International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

Data Leakage Detection Using Fake Data for Identifying Guilty Agents

Ajay N
Final year student Bachelor of Engineering
Department of Computer Science and Engineering
K.S.R. College of Engineering, Tiruchengode, India

Belshick Megason JB
Final year student Bachelor of Engineering
Department of Computer Science and Engineering
K.S.R. College of Engineering, Tiruchengode, India

Hariharan T
Final year student Bachelor of Engineering
Department of Computer Science and Engineering
K.S.R. College of Engineering, Tiruchengode, India

Jagadesh Kumar M
Final year student Bachelor of Engineering
Department of Computer Science and Engineering
K.S.R. College of Engineering, Tiruchengode, India

Mrs. Vasuki P
Assistant Professor
Department of Computer Science and Engineering
K.S.R. College of Engineering, Tiruchengode, India

Mrs. Nivodhini MK
Assistant Professor
Department of Computer Science and Engineering
K.S.R. College of Engineering, Tiruchengode, India

***Abstract*— In a current time, leaking of users data to third parties or unauthorized persons or even online are common now-a-days, to find the users who leak or distributes the data of users to unauthorized persons is a challenging task for the various organizations so, they use a method called "watermarking" method in their document to find their guilty agents. This method is an old and outdated method. By using watermarking methods there are various disadvantages which cannot be ignored. Day-by-day user's data are leaked by agents who work in various organizations. So, to overcome this issues an algorithm is used the algorithm is called as RSA algorithm. By the use of this algorithm, a key is generated for each and every document which are uploaded to the organization database. So, to access the document's key is required but not only the key, for additional security layer an OTP will be generated and will be sent to agents registered e-mail id. So, by entering Key and OTP then the agent can access the document from the database. Whenever an agent downloads a file from the database intimation will be sent immediately to the admin of the organization. By using this method admin can track all the tasks done by agents at all-time which will reduce the leakage of data to the unauthorized persons.**

Keywords*— *Data leakage, RSA algorithm, OTP, guilty agents, watermarking

1 INTRODUCTION

Data leakage is an unauthorized transmission of data from an organization to any other third parties. Data leakage may be defined as an accidental or intentional distribution of sensitive or private data from the organization. Sensitive data or private data can be anything it can either patient treatment documents, customers data of their company or even our personal data.

Traditionally watermarking methods are used which is an old and outdated method. As we all know there are more issues in the watermarking method such as by using watermarking on a document it can modify the original document or if the user is malicious then the document can be destroyed.

So, to overcome this issue and protect the leakage of data to the unauthorized person here instead of watermarking an RSA algorithm is used. By using this RSA algorithm whenever the admin uploads a document into their organization database a key will be generated to protect the document from being accessed or being downloaded. Suppose a user needs to access the particular document he needs to send a request to the server for granting the permission for accessing the document then that user will receive the key which is generated during uploading of the file and as an additional security layer an OTP will be generated for the particular user only and will be sent to that user's registered E-mail id. Then that user needs to verify both key and OTP which is sent to his/her registered e-mail id to view or download the document from the database.

By having this features (validation of key and OTP) it makes this application more robust and if the agent tries to misuse the key or tries to leak the data to any other third party can be easily found.

2 EXISTING SYSTEM

Traditionally, data leakage was identified by using the method called as "watermarking" method. In this method, some codes are embedded in the file to identify the guilty agents or users. So, there are not robust to protect the data from being leaked by the user.

2.1 Disadvantages of Existing System

1) By using the watermarking method in the document, then the document can be modified from the original document even there can be a loss of some data.
2) If the user has malicious content on his/her laptop or any other devices, and then the document can be destroyed.
3) By using malicious software the code which is embedded in the document he/she can it destroy easily, later he/she cannot be identified as a guilty agent.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

3 PROPOSED SYSTEM

In the proposed system, we will study the techniques which will be used for detecting the agents or users who leak the data to unauthorized persons. Here instead of watermarking technique, we are using an algorithm known as RSA algorithm. By using RSA algorithm we generate a private key during uploading of the document into the server. When the document is uploaded an admin can view the key for the uploaded document in his admin panel. So, on another side when the user needs to access that particular document he needs to send a request for accessing the document. Admin sends the key to that user. The user needs to enter the key sent by the admin to access the document. By just entering key the process doesn't stop here. So, we have added another security layer called as OTP. The agent or user needs to verify his/her OTP which will be generated and sent to his e-mail id at the time of accessing the document. This OTP cannot be transferred nor can it be used by any other user. After verifying all the credentials he/she can view the document

3.1 Advantages of Proposed System

1) Verification of credentials such as key and OTP makes any user leak the data to any unauthorized person.
2) After verifying all the credentials successfully user can view the document, but he cannot move or switch out of the current window which will end the session and needs to verify all details again.
3) Right click of the mouse, cut, copy and paste, taking screenshots and printing the page all are disabled for the all user panel by using their respective queries which makes this application more robust than any other in the field of data leakage detection.

