Data Leakage Detection

Chandrapal Chauhan[1], Rupal Lonare[2], Divya Mankar[3], Sakshi Bujade[4]
[1]Assistant Professor, Dept of Computer Science and Engineering
[2, 3, 4]Dept of Computer Science and Engineering
[1, 2, 3, 4] Priyadarshini College Of Engineering Nagpur, Maharashtra

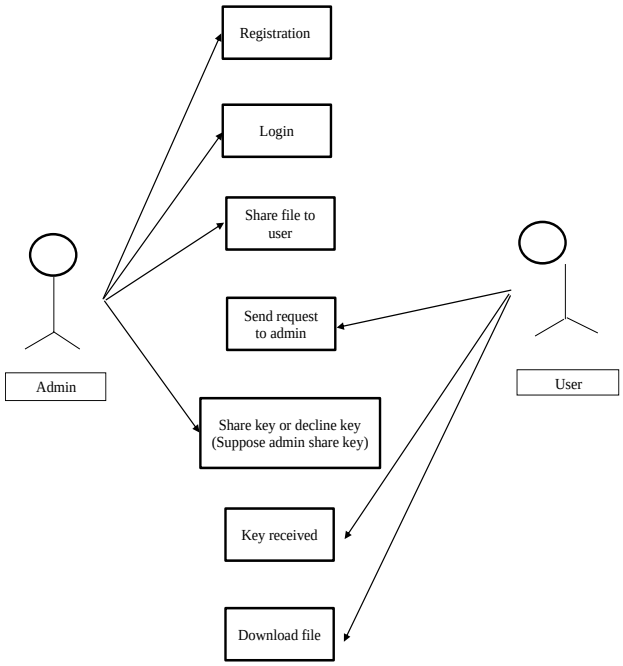
Abstract- *In the business, the data which gets distributed to the authorized person but instead of authorized person third party person try to misuse that data, (eg. Found in unauthorized place) at this time we called it as data leakage.When distributors data gets leaked and to identify unauthorized person, we propose some security steps to that improve the probability of identifying leakages. Our goal is to detect the leaker and provide security to data. In order to reduce this data leakage some security steps are applied on system. Such as otp generation, password protected files.*

Keywords- leak detection, watermarking, companies, data privacy, data leakage detection.

I. INTRODUCTION

Now a days, providing security to data is very important, so that it should not be misused in future. For ex. Company do partnerships with other companies which require sharing of sensitive data. Another company may outsource its data for processing, so data must be given to various other companies. It may possible that third parties leak their data. Traditionally, watermarking was the way to handle data leakage. E.g., Unique code was there in each copy. If that copy is later seen to unauthorized person, the leaker can be identified. In some cases, watermark is very useful but again there is some modification in original data. Specifically, we develop a model for identifying leaker. In which we involved some security steps, such as otp generation, mail/message notification, password protected files. So, by this it will get easier to identify leaker and save the data from getting misused.

USE CASE DIAGRAM – for how to send request key and how receive the secret key and how to download



- First of all, admin will do registration and login.
- Admin will share the file to the user.
- Then the user will send the request to admin for the secret key.
- The admin will either accept that request or decline it. If the admin has shared the key to the user, then the user will receive it then will able to download the file.

II. LITERATURE SURVEY

The secret key method that we are using it so that the data is not leaked. In this shown, how the request is sent, how it is received and how it is downloaded. After downloading, it has shown how to bring it without sending a request to it. In this we apply prevention so that the leaker cannot leak the data.

III. EXISTING SYSTEM

Watermarking is a technique with similarities to stenography. Traditionality, leakage detection is handled by

giving a unique code is embedded in each distributed copy or it can be a translucent image on paper, it can be a logo. And because of all these things, the unauthorized person could not copy the data easily. But the drawback of these technique watermarks is easy to remove.

IV. PROPOSED SYSTEM

In proposed system, we are included prevention so that the leaker cannot leak the data. We gave created this project for the security of the important data of all the organizations. By applying prevention, the security of the data is increases. And even if the data is leaked, then the authorized person can detect which file he has leaked and when.

MODULE IMPLEMENTATION

This application has two modules: 1) Admin 2) User.

1) Admin - Here Admin have all the rights about all process. Admin can send data and also can view data shared by another. If anyone is trying to leak the data then admin have the authority to view the information about Leaker and can also dismiss the person from organization.
2) User - Here user only can send and can view data shared by another. User do not have authority to know the leaker information.

