

Electronic Secure Email Detection System over Data Storage Security System

Shilpa Aggarwal, Vandana Venkiteswaran, Ria Vishnoi

Department of Information Technology
SRM University NCR Campus

ABSTRACT:

A company or an organization allows its employees to interact with the client for the organizations benefit. With technological growth in the industry this interaction has been made easier with the use of electronic mails. The employee is allowed to send mails to client through the company's portal. As the employee has full freedom he may use this for his own benefit. Therefore, it is important for the company's security that an administrator must watch over the mails that are being sent to clients by the employee. But watching every mail may become cumbersome. Therefore we propose a system that searches specific words in the mail and direct it to the administrator instead of the client if something suspicious is found. Through this more security is ensured.

KEYWORDS-: organization, electronic mail, employee, administrator, suspicious

I. INTRODUCTION:

The proposed project's main objective is to prevent frauds that are committed by employees. The organization has given the employee the freedom to contact with its clients through email. The employee can send mails to client directly if the mail contains nothing suspicious as shown in figure 1.

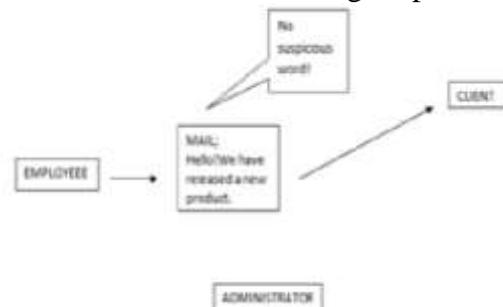


Figure 1: Mail with no suspicious word

The second case occurs when the mail contains a suspicious word. In such a case the mail is forwarded to the administrator instead of the client. The administrator may further go through the mail and decide whether the suspicious word is used in a wrong context or not.

If the mail poses any threat to the organization it will not be forwarded to the client. Otherwise, after going through the mail properly it may also be forwarded to the client. The figure 2 depicts such a case.

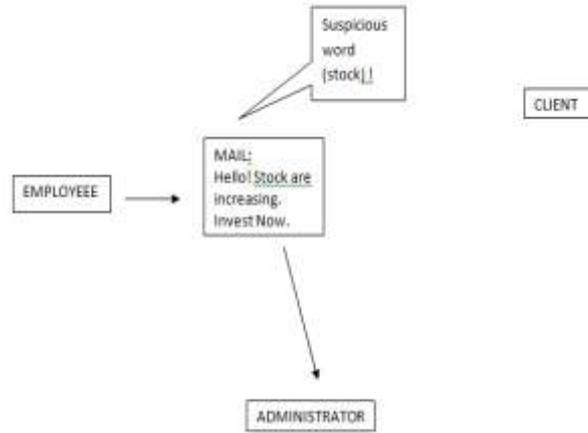


Figure 2: Mail with suspicious word.

Therefore, not only stopping suspicious mail from reaching clients, the administrator can also maintain the data storage.

II. RESEARCH BACKGROUND:

“Suspicious E-mail” existing system is one, which is very primitive and requires manual labour for functionality. By manual labour it that hands do all entries in the record books and these record books are maintained manually. These record books contain entries of each employee. Everything used in the system is hardware oriented, or physically existing pieces of equipment. Software has not been introduced in the organization at any level of operation. Therefore, the new system being created has been designed to convert, as much as possible, the hardware into software packet.

With the technical growth hand written letters are dispensed with and there has been an introduction of electronic mails. These mails are being sent freely and more easily from one person to another. The transmission of mail occurs through internet and is faster than speed post, courier etc. Managing of mails is also easier than that of the letters. But with the introduction of emails the security is a major concern. The organization that provides its employee’s to contact clients through email must be secured and supervised so that the confidentiality is maintained.

III. GENERAL SURVEY:

No	Questions	Yes	No	Total
1	Does your organization allow you to contact its clients?	100	20	120
2	Do you connect with your client through email?	73	47	120
3	Is there any limit in number of email you can send?	22	98	120
4	Do you use antivirus for scanning mail and attachment?	89	31	120

5	Has the organization you work for faced information leak?	69	51	120
6	Are you aware of any system that would prevent information leakage?	10	110	120
7	Do you need a system that prevents suspicious mail transfer?	94	26	120

Table 1:Depicts the survey conducted

From the survey conducted, it is proven that most organizations are allowing its employee to connect with clients through email. There is no limit in number of emails being sent which implies that manual checking of each and every mail will be time consuming as well as a cumbersome process. Therefore need for the proposed system was seen.

IV. RESEARCH METHODOLOGY:

The technology primarily being used is Java and its further implementation. Since the entire functioning of this project involves both maintaining a mail management system and performing word to word checking of the mails, separate platforms within Java have to be used.The entire project is operational and handled using Eclipse IDE(Integrated Development Environment) with version Indigo and above acceptable.

Firstly, the basic login and mail management system is implemented. For this purpose, we use JavaScript based web page designing to accept user’s authenticated data and match his login credentials with ones stored in the database. A slight use of HTML was required for enhancing the interface within which the user interacts with the User Interface (UI) for creating and sending mails from his terminal.

Secondly, the core coding performed in Java is used to implement the basic algorithm that provides the string matching technique of comparing each word written in the mail with the ones stored in the database at the server.

Lastly, for running the server instance, we configure a local server, primarily, Apache Tomcat Server with compatible settings for smoother implementation.

Thus, to ensure a smoother running and operation of the intended function of this project, we use an integration of the above discussed technologies and therefore, Eclipse IDE proves to be the best platform available for running Java code cleanly without any errors or hassles.

V. FUTURE SCOPE:

The future work in this field could be that the proposed system will not only aim on detecting suspicious mail but can be enhanced for performance appraisal, employee appraisal purposes. The employee who sends most mail and provides most customer/client support services would be calculated and that employee may be rewarded. It can be applied not only in organization involving client based interaction but also for security purposes. This can be applied in government organizations such as defence, which has a lot of confidential information. Another future scope of this software would be in the field of stock management and privacy. The stocks of an organization are one of the most confidential information which the employee may use for their as well as some clients benefit. So this software or another edited version of this software may be applied in this field as well.

VI. CONCLUSION:

The proposed software would minimize the illegal or unprofessional passing of mails that may have an adverse impact on the growth of the organization. The email detection would also result in more productivity and consciousness among the employees. The organization may be able to find leaks in the organization and take action accordingly. Not only this, the employees with no suspicious mail sent from them may be rewarded which will further reduce the amount of suspicious mail. This will increase the productivity of the employee which will further lead to the growth of organization. Thus it may ensure secure transfer of mails between a client and an employee. This proposed software may also be applied in other areas involving stock management, employee appraisal, as well as areas related to security.

VII. REFERENCES:

1. **Balagurusamy** : Tata McGraw-Hill Education, 06-Oct-2009 - 454 pages
2. **Java The Complete Reference**:McGraw Hill Professional, 01-Dec-2006 - Computers- 1024 pages
3. www.google.com
4. <http://www.ijmo.org/papers/146-C105.pdf>
5. <http://www.sciencedirect.com/science/article/pii/S1110866514000280>
6. www.wikipedia.com