Organizational Security by Remote Monitoring

Mohini Prakash Rajage
BE.IT, Pillai HOC College Of Engineering and Technology
Navi Mumbai, India
mohini.rajage09@gmail.com

Priti Narayan Patil
BE.IT, Pillai HOC College Of Engineering and Technology
Navi Mumbai, India
ppriti748@gmail.com

Shweta Suresh Mhatre
BE.IT, Pillai HOC College Of Engineering and Technology
Navi Mumbai, India
shwetamhatre2014@gmail.com

Shamna Sadanand
BE.IT, Pillai HOC College Of Engineering and Technology
Navi Mumbai, India
shamnas@mes.ac.in

Abstract – *Most of the business nowadays depends on the internet for basic tasks. Almost every office has at least one computer system to manage the resource. There are also many acute job carried out by these computer systems like payment transaction. Also delivery of important data is required for organization. So there is a need to be a system that looks after the security of the entire system. Also the employees in the organization can be an insider threat and can leak important information to the outside world.*

Keywords—*Cloud, AES, RAID.*

I. INTRODUCTION

We have planned to develop a system which will solve the problem. Our first priority is to secure the data. For that we are developing a secured encrypted data transfer system. The encryption system will be client side we will develop a program to encrypt the data to be transferred at the client end. After the data is encrypted for sending the data to other employee the person will have to login to a web application and then upload the encrypted file to the server. After uploading is complete, the user can set a password to the file he uploaded. This will ensure that there will require two passwords for decrypting the file. In this way we can implement the secure data transfer system. The motivation behind the undertaking is to build up a framework for the association which will verify the association information alongside foreseeing for dangers by following the representative of the association. By actualizing this framework, the information will be verified and if the sender encodes the information with legitimate, substantial and solid secret word the record will be more diligently to split. Additionally the document will be more diligently to get to if the secret word used to transfer the record is more grounded. The IP following will know the individuals who get to the record utilizing the secret word. The whole information exchange procedure will be secure.

The customer following framework is secure and can be utilized to check if the advantage is representing a risk to the association. By utilizing methods like screen catch and keystroke logging we can precisely locate the rationale of the objective utilizing the framework. By these arrangement of the device that we will create we can really verify the undertakings of any association.

The second important thing is to monitor the employee for checking if he is an internal threat to organization. This can be tested by implementing a monitoring system. To implement this monitoring system we are planning to develop a keystroke monitoring system along with screenshot capturing system which will accurately track the user activity.

II. PURPOSE

The purpose of the project is to develop a system for the organization which will secure the organizational data along with predicting threats by tracking the employee of the organization. By implementing this system, the data will

Definitely be secured and if the sender encrypts the data with proper, valid and strong password the file will be header to crack. The IP tracking will help to understand the members who access the file using the password. The entire data transfer process will be secure. The client tracking system is secure and can be used to check if the asset is posing threat to the organization. By using techniques like screen capture and keystroke logging we can accurately find the motive of the target using this system. By the tool that we are developing we can actually secure the tasks of any organization.

III. CONSTRAINTS

We here define the constraint using the triple constraint of project management:
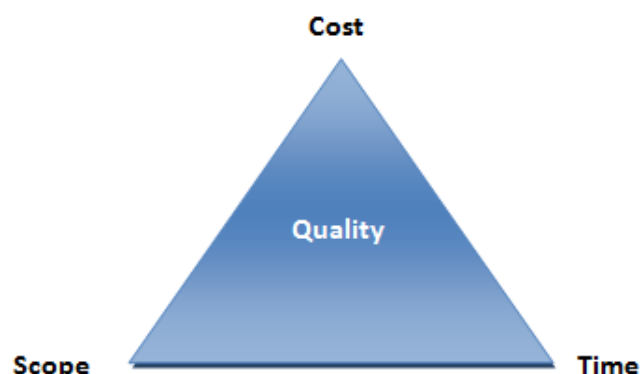
- Cost:The cost of developing a system like this quite minimal. The only thing that will cost a bit is the servers. There are two options for server solution. The organization can use its own personal server or the organization can opt for a hosting plan which can control the system from remote. Also the software that we are using is free to use along with the technologies.
- Time: The time required for developing the project is depended on the complexity of the project and also the number of modules. According to the current specification of the system it will require almost 3-4 months for developing the modules on the respective machine.
- Scope: The final product intend to secure the organization from internal or external threats.

