

# Secure Computing to Avoid Interactive Information Discharge

Sarfaraz Alam

Dept of Master of Computer Applications  
Sir M Visvesvaraya Institute of Technology  
Bangalore, India

Lakshmi K

Dept of Master of Computer Application  
Sir M Visvesvaraya Institute of Technology  
Bangalore, India

**Abstract-** In doing a business activity, normally delicate information needs to be given to supposedly trusted third parties. An emergency clinic could offer patient records to specialists who will devise new medicines. Also, an association could have organizations with various firms that require sharing client information. Another undertaking might re-appropriate its handling; consequently, information ought to tend to change various firms. The proprietor of the data is known as the distributor, and the agents are the supposedly trusted third parties. The goal is to find the agent once the distributor's sensitive information is spilled by him, and, if feasible, to recognize the agent that released the data.

**Keywords**—*Fake object, guilt agent, agent, distributor;*

## I. INTRODUCTION

### A. Problem Statement

Generally, watermarking is a method used to control leakage detection.[1] a novel code is connected to each distributed copy. Assuming that copy is subsequently found in the hand of the unlawful party, the leaker can be known. It included some changes to the original data, yet watermarks can be terribly helpful in some cases. Moreover, assuming the data's beneficiary is malevolent watermarks will commonly be obliterated. [2] The efficiency of the existing system is low and the traditional method of finding the agent leaker is difficult because there is no distribution of data to identify the exact leaker. The security system of the existing system is not much efficient.

### B. Objective

In an actual world,[3] It is not required to hand over sensitive data to users who may inadvertently or uninvitedly leak it. And even if sensitive data needed to be handed over, in an actual world, each entity could be watermarked, so that its origin could be traced with absolute certainty. The model is comparatively straightforward; it catches the essential trade-offs. [4] The algorithm gave a variety of data distribution strategies such as the binomial distribution; it will be used to identify the probability of leaking the data from the system. [5] This will be helpful in identifying the number of leakers using data distribution. Dispersing objects prudently can make a significant distinction in recognizing the guilt agent.

### C. Description of the Project

This project is to look at whether the information is spilled or not. The agent will give the information to communicate the data by means of a server to different agents. It is to check

whether the endorsed client released the data to a different agent.

## II. LITERATURE SURVEY

### A. Existing System

In the existing system securing the information is not much efficient. The information of the initial distributor is going to be modified, and that is understood as a knowledge leak that is combined with the embedded data copies. [6] Historically, leak detection is controlled by watermarking; e.g., a particular code is converged into every circulated copy, and assuming that is later discovered within the hands of an unauthorized party, the source might be known. [7] According to statistics, communications due to human errors and improper encryption of files and is the main cause of the leakage of data. In this system, there are no efficient algorithms for making the system fast and secure.

### B. Proposed System

In the proposed system, [8] distributors of data can determine the unauthorized users and their locations wherever their original data has been modified. In this system, if the unauthorized user is known, then the distributor will stop distributing their information with the agents and will even legally penalize them for information outpouring cases. [9][10] This project includes the development of a specific model by using different types of algorithms that support the distributors to identify the unauthorized data users and it can be used to determine the faults done by the third-party agents by using fake objects. Here fake objects act as a type of watermark. [11] This project has fingerprint matching to make the system more secure, prevent data leakage from the outside world, and also use advanced Encryption Schemes (AES) with 128-bit. So, it is powerful and it will encrypt the file using more round keys in the process of encryption.

### C. Feasibility Study

An understanding of the main requirements for the system is important for feasibility analysis; some key considerations involved in the feasibility analysis are

#### 1. Social Feasibility

It is to actually take a look at the degree of acknowledgment of the system by the client. This incorporates the most common way of training the user to capably utilize the system. The system is mainly used by the customer. The customer can

access the system using a secure system. It will make the proper communication between the System and user; the user can be able to access our project easily. The user should not feel dreaded by the system, despite should acknowledge it as a need.

## 2. Technical Feasibility

The proposed system is technically feasible in all ways because Java is used to develop the project. Java is the most popular language and it makes the system more secure. Using Java, various security systems can be implemented. Moreover, Java is the highly demanded language in the market. All the technical requirements for the project are very low. This System will require low configured RAM, storage, and all the hardware and software requirements.

## 3. Operational Feasibility

Data leakage is one of the important concerns nowadays and protecting the data is one of the biggest challenges. The implementation of the efficient algorithm and data distribution strategies is used to protect the data from unauthorized access, which the existing system did not have. The project is operationally feasible as it meets the organization's needs.

## 4. Financial Feasibility

This is used to monitor the economic feasibility of the project. The project is economically feasible for the customer. All the required software used in a project is available in open source, so there is no need to spend money on the software. All the requirements are available at a low cost and the resources needed for the project are also less. so it is economically feasible.

