfer the username and the query received by a DNS recursive.

3: Research Methodology:

3.1 Introduction:

The methodology section explains and describes the overall research. It describes how the research is being conducted. The methodology contains different procedures and techniques while performing the research. This chapter outlines the stages involved while doing this research about "Investigating how the security of email can be enhanced by DMARC and DNS data". The methodology will give an overview of the research philosophy, research

design, data collection method, research limitation, and others. The timeline will show the flow of various stages in the method of research. This chapter provides the evaluator with different techniques which are adopted while researching email security by using DMARC and DNS data. There are specific products and techniques which are used to analyse the information about the investigation done by protecting and safeguarding the data. Moreover, this chapter covers all the areas associated in the area of the research.

3.2 Method outline:

The research outline states that systematic procedure is needed while doing the research. While researching cybersecurity there should be proper planning needed so that the research can proceed efficiently. There are various strategies and approaches in order to reach the appropriate goal. There are a lot of people using the internet for important purposes. Millions of people use email for the exchange of information. These emails get hacked by hackers many times which creates a massive problem. In order to protect the data certain methods are used to protect the data such as DMARC and DNS data (Kour, and Ahmed, 2020). The data are collected from various sources in order to find the effective result of the study. After getting the relevant information from the various sources and then analysing the data using an appropriate technique which yields the final result. There are other crucial methods used in the research so that it gives meaningful information. The method outline indicates what techniques are used in the methodology while doing the research. Thus, research outlines indicate the five steps in the research procedure which involve data collection, research approach, research approach, research design, and research strategy. This outline will provide significant results.

3.3 Research philosophy:

Researchers had developed different philosophies of the research which help to reach the strategic objective and the purpose of the study. Research philosophy is how data of cyber security problems are gathered and analysed so that effective results can be produced. Different philosophies have adopted different techniques in doing the research to be successful. Some of the types of philosophies are as follows- pragmatism, positivism, constructivism, objectivism, and realism (Tatang, Zettl, and Holz, 2021). Pragmatism is the philosophy that focuses on the logical and practical response. Over here, the issues are addressed critically and logically. The cybersecurity problem is a very crucial issue that needs to be addressed properly. Positivism gives a confident result. Sometimes it gives the result hypothetically. They might be wrong in stealing other data or they might not steal other data. Constructivism is the method that is used to help the student to learn something by determining an experiment (Kontinen, 2020). Through the use of this theory, others will learn something from the real world. Through the use of their experiment, how much people can learn from the real world. There is data that needs to be secured so that outside does not get the information.

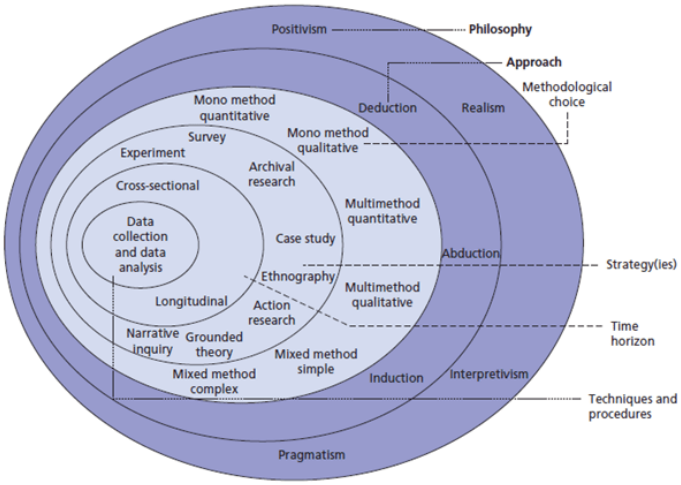

Figure 1: Research philosophy

(Sources:research-methodology.net/research-philosophy/)

3.4 Research Approach:

There are several approaches used to perform the research and conduct analysis of data. It is a plan and procedure through which data is collected step by step in order to conclude the result. There are two types of research approaches commonly used: the inductive approach and the deductive approach. The inductive research approach results are obtained in search of patterns from the development of explanation and observations. The choices of results largely depend on the research approach and research philosophy. In this research, study emails had to be protected by using DNS and DMARC. Thus, the inductive approach answers the mathematical Informatics based on the hypothesis (Patsakis et al.,2020). A deductive approach is a type of approach which is done through scientific investigation. This highlights that investigation is carried out based on information base and knowledge base in order to obtain the result from the research question. This deductive approach helps the researcher to think logically and give meaningful results based on the study of the research. Here, the researcher has to think logically about whether DNS is really effective to safeguard the email (Malinen, 2021). Through this research study, the evaluator will take two statements and evaluation will be done based on the two statements. It is a process that is conducted to be true. it is even conducted and tested whether the statement is true or false.

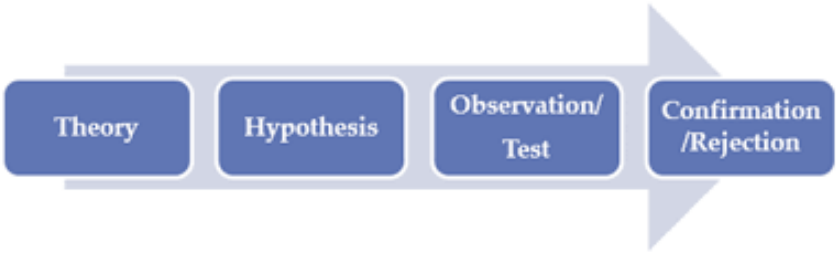

Figure: Deductive approach

(Sources:research-methodology.net/research-methodology/research-approach/deductive-approach-2/)

3.5 Research design:

Explanatory research design is mainly used in this research. The explanatory research allows the evaluator to find the appropriate result which is not studied while doing the research. Though this research does not give a conclusion, it provides an understanding of the problem of cyber security. It helps to understand the problem effectively. the researcher who

researches exploratory research, does according to the objective of the study . Here the objective of the study is to use the DNS data in a better way so that email cannot be hacked. Research design is the framework that contains methods and techniques for research work. The research topics are designed with the help of survey, experimental, correlation, semi-experimental and others. Quantitative research design is normally used in this research study because in this case collecting and analysing the data are essential for the study of the research. The data are collected in the various sources and then the result is formulated in the form of graphs and statistics. Moreover, there are many people who all are using email id for their important purpose but those email id get hacked by the hackers. Those hackers threatened the people in order to get the money in exchange. Through the use of Quantitative techniques, it would be easier to find how many emails got hacked.

