Intranet Mailing System Using Cryptographic Methodologies

Sreya P Kumar[1], Shruti Prasad[2], Reena Babu[3], Vishnu R[4], Aveendran R[5]
[1,2,3,4] *B.Tech Student, Mount Zion College of Engineering, Kadammanitta, Kerala, India*
[5]*Assistant Professor, Department of Computer Science and Engineering, Mount Zion College of Engineering, Kadammanitta, Kerala, India*

Abstract- **The Intranet Mailing System facilitates communication among the users within an organization only. In this fast growing world where organizations are expanding rapidly and are increasing in size. So these organizations has shift times and it is difficult for an employee who is working on a shift to communicate with another employee on a different shift. This can be avoided by using Intranet Mailing System. The employee who is working on the organization can communicate and send mails through the system by registering himself to another employee who is registered in the same system. This increases the consistency and reduces the delay in delivering information by providing enhanced security in transactions.**

Index Terms- Mail System, Intranet.

1. INTRODUCTION

INTRANET is the generic term for a collection of private computer networks within an organization. An intranet uses network technologies as a tool to facilitate communication between people or work groups to improve the data sharing capability and overall knowledge base of an organization's employees. A network that uses technologies of internet protocol to share any type of information within association or Business Company is called Intranet. This technology is used in the proposed system, the "Intranet Mailing System" to make the most out of this technology. This will somehow automate the information passing system.

Now a day's communication are almost done by mails, this makes mailing system more useful. In this proposed system the maintenance time of mail will be reduced and make the system more user friendly efficient and increase speed of processing. The system contains all the features like chatting, mailing, file sharing.

Since the system is a physical network which is used within an organization .These features can only be used by its registered employees in the system. The entire employee in the organization can use these system features with different login id and their secure password. By this it increases the total security of organization. So an unauthorized person cannot be able to use the system. The main features of the system is, it allows only registered employees to access the network. The system also helps the employee who is working on a shift to communicate with another employee of a different shift through group chat. A cryptosystem is an application of cryptographic techniques. Due to the increase in huge number of commercial transaction on the internet, cryptography is very key in ensuring the security of the transactions and increases the data confidentiality. Authentication provides individual access to the system based on their identity .Non-repudiation guarantees the transaction of messages through digital signature. Data confidentiality can be increased by encrypting sensitive files, managing data access, physically securing devices, secure dispose of data, managing data acquisition and data utilization. The system uses RSA algorithm used for particular security purposes which provides public key encryption to encrypt messages and is commonly used when it is sent over an insecure network. MD5 algorithm is also used in the system providing a wide range of security application and is used to check the integrity of files. MD5 accept messages as input and returns output of fixed length digest value to authenticate with the original message. SHA-1 algorithm which is used to check the integrity of a particular data or to verify that a file has been unaltered in the transactions. This is done by producing a checksum before the file has transmitted to the network and also checks again when it reaches the destination. This technologies are used in the proposed system to ensure the security purpose of communication.

2. AIM

Objectives for this project is listed below:

- To get an idea about what is an INTRANET MAILING SYSTEM.
- To provide a communication channel inside an organization.
- To provide security for confidential messages.
- To explain advantages of cryptographic techniques.
- To prevent hackers and unauthorized access.
- To accept mails from authorized users providing security.

3. PROPOSED SYSTEM

Intranet Mailing System provides communication among the members within an organization in a secure way. The proposed system is limited within an intranet. Intranet Mailing System sends mails impulsively without requiring the parties be available at the same time.

It provides a written copy of sending mails.

It is much cheaper and safer than traditional 2-tier system. The system serves spontaneous needs of an organization.

3.1 Login

Login deals with the login process in the system. This allows the users to enter their user id and passwords. It provides the facilities for creating new account. This is done by just clicking the signup option and can then fill the field form. This contains new user details such as their user name and their secure password. After entering the submit button which checks the user id and password to know whether the user exist or not. If the user name is present in the systems database, the corresponding information of the user will be provided. The system also checks whether the user entered correct user id or not. If not the system show error.

3.2 Compose Mail

It allows users to compose new mails and send to other users. Send and received mails storage

The system consist of an inbox database to store received mails and send folder to store send mails.

3.3 Trash

If you delete a message from your mailing service, it stays there in the trash for 30 days. After then it will be automatically and permanently deleted from the mailing sites.

3.4 Outbox

A holding place where messages go after you click send and wait until the program can forward it to mail server.

3.4 Contact

It provides the user’s personal information such as user name, designation, mailid and contact number.

