Enterprise Level E-mail Security System

Abhijit D. Jadhav, Ashvini A. Phalke, Pradnya A. Waman, Usha N. Katore, Santosh R. Salunkhe

Abstract: Data leakage is a process in which a data distributor has given important data to a supposedly trusted agents and some of the data is leaked and found in an unauthorized place or unauthorized user. An enterprise data leak is a scary statement. Security practitioners have always had to deal with data leakage issues that spring up from various ways like email, IM and other Internet channels. One or more agents can leak the data. Moreover, data can also be leaked from within an organization via e-mails. So, there is need to filter these e-mails. The mail can be filtered by blocking e-mails which contains images, videos or sensitive data of an enterprise. The e-mail is one of the sources of data leakage. Principle used in e-mail security is we classify e-mail, sensitive data into the white and black lists with document's digital signature value. The data can also be changed by the trusted agents. The system will detect such a changes of the sensitive data and if founds same as black list it will block the mail or stop for review. Then the distributor will decide to allow or disallow the incoming mails from the agent's. The system will prevent the enterprise data from data leakage. E-mail security system will make the data more secure.

Index Terms– Black List, SHA, TF, White List.

I. INTRODUCTION

Now a day, the enterprises or the different organization perform their main commercial or financial activities using mail. The agents or worker's of enterprise uses there data for processing and also use for different transactions. But many times it may happen that the agent will send that important data to unauthorized user for any suspicious activity.

The existing email filtering system does not check individual attachments nor does it block single email. In such a case, we can have a system for resisting the guilty user. The system can check the mails instantly of different user's. The purpose of e-mail security system is to detect the agent who will try to leak the data and block such a mail which contains the black listed data or also other important data. The data can also be changed by the trusted agents. The system can detect such a changes of the sensitive data. The distributor will decide to allow or disallow the incoming mails from the agent's.

If the agent copy the data in email body, for that TF algorithm is used for checking the body section of e-mail. The system will prevent the data from leakage. The e-mail is one of the sources of data leakage. E-mail filtering system does not allow any data leakage. The system provides security to the sensitive data of enterprise.

Manuscript Received 22 February 2014.

Abhijit D. Jadhav, Department of Computer Engineering Sharadchandra Pawar College of engineering, Otur Maharashtra, India.

Ashvini A. Phalke, Department of Computer Enginnering Pawar College of engineering, Otur, Maharashtra, India.

Pradnya A. Waman, Department of Computer Enginnering Pawar College of engineering, Otur, Maharashtra, India.

Usha N. Katore, Department of Computer Engineering Sharadchandra Sharadchandra Pawar College of engineering, Otur, Maharashtra, India.

Santosh R. Salunkhe, Department of Computer Engineering Sharadchandra Sharadchandra Pawar College of engineering, Otur, Maharashtra, India.

Employees or agents activity could be unauthorized data use, misuse of enterprise computer's, misuse of important passwords. The data which agent trying to leak, it can be in any form as PDF file, word documents, zip files and many more.

In the system, the owner of data is distributer (admin) and supposedly trusted person is the agent (client). The main purpose of the system is to prevent the distributor's sensitive data and detect the guilty agent who had been tried to leak the data.

II. SYSTEM ARCHITECTURE

The admin application is installed on the distributor's side with the many data preventing function's and the function's for categorize the data in black and white list. The admin is provided with the internet connection. The client application is installed on the agent side with some e-mail related functions without the internet connection

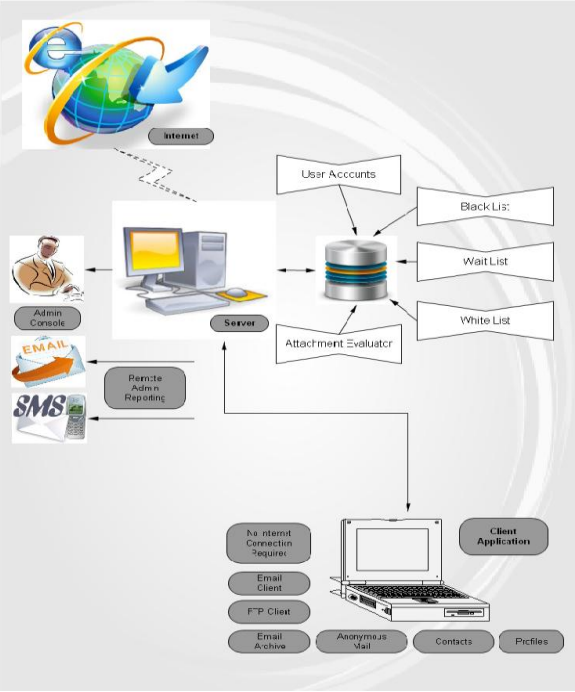

Fig. 1: E-mail security system architecture

The proposed system gives the facility that admin will able to identify the guilty user and the application can prevent the data from leakage.