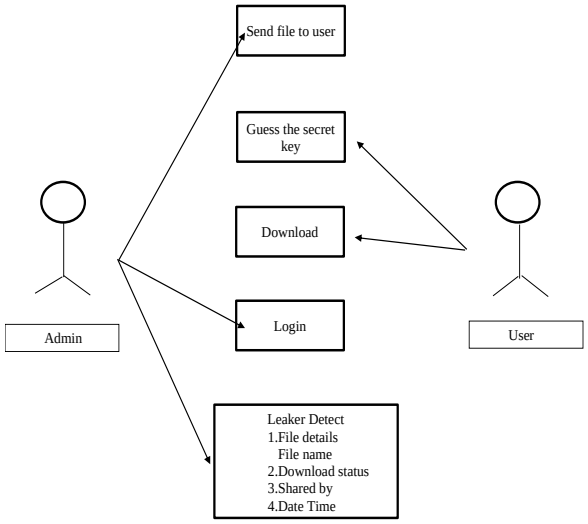
This application contains following features:

- Registration/Login
- Data sharing
- Prevention Of Data
- More Security to Data
- Knowing Leaker Information

New employees need to register first to get an account id. The employee needs to provide the following information to the application – customer name, email address, password. After registration the employee will be assigned a unique account id and he/she can login using account id and password. One employee can only register one account and each account must belong to exact one employee.
Register – The user needs to be register in order to login.

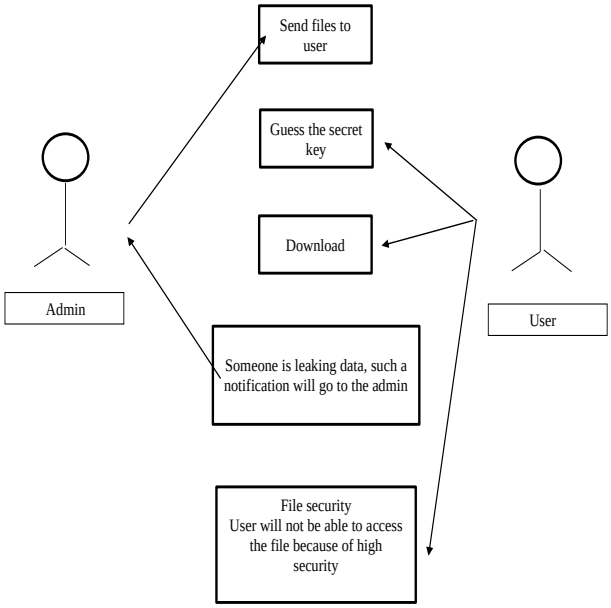
Login – The users need to login to get access to the system.
Share Files – Here the user can share files to another user.
Sent Files by me – The user can see files shared by own account.

USE CASE DIAGRAM – for download it by guessing without sending a key request and detect as a data leaker



- Admin will share the file to another user.
- If the user guesses the secret key without sending the request to the admin and download it then the user can easily leak the data.
- And when someone is leaking data, notification would be sent to the admin that someone is leaking data.
- We have also put another file security in it so that the user will not be able to download file easily.

USE CASE DIAGRAM – for Prevention (security)



- Admin will share file to user.
- If the user guesses the secret key without sending request to the user.
- At that time the admin will detect that leaker that when, which user has leaked which data.

VI. CONCLUSION

Sensitive Data can be leaked by unauthorized person unknowingly or maliciously. So our main aim is to identify leaker using some strategies and provide security to data.

REFERENCES

[1] Panagiotis Papadimitriou and hector Garcia-Molin, "Data Leakage Detection", IEEE Transactions on Knowledge and Data Engineering. Vol. 23, no. 1, 2011.
[2] Abhijeet Singh and Abhijeet Anand, "Data Leakage Detection using Cloud Computing", and Computer Science, vol.6, no. 4, April 2017.
[3] Abdullah Bamatraf, Rosziati Ibrahim, Mohd and Najib MohdSalleh, "A new digital watermarking algorithm using combination of least signification.Bit(LSB) and inverse Bit", International Journal of computing, vol.3, no.4, April 2011.
[4] Xin Zhou and XiaofelTang, "Research and Decryption", International Forum on strategic Technology, 2011.
[5] Riya Naik, Manisha Naik Gaonkar, "Data Leakage Detection in cloud using watermarking Technique",Computer Communication and Informatics(ICCI) 2019 International Conference on, 2019