3.6 Research strategy:

The research strategy explains the tactics which are used while doing the research work effectively. This strategy will help to draw the result effectively. The researcher obtains the result by using the type of strategies by performing surveys. The survey is done through face to face or from the internet as well. This is one of the efficient strategies that researchers use to obtain the result from the study. DMARC policy is one of the techniques used to control the email messages being hacked (Chen, Paxson, and Jiang, 2020). Case study is needed to be done on the topic security of email can be enhanced by DMARC and DNS data so that no confusion and issue arises in the future. Through the use of the case study, detailed information can be obtained about email cyber security. Some experiments need to be done in order to find the actual information of the study. The experiment is not done in the physics lab in order to get effective information, since we have to bear the cost of servers which are huge. Action research is done by the research in order to the in-depth inquiry about the cyber security problem.

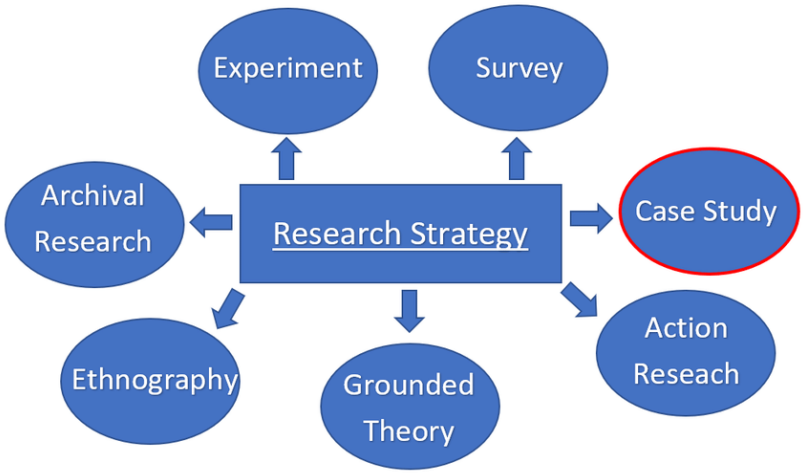

Figure 2 : Research strategy
(Sources:.researchgate.net/figure/Types-of-Research-Strategy-Adopted-from-Saunders-et-al-2009_fig5_342314751)

3.7 Data Collection Method:

In order to decide on a certain statement, data needs to be collected. This collected data will help to conclude this topic. In order to solve the problem, specific things are required to analyse the performance of the assumptions. Both secondary and primary research is required to find the actual result (Hu, and Wang, 2018). Cyber security information can be gathered from both primary and secondary research. Most of the researchers used to collect data by

using primary and secondary research. Data collection plays an important role in all streams of research. Primary data collection method is a type of data collection method which is used to obtain and gather information through experiments, observation, and surveys. Primary data collection is of two types- quantitative data collection and qualitative data collection. Most of the primary data collection is used to collect data. Quantitative research is the type of research that is expressed in terms of numbers and charts. There are certain theories and assumptions needed to find the actual answer. The quantitative methods are close-ended questions. The result of the answers is expressed in the form of graphs and tables. Some of the quantitative data collection methods are surveys, experiments, and observation. The survey needs to be done in order to find which people are having problems regarding the cyber security of email. Certain experiments need to be done in order to get the actual result of the topic. Through the experiment variables are controlled. Qualitative research is expressed in words and expressions. Some of the qualitative data collections are focus group, interviews, and literature review. Qualitative reach contains open-ended questions. Through the interview, the interviewer takes the information from the interviewee. By doing a survey , the interviewer gets relevant information from the people (Ahlborg, 2021). The focus group is another source from where the information can be obtained. In the focus group the people sit together in order to discuss the particular topic so that relevant information can be gathered. There should be five to seven people sitting together in the focus group. The moderator is there to control the discussion regarding the topic. The literature review is another source from which information can be gathered. Different authors gave different statements regarding the topic, cyber security done to protect the email messages.

3.8 Research limitation:

According to the above-conducted study during the time of conducting the research, the researcher had to face numerous complications and challenges. Moreover, it included both positive and negative parts at the time of gathering information for the paper. During the time of data collection, the available sample set was small for the part of gathering accurate information for the research (Pirocca, Allodi, and Zannone, 2020). On the other hand, although the research was based on secondary data collection techniques, the information related to the DMARC application varied from one source to another. However, the major issue was associated with the system of gathering the data for the part evaluating the current complication faced by the system for the part of mitigating and controlling the issues in the near future.

Thus, the respective segment leads to increased time consumption for the researcher to complete the research within the planned schedule. On the other hand, the second data collection technique used in the research paper had wide data. It leads to a challenging part for the researcher in the area of selecting the beneficial information for the successful conduct of the research. Moreover, the selected design, methodology and artefact for the research work was so wide that it was difficult to conclude the actual findings and analysis within the overall segment of the conducted study.

3.9 Conclusion:

This chapter provides a detailed summary and outline of doing the research. Their research focuses too much on qualitative and quantitative techniques. The open-ended and Coles end questions are asked in order to get the result of the cyber security made to protect the email messages. There are millions of people using email for their important purpose. If the email gets hacked, then information will be stolen. It is better to keep the information safe so that

hackers do not black main normal people. This chapter gives the entire summary of the methodology. This chapter contains a research strategy that specified the strategy required to complete the project. The research design specifies the exploratory research which gives the appropriate result of the study. This chapter also highlighted the research limitation and research philosophy and other statements regarding the topic of cyber security done to protect the personal and professional mail Id.

4: Findings and Analysis:

The primary aim of the current research paper is to find out and to confer the application of the DMRC and its importance in managing emails. Form the technical specification, the security mechanism is used for, and it also ensure the end-to-end encryption in mail. Above all the particular strategy helps to monitor the internet traffic and monitor the authentication of the mails for further protections. Moreover, the security mechanism is based on the results of DKIM and SPF that helps to determine the place of the email domain and support the mechanism of the system (Ogwu et al., 2020). Even DMRC found to help the record of DNS that makes the users safer hand. The process of work follows a specific algorithms and process that undergoes through status of SPF and DKIM status. Nevertheless, the process underpass through SPF or DKIM rather hardly observed to pass both. Hence, it referred as "DMRC alignment" often that denote the identifier alignment.

Apart from this, the DMRC records convey the server of email along with the XML reports to the reporting address of email. Furthermore, the process shuffled only between the registered address instead of addressing random or unauthentic address. The process may also determine the movement of the ecosystem that allows the users to identify their email domain. In case of the users avoiding the mechanism of DMARC, the user may figure out the issues regarding phishing, spam and other filtering issue. On the other hand, with the application of the same one may get reliability for brand increase or monitoring domain (Ogwu, 2016). The specific disparity that may define is with the usage of DMARC the user can have entire permission to manage their mail flows and to block any unsafe email whereas without the mechanism one may not be able to do so.