3.5 Attach Files

Intranet Mailing System allows users to suitably attach files to their mails, these include adding attachments like’s files or photos to your mails.

3.6 Group chat

Create unwanted chat groups and control who can view and send message in these groups. These can only be created with authorized persons in the organization.

3.7 Logout

In the logout section, by clicking the logout button the user can leave from the site in a secure manner. If the user wants to renter the system, then they must again needs to register to the site.

4. FEATURES TO BE IMPLEMENTED

4.1 Group chat

Intranet mailing system is applicable only within an organization so without an internet connection we can communicate with the employees inside an organization. It also Create unwanted chat groups and control who can view and send message in these groups. These can only be created with authorized persons in the organization.

4.2 Mail Priority Checker

The system uses a data set to check the priority of mails.it compare the data set values to the contents of mails. Based on this comparison the priority of mails are checked and analyzed. There are three categories of mail Priority-High, Medium, Low. If the priority is high or medium are used and if it is Low the encryption techniques are used.

4.3 RSA Algorithm

It is a cryptographic technology. The algorithm is an asymmetric cryptographic method. This is widely used in providing security for sensitive data, particularly when it is send through an insecure network. These are commonly used to encrypt and decrypt messages. When A sends a message to B without any cryptographic keys. A just uses public key of B to encrypt the message and B decrypts the message with its secured private key.

RSA algorithm guarantees the secure transfer of data in digital environment.it is most commonly used to find the largest prime factors of integers.

4.4 MD5 Algorithm

It is a hashing algorithm.it is a cryptographic technology which takes input message of variable length and return an output of fixed length. The fixed length output is the digest value for authenticating with original message. it is used to check the integrity of files. Md5 is susceptible to length extension attack. Whenever a transaction data detail is send to URL, it will validate the authentication of that transaction data using MD5 algorithm. This algorithm is mainly used in digital signature methods, where a mass amount of data and files are compressed in a secure manner before being encrypted.

4.5 SHA-1

This algorithm is a cryptographic algorithm which uses a hash function.it is used to verify whether a file is altered or not, by generating a checksum values before it is send and again rechecks before it reaches the receiver.

The hash function takes an input and produces a 160 bit hash value known as message digest.it provides data integrity and authentication during transactions of mails by using a 160 bit encryption key. it is cryptographically stronger and are suggested when there is excessive need for security.

5. ADVANTAGES

5.1. Advantages

Communication:

It provides enhanced communication within an organization providing more security than other mailing system

5.2 Productivity:

Information can be accessed anywhere and at any time.

Less mailing time: The required data and information is transferred to the users. It takes less amount of time to process it.

5.3 Security:

The system only accepts messages from authorized users providing security.

5.4 Mail Priority Checker:

The priority of mails can be checked using datasets provided in the system. These will compare the datasets value to the contents of the mail. By this comparison the mails are analyzed.

5.5 Cost effective:

Whenever the information is needed to users, they can access it through their system.

5.6 Business Operation & Management:

It provides a new alternative way of managing an organization

6. APPLICATIONS

Intranet Mailing System is mainly used for managing institutions like schools, Hospitals and Business Organizations, where they can have internal communication.

7. CONCLUSION

Intranet Mailing System provides a new way of managing an organization that allows users to access intellectual assets of organization. Here the system provides a web based intranet mailing system. But registered users can transfer information without using internet. The system benefits the organization to a great extent. It is more cost effective and reliable than other mailing system. In order to check the integrity of files MD5 algorithm is used. RSA algorithm is used to ensure secure transfer of data in digital environment. SHA-1 cryptographic algorithm provides data integrity and authentication during transaction.

8. ACKNOWLEDGEMENT

The authors would like to thank everyone for having given us this opportunity to conduct this study. We would also like to thank Mount Zion College of Engineering and APJ Abdul Kalam Technological University for giving us this platform.

REFERENCES

[1] N. Freed and S. Kille, ―Mail Monitoring MIB‖, RFC 2249, January 1998.

[2] PHP for the World Wide Web (visual Quick Start Guide) by Larry Ullman.

[3] JavaScript for PHP Developers by Stoyan ss Stefanov.

[4] Eric Allman, ―SENDMAIL – An Internetwork Mail Router‖, Program Documentation, 1982.

[5] T. Berners-Lee, R. Cailliau, J. Groff, and B. Pollermann, "World-Wide Web: The Information Universe", Electronic Networking, Vol. 1, No. 2, Spring 1992.

[6] K. Arnold and J. Gosling, The Java Programming Language, Addison Wesley, 1996.

[7] Uyless Black, Network Management Standards, 2nd edition, McGrow Hill, 1994.