Enhancing Email Dispersion Enforce Using Mail Server

A.Sagayarani, MBA, Assistant Professor, Department of Management Studies, Sri Ramakrishna Engineering College, Coimbatore -641 022, Tamilnadu, India.

G.Dinesh Hariharan, II MBA, Sri Ramakrishna Engineering College, Coimbatore -641 022, Tamilnadu, India

ABSTRACT
The communication plays the most important function in today's world. It may be days or weeks to make the message available to others. Mail service details with the website that manage the electronic way of communication. Through this research study we can create our own user id, send mails to any user and manage inbox. In addition greetings can be sent to friends and peers. We can view incoming mails and greetings and even delete them. Resume can be stored and changed whenever necessary. Any mail related report can be viewed through the site. Deletion of unwanted mails can be made to manage memory. DNS is a relatively simple, text-based protocol, in which one or more recipients of a message are specified along with the message text and possibly other encoded objects. The message is then transferred to a remote server using a procedure of queries and responses between the client and server. In this study, the findings revealed that the protection level for the confidential data are low with no proper accessing rights given to the employee and also the tracking of the email ids by any person within and outside the organization.

KEYWORDS: Mail Server, Communication, Memory, Text-Based Protocol.

1. INTRODUCTION

The communication across the world is must in the modern age communications through postal may take more time. It may be days or weeks to make the message available to others. E-Mail service details with the website that manage the electronic way of communication. Through this project we can create our own user id, sends mails to any user and manage inbox. In addition greetings can be sending to friends. We can view incoming mails and greetings and even delete them. Resume can be stored and changed whenever necessary. Any mail related report can be viewed through the site. Deletion of unwanted mails can be made to manage memory.

DNS is a relatively simple, text-based protocol, in which one or more recipients of a message are specified along with the message text and possibly other encoded objects. The message is then transferred to a remote server using a procedure of queries and responses between the client and server. By these feasibility of using the email in organization the confidential folders are being misused by the employees so by using the mail server this sort of drawback can be avoided and only the authorized person can access the folder. By this we can avoid the hackers and avoid the unnecessary spam mails which indirectly attack the folders which are confidential.

An email client knows the outgoing mail SMTP server from its configuration. A relaying server typically determines which SMTP server to connect to by looking up the MX (Mail exchange) DNS record for each recipient's domain name (the part of the email address to the right of the (@) sign). Conformant MTAs (not all) fall back to a simple A record in the case of no MX. Some current mail transfer agents will also use SRV records, a more general form of MX, though these are not widely adopted. (Relaying servers can also be configured to use a smart host.)

The DNS client initiates a TCP connection to server's port 25 (unless overridden by configuration). It is quite easy to test an SMTP server using the telnet program. DNS is a "push" protocol that does not
allow one to "pull" messages from a remote server on demand. Here the system is designed using Active Server Pages .NET with Microsoft Visual Studio.Net 2010 as front end and Microsoft SQL Server 2005 as back end which works in .Net framework version 2.0. The coding language used is ASP.Net. The reason for taking up the language is they are more user friendly and effective to the end user.

In this proposed system these are the positive notes usage of advanced DNS /POP3 Email Server with tons of features, such mailing lists, anti-spam, multiple DNS gateways, security, and compatibility with any email program. It can also be used as a dedicated mail server, or as a personal local SMTP server. It is a free DNS relay server. It allows relay emails sent to it, directly to their destination, bypassing your provider's mail server. If you need to send large quantities of email, set up a few of these servers on different computers. DNS server program helps to send email messages without help of the ISP (Internet Server Provider), directly from the local PC to recipient mailboxes and use the favorite email client along with this software the way it is used to do it before. DNS relay software allows putting emails directly to receiver mailbox. This is much faster and reliable than using DNS server provided by ISP.

2. REVIEW OF LITERATURES

Genrich, Michael (2004) : Considers the importance of the Internet service's electronic mail (email) to an organization. Comparison of several email servers; Description of mail servers; Tips on avoiding unsolicited email messages. Inset: Built-In Alternatives. Kevin Curran, Ph.D., John Honan Spam (2004) conducted study regarding the Spam which is defined as unsolicited email, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups. Victor Mendez, Julio Cesar Hernandez, Jesus Carretero, And Felix Garcia, (2004) in this study the problem of automatically filtering unwanted e-mail messages is one of increasing importance, because bulk mailers take advantage of the great popularity of the electronic mail communication channel for indiscriminately flooding e-mail accounts with unwanted advertisements are discussed. Kristin Byrond (2008) email senders intentionally and unintentionally communicate emotion and email characteristics make miscommunication likely, and I argue that receivers often misinterpret work emails as more emotionally negative or neutral than intended. Bhatnagar, Ash (2012) in this article the negotiations are about the security risks of the transmission of financial planning client data through email posed by hacking and data theft. An overview is presented of the security aspects of various email systems, passwords, and protocols, third-party and hosted servers, and communication via wireless electronic devices.