DMARC is one of the pillars of email authentication. DMARC is used to protect the authentication protocols of the email address. DMARC provide direction on what the receiver does if the message from the domain fails the test of authorization. It has a power to protect the domain from fraud usages. There are many people use email for their important purpose. This day's emails are getting into wrong hands which is not good. In addition to that more than thousand mails are transferred on the daily basis for business and other purposes. This email messages are really important for daily use for normal human beings. The Email is not only use in the business purposes but used in other purposes as well. In order to safeguard those email, DMARC software is used to protect the data. People send important document through this email.

4.1 Design Specification:

SMTP was designed ten years ago which is even a power concept which is interoperability. It is one of the simple trustworthy protocols for email transaction. After few years it was noted that internet was one of the dangerous places for the human beings. It is not that important and revenant information are sent over the internet, but spam messages were also sent through this email messages. Moreover, there are many hackers who steal this email for blackmailing normal people. Through the investigation, it has seen that there are modern ways to protect the email such as DMARC and DNS. This modern security is really helpful

to detect the authentic sender and receiver. DMARC and DNS really safeguards the data so that the information cannot be leak in the wrong hands. Proper security had to done in order to protect the email so that it do not goes into wrong hands. In addition to that there are many cybercriminals who all are making phishing attack on the customer's assets so that they can draw as much money as they can. DMARC offer direction on what the receiver should do if the message from the domain fails the authorization test. DNS security avoid insecure host-based resolver and its maintained. DMARC records are stored on the DNS server that your email server uses. Within your DNS server, you can create and modify DMARC, SPF and DKIM records to secure your mail server. All the records of DMARC are stored on the DNS server. When your system receives an email, it will do a reverse DNS lookup to see what domain name it came from. Then it compares this with the MX records to see if this server is registered as an email server. If not, it can reject the email as spam. There are huge number of phishers who target the numerous numbers of people for blackmailing and fraudulent practice. Therefore, DMARC and DNS reduce the phishing activity and tried to help the general people to be protected. Cybercrime is too much in found in the present generation so in order to protect them this modern system are being implemented.

DMARC may protect against spoofing, but it doesn't protect against all forms of email threats. Having DMARC in place does not protect against malicious attachments or links in emails, or from emails that are not coming from your domain. A simple DMARC email policy also doesn't protect against cousin domain attacks. Simply put, cousin domain attacks register domains that look very similar to real companies in hopes of tricking recipients into clicking malicious emails. Overall aim of the study is related to enhancing the security of emails. This study will assist with the fact that email security catchy enhance which includes crucial factors such as safeguarding the confidentiality of the data of the users how to preserve the integrity of the data along with promoting the availability for those who are authorized users.

Since Email is the most common entry point for cyber threats, and people are the weakest link in the system so if your employees are clicking harmful links in emails or responding to phishing messages, no amount of encryption or technology will be able to safeguard your system. The most effective strategy to protect your company's data is to implement a company-wide email awareness training program that will educate everyone on what they should and should not do. In addition, to prevent spam and phishing, you should configure SPF, DKIM, and DMARC, which are email security standards that help ensure that your domain is safe and can't be forged. To protect your email, it is recommended that you use an SPF record. Always use an SPF checker to make sure everything is in working condition.

Most precisely the benefits that the users may get with the use of DMARC is related to the security, visibility, and delivery along with the identity. In part of the security, the user may disallow the email domains that are unauthorized or unregistered for protecting the existing users from spam or fraud. Moreover, it helps to increase the visibility in time of maintaining the internet or email domain and helps to gain accurate safety measures (Eboibi, 2021). On the same time, it helps to use the modern plumbing and the mega companies for delivering the mail that even helps to get the identity across the huge footprints. Not only the safety measurements but also the set up or implication of DMARC in the email requires enough knowledge and skill for ensuring the integrity process.

5. Implementation:

The configuration of the application may find to be complicated rather the implication is not easy nutshell. The email security that gets by default is not so strong even not allows the users to get peak security as such DMARC. Hence, the DMARC act as email server as a web host or for administrating or to configure the policies for maintaining the authenticity of email using. Hardly, DMARC found to have default security standard whereas the adoption of the same to get the security benefits as well. The mechanism requires the email administrator or the organization for setting up security policies along with to configure or develop existing ones. According to the recent survey reports, the organizations that are adopted and manipulated by the US government have adopted the security application major in number across the world (Hakim et al., 2020). The sender framework regards as the most flawless part of the DMARC deployment that assists to setup the policies along with the configurations. On the same, the particular helps to specify the exchanges that are authorized and have the domain name.

The basic level that one seeks to follow in time of DMARC adoption and implication is.
* Logging in domain register for managing the option of DNS setting to configure the further management.
* Select the option of “Add new record” option and clicking the “TXT” record
* In section of the host’s name register the domain name by signing the existing address or with @

Pros and cons likewise the other applications, DMARC have impartial impact on the organization that develop the authenticity of technology and instigate the security capacity of the same. Befits that have aforementioned and the protocol for authorized use has the insight of DMARC policies. Hence, with the benefits, back draws may measure that effects the internet use for safety measurement. At most the issue that the users usually found in time of using the system and managing security application in their email is its tricky configuration and implication complexity. The standard of the application is high enough which define as pragmatic though may bother the user in time of implication and operation of the system use (Leukfeldt and Roks, 2020). Moving forwardly, the issue that may identify is related to the cloud computing as DMARC is not enabling to work in the cloud system. Configuration of the application that should be accomplished before using the system in email management may grant as the initial stage whereas the similar security application ends up with it. Not only the configuration, even after the configuration one may find complication and issues due to less knowledge and may not be able to work with the same.

DMARC is the complete form of standard that allows the users form preventing the attack of spammers. Moreover, it is the designed mode of domain that enables the users to deliver the information from one segment to another with the actual permission of the users. However, the complete process associated with the same is known as spoofing. On the other hand, the beneficial part of DMARC process is associated with the functional and operational aspect of its visibility. Moreover, during the point of time the e-mail is send from one user to another it ensures that the e-mail is received to the users at the right point of time. Moreover, the complete process associated with the system of DMARC is associated with the brands deliverability along with the e-mail security strategy. In this, within the respective segment the first and foremost factors appear to be the factor of visibility. Under this, the complete process associated with the same systematically monitors and evaluates the e-mails that are sent from the domains for the part of ensuring the systems authentications. However, the complete process associated with the same is performed through the application of DKIM and SPF process. The second core factor within the respective segment is associated with the

function of brand protection. Since, it is the understandable part that the spoofed messages that are present in the e-mail might bring complete impact on the customer perception for the brand.