## D. System Requirements

Table: 2.1 System Requirement

|                        |  |
|------------------------|--|
| Hardware Requirements: | Processor : Pentium III<br>Hard Disk : 20 GB.<br>Speed : 1.1 GHz.<br>RAM : 256 GB (min).                   |
| Software Requirement:  | Operating system : Windows10.<br>Application server : Tomcat<br>Coding Language : JAVA<br>Database : MYSQL |

## III. SYSTEM DESIGN

The proposed architecture will be used to identify the list of fake agents who are attacking the system. To prevent the systems from hacking, it has a locking system. If anyone is trying to access the system, the admin will monitor the entire activity. [12] The system is accessed through a private network. So, the admin can regularly monitor the activity of each agent. In this case, if any agents try to leak the data or someone tries to attack the system, the admin will get the notification. So, the proposed architecture is identifying the list of fake agents. Meanwhile, all the data will be stored in the cloud which makes the system more secure.

## A. System Architecture

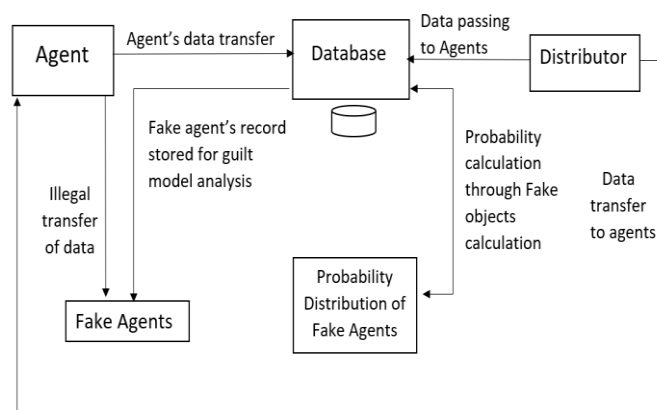


Fig: 3.1 System Architecture

## B. Use Case Diagram

A use case diagram is a behavioral UML or dynamic diagram that showcases the users/actors with their respective roles or functionalities of a system. The interaction may be between the modules or user and module. Here the agent is interacting with the component and can perform operations like creating an account, logging, downloading files, and locking and unlocking the files. Use case diagrams are mainly used to identify the interaction between the different objects in the system.

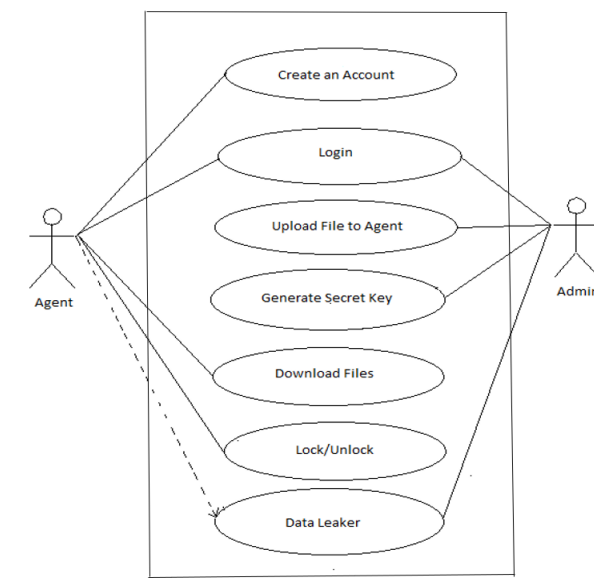


Fig: 3.2 Use Case Diagram

## C. Sequence Diagram

A sequence diagram is a process to check all the events that describe how processes interact with one another and in what order.