IV. OVERALL SYSTEM DESCRIPTION

A. Existing System

The main feature of existing system is that it provides security to data stored in cloud using the encryption/decryption algorithm. In existing system organization stores the data on third party server.

B. Proposed System

The system that we proposed solves most of the problems that we have with the existing system. Existing system saves all the data from the client to their own server which means that the sensitive data goes in the hand of other people. The proposed system stores the client data on their own server which increase the security and prevents loss of data.

C. Algorithms

There are four algorithms used in our system:
1. Admin login:
   - Admin visit our web application
   - Admin enters user name and password
   - If(credentials, valid)
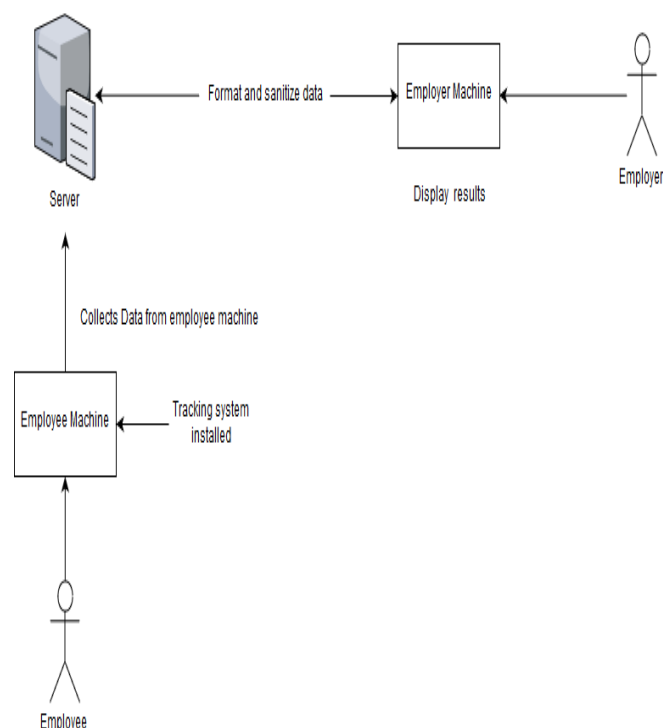   Process to admin panel
     Else
     Show error
   - End
2. Shutdown:
   - Client machine starts
   - Client machine executes rss.exe
   - Rss.exe checks for shutdown request every 30 seconds
   - If(ServerResponce =1)
     Shutdown the system
     Else
     Do nothing
   - End when system shutdowns
3. Remote Command Execution:
   - Client machine starts

- Client machine executes rsx.exe
- Rss.exe checks for commands every 30 second
- If(ServerResponce = command)
  Execute the command
  Reset the command from server
  Else
  Do nothing
- End when system shutdown

4. Remote Command Execution
   - Client machine starts
   - Client machine executes klg.exe
   - Klg.exe store logs in variable
   - Flush the variable to server every 30 seconds
   - End when system shutdowns

D. System Architecture

V. RESULT

CONCLUSION

Our research indicates that existing system provides security only for server but there is possibility that authorized user may leak the sensitive data. To prevent unauthorized access our system contains the Honey Pot concept which stops the attacker from invading the system. This system may provide best solution to overcome these drawbacks.

REFERENCES

[1] "Data Leakage detection and Prevention System" International Journal of Computer Science Trends and Technology (LICST) publish in Mar – Apr 2017.

[2] "A Secure Anti-Collusion Data Sharing Schema for Dynamic Groups in the Cloud" International Journal publish in 2013.

[3] Subhashini peniti, B. Padmaja Rani "Data Leakage Prevention System with Time Stamp".