However, the overall process related to the factor of DMARC function prevents and controls the operation of users from any mode of phishing. It will enable the organization in the area of maintaining and developing the organizational security as a whole within their complete functioning for the current and future perspectives. The most supportive segment within the complete function of DMARC is that with the advanced application of DKIM system it validates the complete process associated with the authentication of e-mails. The complete process associated with the respective function systematically verifies that the messages were not at all altered during the time of transit. In simple words, it can be systematically stated that the complete functional aspects associated with the system of DKIM process prevents a third party from accessing the e-mail without permission. Moreover, within the respective segment, the other core benefit of DKIM process is that it includes the application of ISP that helps in the area of building and developing a reputation in the domain.

5.1 Evaluation:

During the point of time the email is sent under the DKIM process the complete information associated with the e-mail signed and processed by the private key along with this complete information associated with the same is stored under the mail server. However, the complete functional aspects associated with the system of ISP systematically verifies and evaluates the authenticity and integrity of the messages that are sent, However, the complete process associated with the same is performed and evaluated with the complete application of DKIM process. On the other hand, the respective factor guarantees the complete process signed with the system of private key after the information for the same is processed from the part of public key. It is the core initiative of the organization to accurately ensure that the information that are processed and evaluated from the part of private key must be kept in secret. Moreover, during the point of time when step by step information that are sent to the administrator during the process will enable to make the functionality associated with the process easier. Thus, the operational aspects associated with the system of DKIM are regarded as the important technique of functionality undertaken within the system of DMARC function.

6: Expected Outcome:

Nowadays email protection is very crucial due to the cyber security threats which involve social attacks. Various businesses are attacked via their vulnerable points such as emails. Phishing emails, for example, which can convince users to disclose personal information, approve false bills, or download malware that can infect the company's network.
Unlocked domains are exposed to the possibility of being attacked or harmed.
Even after taking better security measures to protect the crimes on the channels in the current years the rate of crimes on these channels is still escalating with every passing year.
Major percentage of hacking attacks of data violation includes email scam. There are several reasons to use a protected or secured emails, like it helps to decrease the rate of risk in business, it also helps preserving all the information which are confidential, it also increases the rate of invalidate chances to get and give reply to the messages, it also helps to identify and avoid larceny, it also helps to abandon the messages which is sent. This is the place where values are added to your email it is DMARC- Domain Based Authentication Reporting and Conformance. Amenity provided by DMARC is that they accommodate complete observation in all types of channels in email, and it also helps to make it visible the scam

attacks. DMARC is proven to be robust. DMARC have the capability to diminish the effect of phishing and malware attacks, it put a stop to spoofing and preserve against brand abuse, scam, and avoid business email compromise.

There are several organizations that are getting effected as various hostile emails are sent to their clients on their behalf. DMARC have got the right to stop this kind of attacks.
A cyber security risk assessment can help you discover areas where your company is vulnerable and develop a plan of action, which should include user training, advice on safeguarding email platforms, and protecting company's data assets. Nowadays email protection is very crucial due to the cyber security threats which involve social attacks. Various businesses are attacked via their vulnerable points such as emails. Phishing emails, for example, which can convince users to disclose personal information, approve false bills, or download malware that can infect the company's network.
Unlocked domains are exposed to the possibility of being attacked or harmed.
Even after taking better security measures to protect the crimes on the channels in the current years the rate of crimes on these channels is still escalating with every passing year.

Major percentage of hacking attacks of data violation includes email scam. There are several reasons to use a protected or secured emails, like it helps to decrease the rate of risk in business, it also helps preserving all the information which are confidential, it also increases the rate of invalidate chances to get and give reply to the messages, it also helps to identify and avoid larceny, it also helps to abandon the messages which is sent.

This is the place where values are added to your email it is DMARC- Domain Based Authentication Reporting and Conformance. Amenity provided by DMARC is that they accommodate complete observation in all types of channels in email, and it also helps to make it visible the scam attacks. DMARC is proven to be robust. DMARC have the capability to diminish the effect of phishing and malware attacks, it put a stop to spoofing and preserve against brand abuse, scam, and avoid business email compromise.

There are several organizations that are getting effected as various hostile emails are sent to their clients on their behalf. DMARC have got the right to stop this kind of attacks.
A cyber security risk assessment can help you discover areas where your company is vulnerable and develop a plan of action, which should include user training, advice on safeguarding email platforms, and protecting company's data assets.
By using DMARC we can make the world aware about handling and to identify the uncertified email domain usage. DMARC mainly follows three policies which are-

- It has got the right to monitor the traffic of your email in which any further actions cannot be taken.
- It has its own setting update to send unofficial junk mails.
- And the third policy which DMARC consider as their ultimate target is to make sure that the uncertified or unofficial emails does not get sent at any point.

In nowadays email has become a necessity for all type of users and it has got high chances that the network might get attacked in absence of DMARC server. Without DMARC it is not easy to identify whether the email is real or fake. With the help of DMARC the domain owners can prevent their domain from sending fraudulent mails. DMARC protects the domain.
An operator of internet domain will be able to inform the world with the help of DMARC that the mails sent by me are all recognized through DMARC, be at ease to send mail that appears that it is me.

DMARC has a technology that enables the operators to recognize authenticate mails rather than removing scam mails. It does not allow all type of operators to identify which is an authorized and unauthorized email. DMARC has taken place of previous models with better security features to correct the imperfection out of the bad mail security with the new and improvised filtered model. For controlling a domain what happens when a mail fails authentication DNS txt have been published.
Using of DMARC as a part of email operation can-

- Verify the valid mails and all the sources of the sender's domain. It discards all the scam mails from the verified mails.
- It can report policies that can tell the mail service provides to distribute and predispose the unauthenticated or unidentified mails.
- It can obtain surveillance on every domain of all the email messages from across the net.

There are also some addition benefits of using DMARC on your email server. Many Government organisations and reputed brands have adopted DMARC as-

- DMARC can help to identify whether the company's domain is being used for any kind of fraud practices or not.
- It can make sure that no fraud or deceptive mails are being sent and only the authenticated and valid mails are getting sent.
- It can help to point out the origins and the appearance of the hazards by which preventive measures can be taken to protect from such attacks.
- It can improve their overall email reputation score and trustworthiness.

