International Journal of Modern Trends in Engineering and Research

ADVANCE EMAIL SECURITY AND FEATURES

Mr.Dharmadurai.S[1], Mr.Dhanaseelan.A[2], Mr.Venkatesh.R(AP/IT)[3]

[1,2,3]*Department Of Information Technology, S.K.P.Engineering College,Tiruvannamalai,Tamil Nadu,India*

Abstract-The email malware deduction project used to filter the spam file and content. And update the new message to same id. If any user sends mail with multiple file to other user means in server side check the file if any ex-e file include in the multiple attachment server filter the particular file and send the original file to user in-box. If user sends wrong mail to other user means they can update new message to same email id. Admin add some restricted word. If user sends that restricted word means that mail will not send. User also give some suggest word to admin. Admin find the count of spam word sending mail id and IP. Which email and IP address got highest count that email and IP address will be blocked by admin. Nobody can track other user details.

Keywords-Compose Mail Module,Malware Filter Module,Spam Filter Module,Resend Mail Module,Suggest word Module,Trash Module,IP and user Blocker

I. INTRODUCTION

Malware emails are also sent out when certain events like computer restart are triggered. Thus, at an arbitrary time t, a user may receive multiple malware email copies from an identical neighboring user who has been compromised. In order to represent the repetitious spreading process of the reinfection and the self-start, we introduce virtual nodes to present the infection caused by infected users opening the malware email copy.

II. PROPOSED

Compose Mail Module–

In compose mail module user used to create the mail which he need to send. Compose mail module contains details such as to, from, message, attachment, user can attach any kind of file our email server will support all kind of attachments.

Architecture Diagram
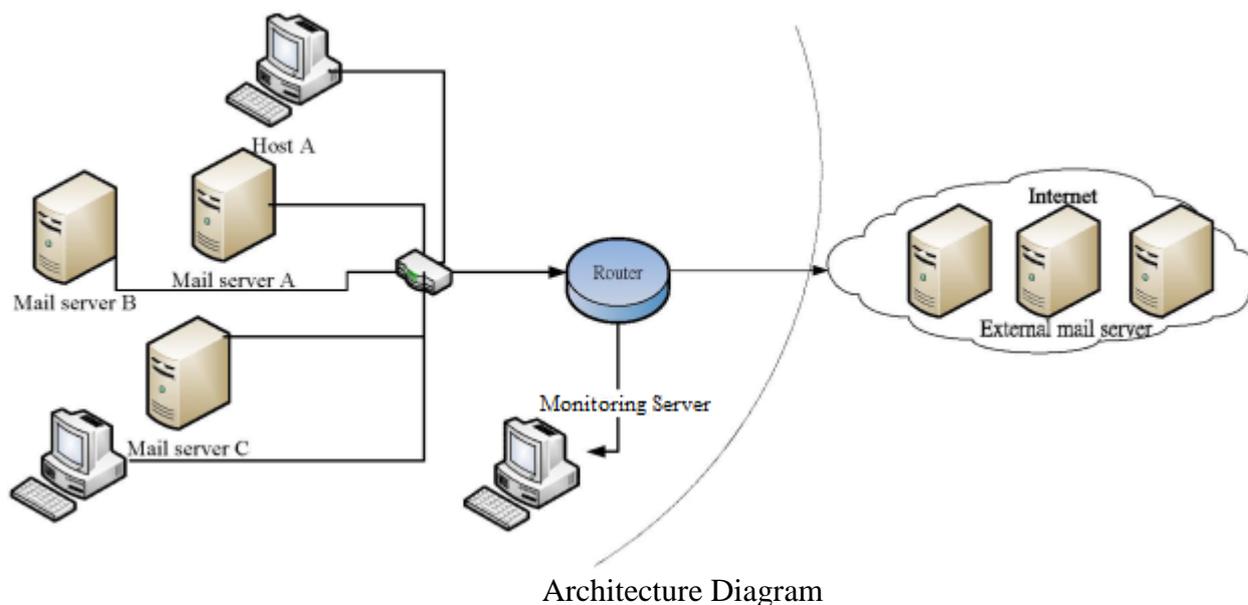
Malware Filter Module–

This module used to identify the malware file which is attached in the email. If suppose the user sending a file which is affected by malware such file is extracted from the mail separately and will be moved to Malware ware drop box and the remaining mail content will be send to the receiver side.

Spam Filter Module–

The spam filter module is to restrict the illegal usage of business and advertisement related mails spreading. Our mail server will automatically scan the entire contents of the mail which is sending by the user and will move it to spam drop box, such illegal data containing mails will not send allowed to send. This spam filter will filters the illegal words that may be advertisement related, business related or bad words all such words are taken as spam data.

Resend Mail Module–

This resend mail options is not available in most of the mail servers this is to reduce the unwanted wastage of mail server space. Using this resend option the user can replace the old message with the new one, for instance if a user send a wrong mail to the receiver no need to send another mail the user can edit the sent mail and resend it again such mail will not receive as another mail instead of that the new mail replace the old mail.

Suggest word Module–

In this module users can suggest words can be add to spam filter, This helps the admin to find many illegal words which is used in worldwide languages, and also to improve the mail server quality. Admin will view the suggested word and once the word is added to the spam filter such word contains word will not allow sending.

Trash Module–

This Trash contains unwanted deleted mails those mails will be stored in the trash for two days then will delete automatically. If a user need to retain the deleted mail within this two days in the sense user can move it to inbox again.

IP and user Blocker–

If a user sending mails contains spam words or malware for more than three times per day that user Id and IP will be blocked for that day. This blocking is for security purpose blocked users cannot able to access their account for a day.

III. CONCLUSION

Thus we are using this technique we have to reduce the storage capacity of server side and time consumption of user.This technique is also used to protect against the malware or other kind of illegal contents.

REFERENCES

[1] M. FOSSI AND J. BLACKBIRD, "SYMANTEC INTERNET SECURITY THREAT REPORT 2010," TECHNICAL REPORT SYMANTEC CORPORATION, MAR. 2011.

[2] P. Wood and G. Egan, "Symantec Internet Security Threat Report 2011," technical report, Symantec Corporation, Apr. 2012.

[3] C.C. Zou, D. Towsley, and W. Gong, "Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 2, pp. 105- 118, Apr.-June 2007.

[4] Z. Chen and C. Ji, "Spatial-Temporal Modeling of Malware Propa- gation in Networks," IEEE Trans. Neural Networks, vol. 16, no. 5, pp. 1291-1303, Sept. 2005.

[5] C. Gao, J. Liu, and N. Zhong, "Network Immunization and Virus Propagation in Email Networks: Experimental Evaluation and Analysis," Knowledge and Information Systems, vol. 27, pp. 253-279, 2011.

[6] S. Wen, W. Zhou, Y. Wang, W. Zhou, and Y. Xiang, "Locating Defense Positions for Thwarting the Propagation of Topological Worms," IEEE Comm. Letters, vol. 16, no. 4, pp. 560-563, Apr. 2012.