International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Detection of Data Leakage

Chandrapal Chauhan[a]*, Divya Mankar*[b]*, Rupal Lonare*[c]*, Sakshi Bhujade*[abc]*

Priyadarshini College Of Engineerng, Nagpur-440019, India.
[*]Corresponding Author Email: divyamankar1999@gmail.com, Tel: +917385507004

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, (e.g., 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.

1. 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 otpgeneration, mail/message notification, password protected files. So, by this it will get easier to identify leaker and save the data from getting misused.

2. Overview

It is a web application which is developed in HTML, CSS, PHP, MYSQL. The purpose of this project/application is to manage unauthorized activities in an organization.

Fig. 1: USE CASE DIAGRAM for how to send request key and how receive the secret key and how to download.

- First, 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.

* *Corresponding author.* Tel.: +0-000-000-0000 ; fax: +0-000-000-0000.
E-mail address: author@institute.xxx

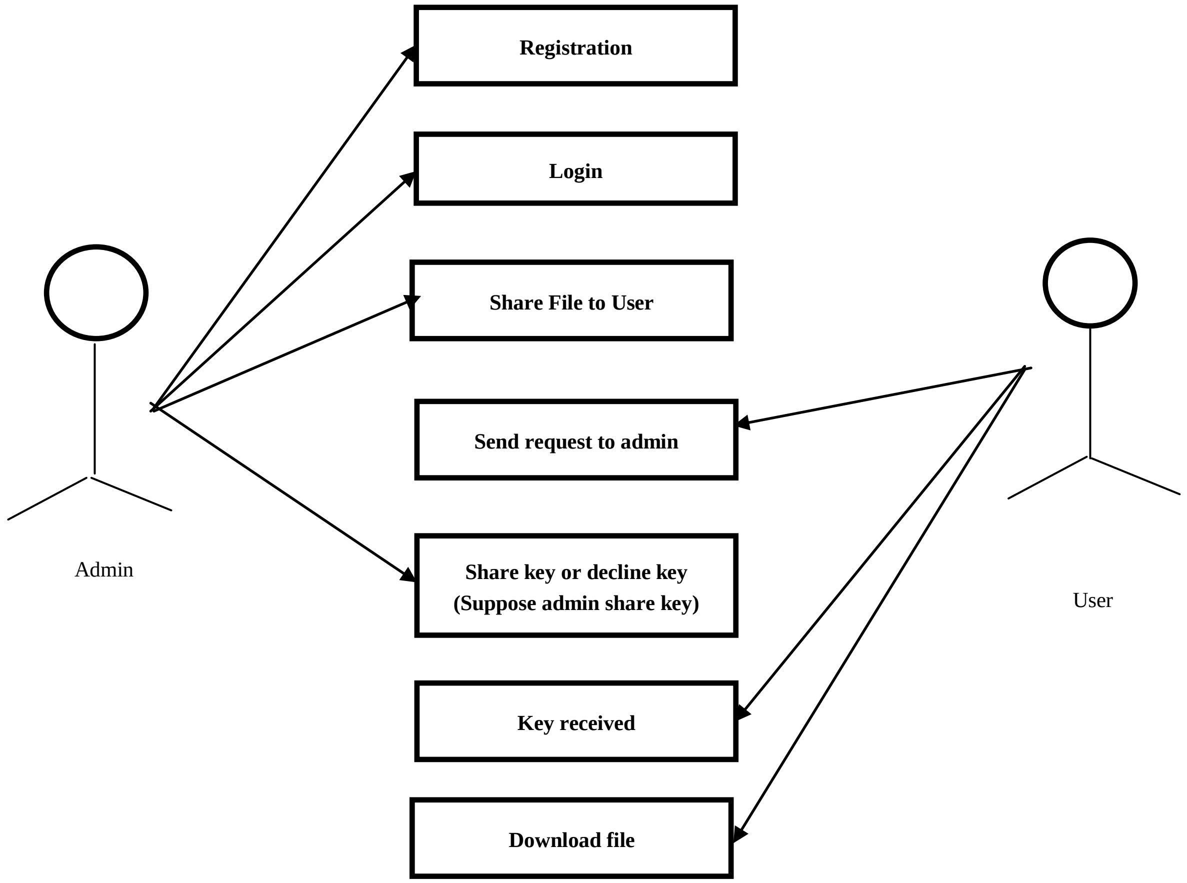


Fig. How to send request key and how receive the secret key and how to download

3. Literature Survey

Literature Survey is very important step in any software development process. Leakage of confidential data to the public is growing concern among organizations and individuals. Traditionally data was preserved using security mechanism such as firewalls, virtual private network and intrusion detection systems.