DMARC records are stored on the DNS server that your email server uses. Within your DNS server, you can create and modify DMARC, SPF and DKIM records to secure your mail server. DMARC may protect against spoofing, however it does not protect against all forms of email threats. Having DMARC in place does not protect against malicious attachments or links in emails, or from emails that are not coming from your domain. A simple DMARC email policy also does not protect against cousin domain attacks. Simply put, cousin domain attacks register domains that look very similar to real companies in hopes of tricking recipients into clicking malicious emails.
It has been reported that the number of domains using DMARC rose from 125,000 in January 2017 to almost a million in January 2020. Which indicates that more organizations in the future will adopt using DMARC.

DMARC is beneficial at a small scale, it can improve your reputation and increasing your visibility into your email programme, but it also benefits the wider email community by setting a consistent standard that increases the overall trustworthiness of email communications.
DMARC can provide the domain users with the following benefits :

- Anyone who uses emails will definitely get an advantage of using DMARC. When there is a strong security against the prevention of scammed and fake e-mails the reputation of the brand is also enhanced, and their clients also intend to trust them even more.
- It can prevent the usage of fraud practices of your email by guarding it from spams and hackers.
- It can help to make aware as to who is sending mails by using your domain from all over the world.

DMARC can block unsolicited emails. The phishing mails are constructed in such a way that it can mislead the victims into believing that the mails that are delivered to them are from an

authenticated or trusted sender. It is possible with the help of email spoofing. It is a method that does not require any proper hacking skill but still it will cause serious damage if it is done in a proper way. This is the reason why DMARC can be used in order to protect the domain from any kind spoofing issues.

To make use of DMARC, DKIM AND SPF is compound, and it needs measures. Every time a business adds on a latest service for example SaaS Vendor the DMARC records the alerting senders and even when the services are discarded the same thing happens.
Show name spoofing is a technique in which the hacker divulges in the sender field the name that is displayed. The display name that is being chosen by the hacker can be of any sort which looks absolutely authentic and verified but it is actually fake and is a scam.
Natural Language Processing (NLP) is AI-Based, which helps to understand the texts and make use of text clots. It examines and analyse the texts in order to identifies the texts in order to identify the spear phishing.

DMARC is a crucial step in order to protect your business, but it has to be combined with other cyber security technologies as well in order to get excellent protection.

- DMARC which stands for domain-based message authentication reporting and conformance an email spoofing is detected and prevented by a validation system. It is used to combine few techniques which is most of the time used in frauding and junk email. Suppose email with a fake senders address that might come from an authorized organization, that is what is being prevented.

- SPF defines a Senders Policy Frameworks, this protocol is structured in such a manner that it can detect and block the mail which is a junk. It has got the permission which allows it to exchange mails, receive and send both but from such a domain which drop from an authorized IP address that got approved from that particular domain.

- Domain Key Identified Mail (DKIM) is a substantiate method that helps identify email spoofing, it gives permission to the receiver to check whether a mail which claim to come from a specific domain from an authorized owner or from any other domain.

- Binding Operational Directive 18-01—The Department of Homeland Security has introduced with Binding Operational Directive 18-01 for agencies to upgrade and modify their email and web security more with features. These Agencies will need to execute SPF, DMARC, and STARTTLS competently.

- DMARC is an open email protocol that provides protection of the email channels from domain-level.

- It is necessary to pass through to pass SPF authentication SPF alignment and/or pass DKIM authentication and DKIM alignment for a message to pass through DMARC authentication. If a message fails while passing through DMARC, sender has the right to command receiver what to do with the message, keeping in mind the DMARC policy. There are three major policies that every domain owner can implement and that is:- (i) None; (ii) Quarantine; (iii) Reject.

- The DMARC policy of “none” is the first step. Overhear, the domain owner can ensure that whether all legalized email is authenticating properly or not. DMARC reports are

received by the domain owner to make sure that all legalized email is identified and passes authentication process. Once the domain owner is sure about the entire process, they have identified all legal senders and have fixed all kinds of authentication issues they came up with, they can move to the final policy of "reject" and block phishing or fakers, business email compromise (BES), and other email fraud attacks. And as an email receiver, an organization can ensure that whether it's secure with email gateway enforces that DMARC policy implemented to the domain owner. This will protect employees against inbound email threats including all types of junk and spam diversions.
Due to the size of DMARC reports that an email sender can receive at its extent and the shortage of transparency provided within DMARC reports, at that point of time fully implementing DMARC authentication can be difficult for the receiver. DMARC reviewing tools can help organizations to make information with sense which is included within DMARC reports. Additional data and awareness included within DMARC reports assist organizations to identify the email senders faster and more precisely. This helps to speed up the process of applying DMARC authentication and reduces the risk of blocking legal and authorized email. Those who are Professional services consultants engaged with DMARC expertise can help organizations with DMARC implementation. Consultants can help pick out all legal senders and fix all type of authentication issues and can even work with email service providers to make sure that they are authenticating properly. Organizations can create a DMARC records and start gaining clarity through DMARC reports by implementing DMARC policy of "None."

By using DMARC we can make the world aware about handling and to identify the uncertified email domain usage. DMARC mainly follows three policies which are-
It has got the right to monitor the traffic of your email in which any further actions cannot be taken. It has its own setting update to send unofficial junk mails. And the third policy which DMARC consider as their ultimate target is to make sure that the uncertified or unofficial emails does not get sent at any point. In nowadays email has become a necessity for all type of users and it has got high chances that the network might get attacked in absence of DMARC server. Without DMARC it is not easy to identify whether the email is real or fake. With the help of DMARC the domain owners can prevent their domain from sending fraudulent mails. DMARC protects the domain. An operator of internet domain will be able to inform the world with the help of DMARC that the mails sent by me are all recognized through DMARC, be at ease to send mail that appears that it is me.

DMARC has a technology that enables the operators to recognize authenticate mails rather than removing scam mails. It does not allow all type of operators to identify which is an authorized and unauthorized email. DMARC has taken place of previous models with better security features to correct the imperfection out of the bad mail security with the new and improvised filtered model. For controlling a domain what happens when a mail fails authentication DNS txt have been published.
Using of DMARC as a part of email operation can-

- Verify the valid mails and all the sources of the sender's domain. It discards all the scam mails from the verified mails.
- It can report policies that can tell the mail service provides to distribute and predispose the unauthenticated or unidentified mails.
- It can obtain surveillance on every domain of all the email messages from across the net.