3. SIGNIFICANCE OF THE STUDY

The study arises because of the feasibility of using the confidential messages or mail in the organization by the employees and the other hackers who try to destroy the information. At present in this era the most needy is communication and that too in the trusted manner which should not harm any side of the parties that is both the employee and employers. Here even the clients are also taken into account.

4. OBJECTIVES OF THE STUDY

- To analyze whether the company email is being tracked by the any person.
- To provide security for the confidential folders in the organization.
- To provide email sending and receiving rights for the right employee.
5. METHODOLOGY

It is designed using Active Server Pages .NET with Microsoft Visual Studio.Net 2005 as front end and Microsoft SQL Server 2005 as back end which works in .Net framework version 2.0. The coding language used is ASP.Net.

6. DATA MODULES AND REPORTS

The modules used in this study are divided as below based on the needs and requirements of the organization. They are:

1. Company Creation
2. User Creation
3. User Rights
4. Hacker list
5. Mail Processing
6. Mail Configuration

**Company Creation:** It consists of entering username, password and other basic details to create a company, this module is only enabled for admin those who creates the company. While creating company all the basic company details should be entered.

![Login Page](image1)

![EMAIL DISPERSION](image2)

![Company Creation](image3)
User Creation:

Here the compaction by admin can create various users for their company, as well as they can able to share the group mails inside the group of companies. These mails will not be stored in the junk mails, because these all are confidential mails.

User Rights:
After creating the user by the admin, he can able to create user rights for the created user. So from the methods the users can be categorized as well as the prior user of the mail server will not be responsible for any other problem. This rights can be given to all the users of this mail server.

**Hacker List:**
Hacker List Display

Mail Processing:

Hacker list is the instruction detection method, which helps the user to find out the other users entering into the network. It contains an IP tracker, password checker, date of attack and time of hacking. So the user can identify who is the other user intruding into the network. So that user can identify the hackers easily through their IP address.

Mail Processing:
It consists of SMTP mailing process this helps the user to find out the prior mail addressing node. So all the confidential mails will separate and sends to the particular node. This process will stops the leakage of sensitive information.

Mail configuration:
It consists of viewing all the mails come to us whether we already read or not. From this, we can select one and read. Unwanted mails can be deleted. This process delivers mails strangely from the mail server itself, so no one can crack or hack the mails while sending and receiving it.

7. CONCLUSION

It is concluded that the application works well and satisfy the users. The application is tested very well and errors are properly debugged. The site is simultaneously accessed from more than one system. Simultaneous login from more than one place is tested.

The site works according to the restrictions provided in their respective browsers. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one. The speed of the transactions become more enough now.

The Object of the study are fulfilled by having proper security for the confidential folders within the organization and also the tracking of the person who hacks the data from the organization along with the restrictions like to whom the various rights is being enabled and disabled are done effectively by using this system for the organization.

8. SUGGESTION

Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Changing the existing modules or adding new modules can append improvements. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one.

References:

Book


Journal
• Victor Mendez, Julio Cesar Hernandez, Jesus Carretero, And Felix Garcia,2004 are at the department of Computer Science, Universidad Carlos III de Madrid.
• Genrich, Michael ”E-mail Servers” Macworld; Apr2004, Vol. 21 Issue 4, p30-32, 4p
• Kevin Curran, Ph.D., John Honan ,2004is at the School of Computing and Intelligent Systems, University of Ulster, Northern Ireland, U.K.”Spam”
• Kristin Byron, 2008,” Carrying Too Heavy A Load? The Communication andMiscommunication Of Emotion By Email” Syracuse University.
• Petros Belsis, Kostas Fragos, Stefanos Gritzalis and Christos Skourlas 2008 “Applying effective feature selection techniques with hierarchical mixtures of experts for spam classification”, University of the Aegean, Samos,.
• Robert K. Plice, Nigel P. Melville, and Oleg V. Pavlov May 2009 | vol. 52 | no. 5 “Toward an Information- Compatible Anti-Spam Strategy”.

WEBSITE REFERENCE

• http://www.queenslibrary.org/?page_nm=Print+and+Audio
• http://www.asp.net
• http://www.osborne.com
• http://www.microsoft.com