4 SYSTEM ARCHITECTURE

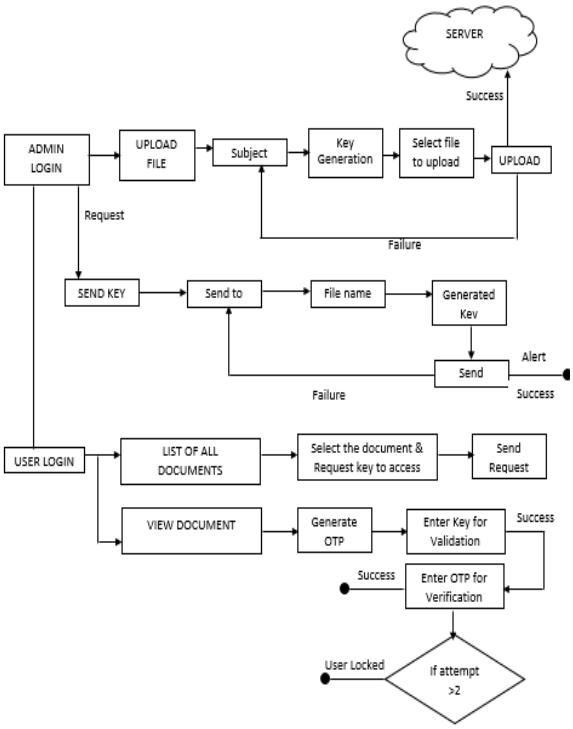

Fig. System Architecture

5 MODULES

- Data Allocation

This is the main area of our project that is data allocation. Here admin store the fake data in their database. So, agent needs to raise the request to access the data which is stored in the database. If the agents raise any request to get access to the data, admin verifies the user and sends the key in order to increase the chances of detecting agents that leaks the data to third parties.

- Fake Object

The admin can create and add the fake data into their database and that data can be distributed to the agent. Fake object is a type of object which is only generated or stored by the admin into their database. So, to track the agents who leak the data to third parties this fake data is used.

- Data Distribution

Data distribution which may consists of sensitive data which are only distributed to trusted agents. Leaked data can be found on any unauthorized places such as web or even through social media. So, after distributing the files to the agents, admin can view which files have been distributed to which agent so that admin can track each and every moment of the agent. If the agent leaks the file he can be tracked by the admin easily.

- Guilty agent

When the agent gives request to the admin to access the file. Then admin receives the request from the agent with his/her details and then admin generates the unique key for the agent and also for the agent and send the details to the agent. If the agent shares his unique key to any other agent or any other unauthorized person and tries to open that files he/she tracked immediately as a guilty agent and his/her account can be locked immediately by the admin for security purpose.

6 CONCLUSION

Our main aim behind for this project was to develop an application which helps the organization to find the agents or employees who steal the data of their customers from their servers and sell them to third parties or you can say it as they leak the data to any unauthorized persons. So, our aim was to stop such illegal activities and to help various organizations to find those peoples who leak their customer's data. So, we have developed such a robust application which will help the admin of the organizations to track each and every document being accessed by their agents and even admin has the rights to lock the user if they found him/her guilty.

Our main aim behind for this project was to develop an application which helps the organization to find the agents or employees who steal the data of their customers from their servers and sell them to third parties or you can say it as they leak the data to any unauthorized persons. So, our aim was to stop such illegal activities and to help various organizations to find those peoples who leak their customer's data. So, we have developed such a robust application which will help the admin of the organizations to track each and every document being accessed by their agents and even admin has the rights to lock the user if they found him/her guilty.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

REFERENCES

[1] Panagiotis Papadimitriou, Student Member, IEEE, and Hector Garcia-Molina, Member, IEEE "Data Leakage Detection" IEEE Transactions on knowledge and data engineering, Vol. 23, NO. 1, January 2011

[2] J. Clerk Ma P. Papadimitriou and H. Garcia-Molina, "Data leakage detection," Stanford University.

[3] YIN Fan, WANG Yu, WANG Lina, Yu Rongwei. A Trustworthiness Based Distribution Model for Data Leakage Detection: Wuhan University Journal Of Natural Sciences.

[4] Mr.V.Malsoru, Naresh Bollam/ REVIEW ON DATA LEAKAGE DETECTION, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 3, pp.1088-1091 1088.