There are also some addition benefits of using DMARC on your email server. Many Government organizations and reputed brands have adopted DMARC as-

- DMARC can help to identify whether the company's domain is being used for any kind of fraud practices or not.
- It can make sure that no fraud or deceptive mails are being sent and only the authenticated and valid mails are getting sent.
- It can help to point out the origins and the appearance of the hazards by which preventive measures can be taken to protect from such attacks.
- It can improve their overall email reputation score and trustworthiness.

DMARC records are stored on the DNS server that your email server uses. Within your DNS server, you can create and modify DMARC, SPF and DKIM records to secure your mail server. DMARC may protect against spoofing, however it does not protect against all forms of email threats. Having DMARC in place does not protect against malicious attachments or links in emails, or from emails that are not coming from your domain. A simple DMARC email policy also does not protect against cousin domain attacks. Simply put, cousin domain attacks register domains that look very similar to real companies in hopes of tricking recipients into clicking malicious emails.

It has been reported that the number of domains using DMARC rose from 125,000 in January 2017 to almost a million in January 2020. Which indicates that more organizations in the future will adopt using DMARC. DMARC is beneficial at a small scale, it can improve your reputation and increasing your visibility into your email programme, but it also benefits the wider email community by setting a consistent standard that increases the overall trustworthiness of email communications. DMARC can provide the domain users with the following benefits. Anyone who uses emails will definitely get an advantage of using DMARC. When there is a strong security against the prevention of scammed and fake e-mails the reputation of the brand is also enhanced, and their clients also intend to trust them even more. It can prevent the usage of fraud practices of your email by guarding it from spams and hackers. It can help to make aware as to who is sending mails by using your domain from all over the world.

DMARC can block unsolicited emails. The phishing mails are constructed in such a way that it can mislead the victims into believing that the mails that are delivered to them are from an authenticated or trusted sender. It is possible with the help of email spoofing. It is a method that does not require any proper hacking skill but still it will cause serious damage if it is done in a proper way. This is the reason why DMARC can be used in order to protect the domain from any kind spoofing issues.

To make use of DMARC, DKIM AND SPF is compound and it need measures. Every time a business adds on a latest service for example SaaS Vendor the DMARC record the alerting senders and even when the services are discarded the same thing happens. Show name spoofing is a technique in which the hacker divulges in the sender field the name that is displayed. The display name that is being chosen by the hacker can be of any sort who looks absolutely authentic and verified but it is actually fake and is a scam. Natural Language Processing (NLP) is AI-Based, which helps to understand the texts and make use of text clots. It examines and analyse the texts in order to identifies the texts in order to identify the spear phishing.

DMARC is a crucial step in order to protect your business, but it has to be combined with other cyber security technologies as well in order to get excellent protection. DMARC which stands for domain-based message authentication reporting and conformance an email spoofing is detected and prevented by a validation system. It is used to combine few

techniques which is most of the time used in frauding and junk email. Suppose email with a fake senders address that might come from an authorized organization, that is what is being prevented. SPF defines a Senders Policy Frameworks, this protocol is structured in such a manner that it can detect and block the mail which is a junk. It has got the permission which allows it to exchange mails, receive and send both but from such a domain which drop from an authorized IP address that got approved from that particular domain.

7: Conclusion and Recommendations:

7.1: Recommendations

The paper has provided an opportunity to investigate the manner in which security mail can be improved using DMARC and DNS data. Therefore, based on the above understanding, it can be recommended that companies can integrate DMARC policy to ensure the security of emails. Many email providers are integrating this policy in order to minimize the scope of scams as it can be a good initiative for email security. Even though there have been various methods through which emails from spoofed addresses are tried to be identified, frauds in the email are still the major concern (Cobb 2019). DMARC provides the ability to notify the email provider to understand the ways to be undertaken when the emails are not being protected by SPF or DKIM. In this case, the policy can be integrated into which email systems used by the spammers can be identified. Therefore, the DMARS policy published in the DNS can be helpful to indicate if the messages are protected or not and the reason for failure in the authentication. For example, Google is aiming to move towards a very strict DMARS policy to be integrated into Gmail where the mails will automatically get rejected once it fails to meet authentication checks. This can be a big step to deal with spoofed emails and the way Google works (Mimecast 2020). For this purpose, Google has decided to support Authenticated Received Protocol to allow mail operators to send mail via Gmail account and not through the server. This protocol also tracks record any modification made in the message or caused by any failure in the authentication of DMARC when the mail reaches its final destination.

Furthermore, it has been found that the implementation of DMARC into the DNS record can be highly effective to gain in-depth insight into the different channels of email. In this case, ISPs will offer Aggregate and Forensic DMARC reports at regular intervals that can be sent to the email addresses that are being integrated into the DMARC record (Strom 2019). The Aggregate DMARC Report will provide an overview of email traffic including IP addresses that attempts to send emails using the domain name. On the other hand, Forensic DMARC reports can also be equally effective as it provides real-time data, include original message headers and original messages but can be only sent at the time of failure. The use of DMARC Analyzer will help to monitor and analyse the SPF, DKIM and the results of DMARC all at the same time. Also, the consideration of the 3 DMARC policies is extremely important to understand the end results of the emails (Cobb 2019). The ‘none’ policy will help to collect and monitor data, the ‘quarantine’ policy will automatically deliver the fraud emails to the spam and the ‘reject’ policy will not deliver malicious mails at all. It is being recommended for IT managers to look for the above integration to ensure security solutions. As discussed in the above part of the paper, Google has also been a motivational factor for other enterprises. Adding these protocols can be highly beneficial to integrate the best email solutions that can keep the data of customers protected.

The security vendors are also required to improve their services by making the process of deployment much easier. The best examples can be Vali mail, Barracuda, and Agari that have adopted a free interactive tool to create the records of DMARC (Strom 2019). Also, there is a

requirement to adopt the new standard of Brand Indicators for Message Identification which will help to display logos on each mail until the spammers are able to display phony logos on the screen. There is a need to implement email infrastructure that comprises a few protocols to ensure that the mails are not being forged easily and blocked before getting into the inboxes. The first step is to use a combination of standard authentication and encryption tools and also adding DNS records to ensure proper authentication of mails coming from the domain (Mimecast 2020). The next step is to use message headers that are more likely to separate the actual content from the message itself such as To, From, and BCC options.