The figure.1 shows the system architecture of proposed system. The admin gives the data to the client for any enterprise activity. The client uses that data but some client try to leak that data. The client application data will proceed to the internet through the admin side. Then admin side system will check the client's data. If the data is found same as a black listed data, the system drops such mails.

If it is white listed, it is forwarded to internet and in some other unauthorized activity the system can also stop the mail for review. The system will alert the

admin through message or e-mail that he has some messages for review.

We have used two algorithm SHA-1(Secure Hash Algorithm) and TF (term frequency) Algorithm for security purpose.

SHA-1(Secure Hash Algorithm) is a cryptography hash function designed by the United States National Security Agency (U.S.A). SHA-1 produces a 160-bit (20-byte) hash value. The generated 160 bit value of SHA-1 is converted into hexadecimal number and then used in a system. SHA-1 is the most widely used algorithm in several applications and protocols. It is more secure algorithm.

TF stands for "Term Frequency". By using this algorithm we score the importance of words (or "terms") in a document based on how frequently they appear across multiple documents. If word frequently appear in document then we will say that document contain organisation sensitive data. If leakers try to leak that document then we will stop leaker by this method. And provide security to organisation sensitive data by using this algorithm.

E.g. If any document contain more than 15 word same with black listed data then this document in not allow to send.

III. WORKING METHODOLOGY

The proposed e-mail security system checks the individual mail and it block single mail also. The working of our system is same as the client-server architecture. The client will request for data to admin whenever required. Admin will provide the data. The client has many functions as receiving mail, sending mail, managing users, managing contacts and many more.

The client can have any business e-mail id. Client has some modules.

A. Log In

The user is provided with the e-mail and the system checks whether the user is authorized or not, then provide access to the e-mail application.

B. Send and Receive Mail

In this module, the facility of sending mail is done through this function. The client can send mail to any other user. The mails of particular client will be received by receive mail function. For send and receive mail SMTP protocol is used this is present at both client and receiver side.

C. Manage Contacts and Groups

The contacts and groups which are necessary within organization can be handled.The client can use above all this modules and send the mail. The mail is forwarded and received at admin side and the mail is processed by admin system .While processing the data such as e-mail attachment, body of client is checked and the system decide that to forward the mail or not. According to the data the system will perform the work of blocking mail, allowing mail and stopping mail for review.

The admin also has some important function to be carried out. The admin can manage the different users, user's important data of the enterprise. The admin side system will check the attachment by matching it with digital signature value stored in black and white list. The user may copy the data in e-mail body. The system also checks the body content using TF algorithm. Important keywords regarding sensitive data are stored in the system and depending on number of occurrences of words; the data within body is authorized or unauthorized is decided. Admin can take action against agent who sends that black listed data. Admin can check that data with help of the system in very careful manner. Admin has some modules.

A. Admin Login

Authentication of admin is the important, so the login of admin is necessary. The admin should be trusted and authenticated person.

B .Manage Digital Signature

In this module, the digital signature is assigned to the documents using SHA-1 algorithm and according to the list; the value is stored in lists of the corresponding document.

C .Black List

Using this module, the admin categorize data in black list. This list contains the data with digital signature which is unauthorized for clients to be sent over the network.

D. White List

It contains the data which is authorized for client to be sent over the network. It also has the documents digital signature value with it.

E. View Blocked Mail

The e-mail with black listed document as an attachment is blocked by system attachment evaluator and it can identify the guilty user in this module. The mail which contains the unauthorized data in body section of e-mail stopped for review. The admin is alerted by message or e-mail that he has some messages for review then admin decide to allow or disallow the mail.

IV. CONCLUSION

Now a day, when serious business and other type of transaction over the internet to large extent or improper security mechanisms can bring the whole business down. In reality, there is no need to give the sensitive data to agent who will leak that data. And even if we give data, the enterprise has to take care about that. We can have the guilty agent who had tried to leak the data. So we have system to capture such malicious activity. The main thing we can achieve is that we protect the data of enterprise and can find guilty user of enterprise.

The e-mail is one of the sources of data leakage. Through email large number of data can be leaked. Thus by using E-mail security system we can make the data more secure**.** Purpose of the system is to find out leaker who had been tried to leak the data. If user can leak data then find out that leaker and prevent the organisation data from leakage.

REFERENCES

1. Hector Garcia-Molina and Panagiotis Papadimitriou "Data Leakage Detection," IEEE Transactions on Knowledge and Data Engineering, Vol 23, No.1 january2011.
2. Mayur Gaikwad, Ankit Agarwal, Vahid Inamdar, Kapil Garg, " Robust Data leakage and Email Filtering System" 2012 IEEE.
3. Behrouz A. Forouzan, "Cryptography & Network Security",
4. www.vanemery.com/protocols
5. http:/ / www.parashift.com/ c+ +-faq-lite/ serialization. html