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.

4.Analysisand Design

System analysis is a problem-solving technique which improves the system and ensures that all the components of the system work efficiently to accomplish their purpose. The main goal of this system analyst is to detect the leaked data and prevent it from unauthorized activities and from hacking.

5.Development Requirement

Software Requirement:

- Windows / Linux / Unix
- MySQL
- Eclipse / NetBeans
- XAMPP Server

Languages:

- JSP
- JavaScript
- HTML
- Servlet
- Java
- CSS

Linux/ Unix/ windows – It is an operating system.
MySQL – It is an open-source relational database management system.
Eclipse/NetBeans – Both are open-source IDE's.

6.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.

7.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.

8. 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.
   Features Of Admin
   - Access of all data
   - Send Files
   - Send Files by Me
   - Send Files by Another
   - View Total User
   - Have power to know the leaker details
2) User - Here user only can send and can view data shared by another. User do not have authority to know the leaker information.
   Features of User:
   - **Register**: The user needs to be registered in order to login.
   - **Login:** The user needs to login to get access to the system.
   - **Share Files:** Here user can share files to other users
   - **Sent Files by Me:** The user can see files share by himself/herself.
   - **Send Files by Another:** Here user can see files send by another.
   - **Secret Key**: User needs to enter secret key to get access to file.
   - **Profile:** User can see profile of him/her.

This application contains following features:

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

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

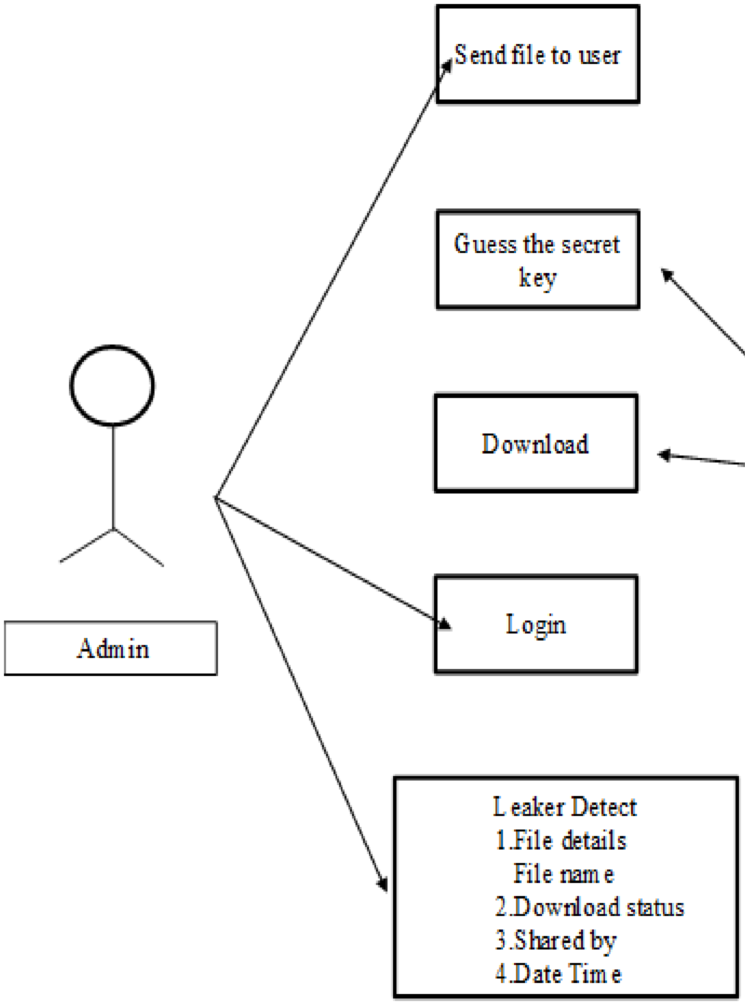
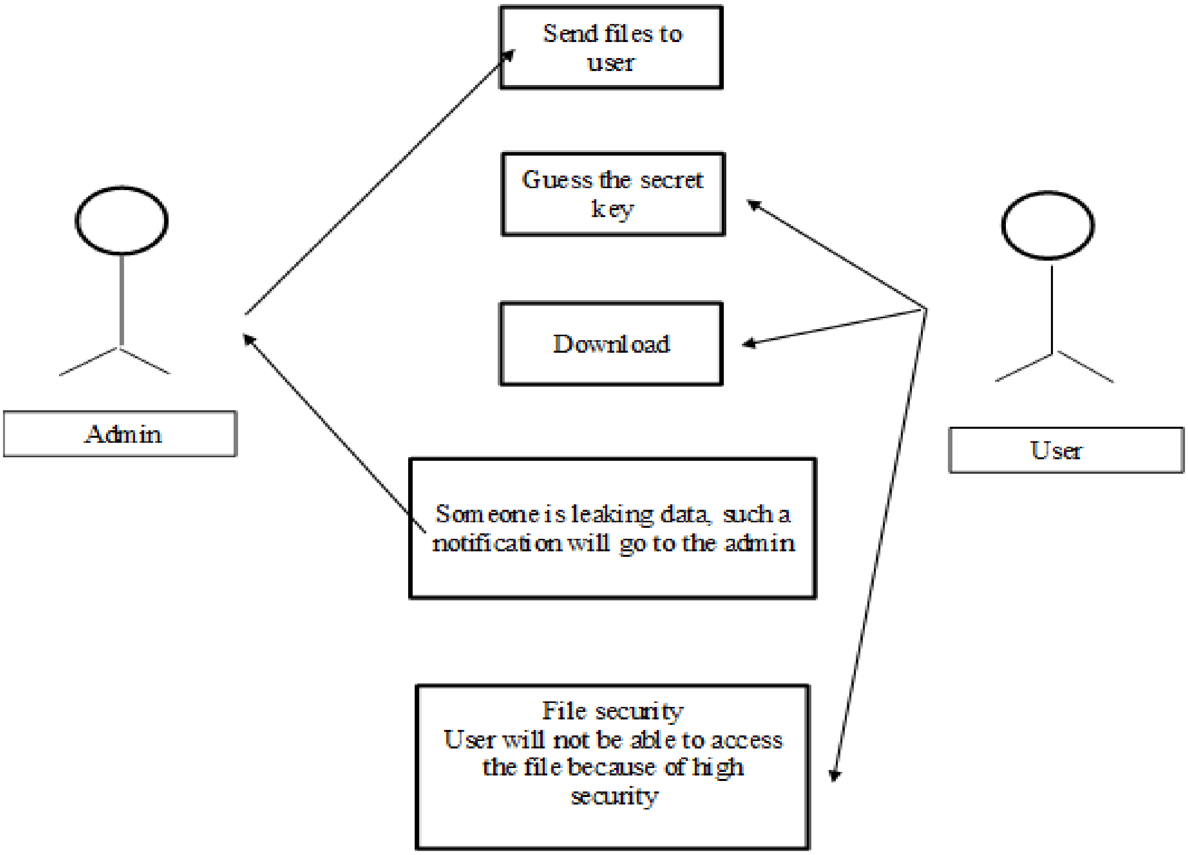


Fig. Download it by guessing without sending a key request and detect as a data leaker

- 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)


Send files to user
Guess the secret key
Download
Admin
User
Someone is leaking data, such a notification will go to the admin
File security
User will not be able to access the file because of high 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.

9. Future Scope

There can be various things that can be made it simple and user friendly. By increasing some little features, we can actually improve its functionality. Work of future includes the investigation of guilty agent models that captures the leaker scene that are not yet consider. The extension of data strategy in our system that they can handle user request in an online fashion. We will add more security to system in future so that data will not be leak.

10. Conclusions

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 Mohd Salleh, “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 Xiaofel Tang, “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