Arriving at the best practices for email deliverability, there are a few email authentication standards that need to be followed. Nowadays, spam emails are constantly increasing, and customers are more concerned to ensure that subscribers are sending an email that is valuable and safe (Pathwire 2019). Therefore, the following points can be followed to ensure the successful and safe delivery of the emails.

- At first, it is most important to determine the origin of the emails received.
- Then the next step is to ensure that the sources of the received emails are legitimate.
- The third step is to ensure that the emails are not being ordered during their processing stage (ARSENAULT 2020).
- And the last step is to communicate with the service providers of email to make sure authentication protocols have been used for proper authenticating the emails.

This infrastructure of the email will allow the spam filter to separate the emails that are spam or malicious. This can also require the use of more than one authentication standard that will help to protect the emails in a better manner and remain secured from attacks (Pathwire 2019).

It is also recommended to protect the lists of emails with the process of email validation. It has been observed that the list of subscribers may get overlooked and emails are being sent without knowing anything about it that can be dangerous for the reputation of the sender. Therefore, the use of services that can help to remove spam mails can be beneficial. Also, to validate the email lists, the tools that can be used are MailGun, SearchBug, TowerData, and ZeroBounce (ARSENAULT 2020). The user can also implement a seed list testing method that helps to validate the delivery of the emails before sending it to entire lists. Setting up the Google Postmaster tool will also help to track the email deliverability metrics including spam issues and instantly corrects them. Moreover, this system is easy to set up.

7.2:Conclusion:

It can be concluded that, the e-mail providers both under the domestic and international market are giving important emphasis in the area of availing innovative expansion strategies on DMARC policy. The main reason is for the part of preventing and controlling the factor of e-mail fraud for the future. Even, through within the respective segment there are numerous innovative method and techniques adopted for the same, the respective issue associated with e-mail fraud still remains a complicated issue in the market. However, the complete system launched for span filters remains an effective part, but it still lags behind the ever-changing tactics of the spammers. Moreover, the respective condition creates a challenging part for the administrators in the area of failing to remove the blocked messages by these respective filters. Moreover, under this several systematic mechanisms like SPF and DKIM systems have played a supportive part for the part of regulating the respective issue of email fraud. Besides, through the respective process associated with the same, SPF system is considered to be the competitive part when bringing in comparison with other software for mitigating email fraud in the future. However, the entire workings of the domain name system can be discussed as follows.

It is seen that when a user searches in the unique resource locator, a request is immediately sent to the DNS server rather than sending the request to the Google server. On the other hand, the other application such as DKIM adds a mode of digital signature to the email process. It avails better system of facility through which the messages that are delivered from the part of users can easily be published through a DNS application feature. Moreover, through the complete process associate with the same installation of firewalls is an effective measure to prevent attack from external sources by providing a sheet between the computer and the hacker. On the other hand, it is observed that a lot of popup takes place at the time of browsing a particular website. However, the respective measures are also most effective sources of attempts for making phishing attacks. It is advised to click on the close option of these ads in order to reduce the attack of phishing scams. Under this, according to the conducted studies the first and foremost essential responsibility is to translate the domain name into an IP address. With the help of this responsibility, it becomes easier to remember a large bunch of numbers.

On the contrary, for the part of making the respective process upgraded in the future, it includes certain core initiative to be undertaken within the overall process. Moreover, the second most essential responsibility of a domain name server is to specify the mail servers were responsible for distribution of information for the domain name. On the other hand, there is lot of links required for determining the connection prevailing between the computers. With the help of an IP address, it becomes easier to address the location of the internet. In this based on the developed features there are four sets of numbers ranging from 0 to 225 which are used for setting up the IP address. Through the application of these respective steps, it is observed that the occurrence of phishing scams and attacks in the email can be easily reduced by the user account. Under this, the respective tips play an essential role in minimizing the scams of cybercriminals which are associated with the emails. On the other hand, there are a lot of phishing attack methods which are used every day. Moreover, through the effective application of DNS, it becomes easier to use the internet and remember all the IP addresses. Moreover, with related to this respective segment the highest internet speed can be enjoyed with the help of DNS. However, it is considered to be some of the most vital benefits which are utilized by companies and individuals with the help of DNS. Moreover, the process of implementation of DMARC is very simple and easier. For this purpose, a domain name system (DNS) server administrator is required. On the contrary, DNS server administrator is added to your DMARC record. This meets the entire monitoring process of the domain much easier. Furthermore, the administrators of the networks have a right to delegate authority over sub domains of their name space to other name servers. However, under this there are a lot of records which are stored in the database of domain name system. it helps in translating readily memorize domain names to the internet protocol addresses in a numerical manner for identifying and locating computer services with different network protocols. It includes certain techniques and methods that include various ways in which domain-based message authentication reporting and conformance helps in handling unauthorized use of email domains. Moreover, the complete process associated with the system of providing security, visibility, identity, and delivery. On the other hand, the validation process is conducted by DMARC for giving the sender a report on the attempts to use the domain for sending mail. However, the respective process of visibility allows the sender to tune their policy relating to the new threats which are emerging in the near future. It will be supportive part for the customers in the area of preventing and controlling any mode of complications and challenges for the upcoming times. However, for the purpose of

avoiding the occurrence of email scams for companies, it is observed that it is very essential to prevent spoofing. This will help the business against brand abuse.

References:

Derouet, E., 2016. Fighting phishing and securing data with email authentication. Computer Fraud & Security, 2016(10), pp.5-8.

Kumar, S. and Somani, V., 2018. Social media security risks, cyber threats and risks prevention and mitigation techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp.125-129.

Mukherjee, S., 2019. Overview of the Importance of Corporate Security in business. Available at SSRN 3415960.

Ogwu, S., Sice, P., Keogh, S. and Goodlet, C., 2020. An exploratory study of the application of mindsight in email communication. Heliyon, 6(7), p.e04305.

Rastenis, J., Ramanauskaitė, S., Janulevičius, J., Čenys, A., Slotkienė, A. and Pakrijauskas, K., 2020. E-mail-based phishing attack taxonomy. Applied Sciences, 10(7), p.2363.

Simpson, J., 2016. Email Archiving Systems Interoperability.

Stojkovski, B. and Lenzini, G., 2020. Evaluating ambiguity of privacy indicators in a secure email app. In Proceedings of the Fourth Italian Conference on Cyber Security, Ancona Italy, February 4th to 7th, 2020 (pp. 223-234). CEUR-WS. org.

Eboibi, F.E., 2021. Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures. Commonwealth Law Bulletin, 47(1), pp.113-142.

Field, H., 2020. DMARC D. Crocker Internet-Draft Brandenburg InternetWorking Intended status: Standards Track July 27, 2020, Expires: January 28, 2021.
Grilli, M.D., McVeigh, K.S., Hakim, Z.M., Wank, A.A., Getz, S.J., Levin, B.E., Ebner, N.C. and Wilson, R.C., 2020. Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails. The Journals of Gerontology: Series B.

Hakim, Z.M., Ebner, N.C., Oliveira, D.S., Getz, S.J., Levin, B.E., Lin, T., Lloyd, K., Lai, V.T., Grilli, M.D. and Wilson, R.C., 2020. The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior research methods, pp.1-11.

Kagita, M.K., Thilakarathne, N., Gadekallu, T.R., Maddikunta, P.K.R. and Singh, S., 2020. A review on cyber crimes on the Internet of Things. arXiv preprint arXiv:2009.05708.
Kizza, J.M., 2020. Cyber Crimes and Hackers. Guide to Computer Network Security, pp.105-131.

Kontinen, V., 2020. Preventing email forgery in Finland: Research on the current SPF and DMARC implementations.

Kwak, Y., Lee, S., Damiano, A. and Vishwanath, A., 2020. Why do users not report spear phishing emails?. Telematics and Informatics, 48, p.101343.

Leukfeldt, E.R. and Roks, R.A., 2020. Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. Deviant Behavior, pp.1-12.

McAlaney, J. and Hills, P.J., 2020. Understanding phishing email processing and perceived trustworthiness through eye tracking. Frontiers in Psychology, 11, p.1756.

Mugarura, N. and Ssali, E., 2020. Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. Journal of Money Laundering Control.

Nayyar, A., Rameshwar, R.U.D.R.A. and Solanki, A., 2020. Internet of Things (IoT) and the Digital Business Environment: A Standpoint Inclusive Cyber Space, Cyber Crimes, and Cybersecurity. The Evolution of Business in the Cyber Age, 10, pp.9780429276484-6.

Pajankar, S., 2020. Cyber crimes and cyber laws in India. Delta National Journal Of Multidisciplinary Research, 7(1), pp.25-29.

Särökaari, N., 2020. Phishing attacks and mitigation tactics.

Sharma, T. and Bashir, M., 2020, July. An analysis of phishing emails and how the human vulnerabilities are exploited. In International Conference on Applied Human Factors and Ergonomics (pp. 49-55). Springer, Cham.

Tatang, D., Zettl, F. and Holz, T., 2021. The Evolution of DNS-based Email Authentication: Measuring Adoption and Finding Flaws.

Wash, R., 2020. How experts detect phishing scam emails. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2), pp.1-28.

Kour, J. and Ahmed, H., 2020. Email attacks: Investigation about the vulnerability of the Swedish organizations against email threats.
Tatang, D., Zettl, F. and Holz, T., 2021. The Evolution of DNS-based Email Authentication: Measuring Adoption and Finding Flaws.

Kontinen, V., 2020. Preventing email forgery in Finland: Research on the current SPF and DMARC implementations.

Chen, J., Paxson, V. and Jiang, J., 2020. Composition kills: A case study of email sender authentication. In 29th {USENIX} Security Symposium ({USENIX} Security 20) (pp. 2183-2199).

Patsakis, C., Casino, F., Lykousas, N. and Katos, V., 2020. Unravelling ariadne's thread: Exploring the threats of decentralised dns. IEEE Access, 8, pp.118559-118571.
Malinen, L.M., 2021. The Human Element in IT Security.

Hu, H. and Wang, G., 2018. End-to-end measurements of email spoofing attacks. In 27th {USENIX} Security Symposium ({USENIX} Security 18) (pp. 1095-1112).

van Dongen, V., 2018. Verifying email security techniques for Dutch organizations.

Ahlborg, A., 2021. How mail components on the server side detects and process undesired emails: a systematic literature review.

Pirocca, S., Allodi, L. and Zannone, N., 2020, December. A Toolkit for Security Awareness Training Against Targeted Phishing. In International Conference on Information Systems Security (pp. 137-159). Springer, Cham.

ARSENAULT 2020, Email Deliverability: Best Practices For Getting Your Emails Into The Inbox, rejoiner.com, viewed 11 August 2021, <https://rejoiner.com/resources/email-deliverability/>.

Cobb 2019, How can a DMARC policy improve email security?, SearchSecurity, viewed 11 August 2021, <https://searchsecurity.techtarget.com/answer/How-can-a-DMARC-policy-improve-email-security>.

Mimecast 2020, What is DMARC? What You Need to Know in 2020, DMARC Analyzer.

Pathwire 2019, Email Best Practices — Mailgun API documentation, documentation.mailgun.com, viewed 11 August 2021, <https://documentation.mailgun.com/en/latest/best_practices.html>.

Strom, D 2019, What are DMARC, SPF and DKIM? How to master email security with these protocols, CSO Online.

Kontinen, V., 2020. Preventing email forgery in Finland: Research on the current SPF and DMARC implementations.

Hu, H., Peng, P. and Wang, G., 2018, September. Towards understanding the adoption of anti-spoofing protocols in email systems. In 2018 IEEE Cybersecurity Development (SecDev) (pp. 94-101). IEEE.

Tatang, D., Flume, R. and Holz, T., A First Large-scale Analysis on Usage of MTA-STS. Portier, A., Carter, H. and Lever, C., 2019, June. Security in Plain TXT. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 374-395). Springer, Cham.

Tatang, D., Zettl, F. and Holz, T., 2021. The Evolution of DNS-based Email Authentication: Measuring Adoption and Finding Flaws.

Kodama, D. and Okada, K., 2017. Applications Area Working Group G. Yasutaka Internet-Draft Rakuten, Inc. Intended status: Informational T. Akagiri Expires: January 29, 2018 Regumi, Inc.

Draper-Gil, G. and Sanchez, I., 2019. My email communications security assessment (MECSA): 2018 results.

Raulot, A., 2019. Bypassing phishing protections with email authentication. Master Security and Network Engineering, 5.

Keliiaa, C.M., 2019. Protection of Intersecting Information Communications Operational and Virtual Critical Infrastructure (No. SAND2019-3664C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Nowitz, J., 2018. A Modern Perspective on Phishing: An investigation into susceptibility to phishing attacks between mobile and desktop email clients.

Titus Jr, V., House, J.M. and Covin, J.G., 2017. The influence of exploration on external corporate venturing activity. Journal of Management, 43(5), pp.1609-1630.

Vasquez, M.H., 2018. The financial crimes management of account takeover fraud (Doctoral dissertation).