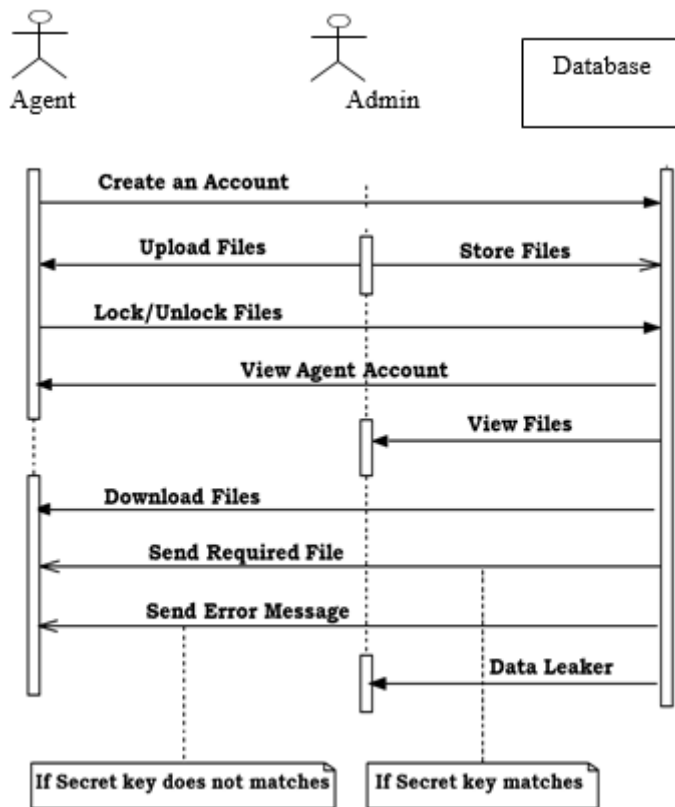


Fig: 3.3 Sequence Diagram

#### IV. IMPLEMENTATION

##### A. Module Description

In this Project we are having four Modules:

- Admin
- Cloud
- Security system
- User

##### 1. Admin

[13] The admin is the authorized person to access the system using their credentials and they can upload the files and they can view all the user details. As the user requests, the files from the admin. He will generate the secret key for each file and will send the secret key to the requested user through email. Agent activity is regularly monitored by the admin. The system is connected through private networks. If the agents try to leak confidential data or if some unauthorized person is trying to access the data, the admin will receive the message.

##### 1.1 ADMIN LOGIN PAGE

It is an admin login page where the admin can log in.



FIG: 4.1 ADMIN LOGIN PAGE

##### 1.2 ADMIN LOGIN MESSAGE

As the login is successful message will be shown.

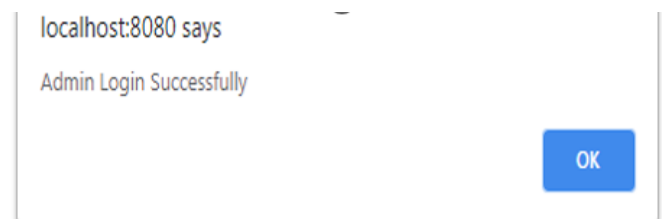


FIG: 4.2 ADMIN LOGIN MESSAGE

##### 1.3 ADMIN HOME PAGE

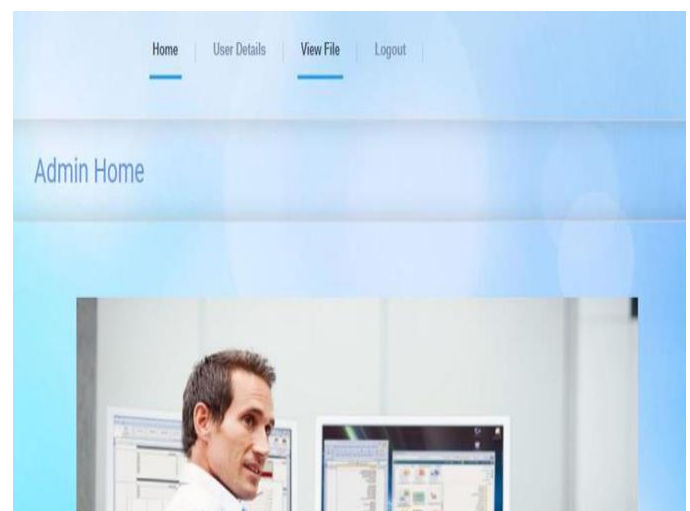


FIG: 4.3 ADMIN HOME PAGE

##### 1.4 VIEW FILE PAGE IN ADMIN

This is the view file page where all file details are shown.



| User ID | Name          | File       | date                    |
|---------|---------------|------------|-------------------------|
| 10      | sudip         | app        | 2016/Apr/16<br>07:40:07 |
| 11      | Gayathri Devi | safdsf     | 2020/Feb/23<br>20:58:55 |
| 12      | suraj         | suraj file | 2020/Feb/24<br>16:20:52 |

FIG:4.4 VIEW FILE PAGE IN ADMIN



| User ID | Name          | Email                     | Gender     | Mobile      | Date of Birth | Send File | Activate |
|---------|---------------|---------------------------|------------|-------------|---------------|-----------|----------|
| 13      | Gayathri Devi | mgayathridevice@gmail.com | 2020-02-23 | 09940975302 | Bangalore     | Send      | Send key |
| 14      | Gayathri      | mgayathridevice@gmail.com | 2020-02-12 | 09940975302 | Bangalore     | Send      | Send key |
| 16      | suraj         | mgayathridevice@gmail.com | 2020-02-24 | 09940975302 | Bangalore     | Send      | Send key |

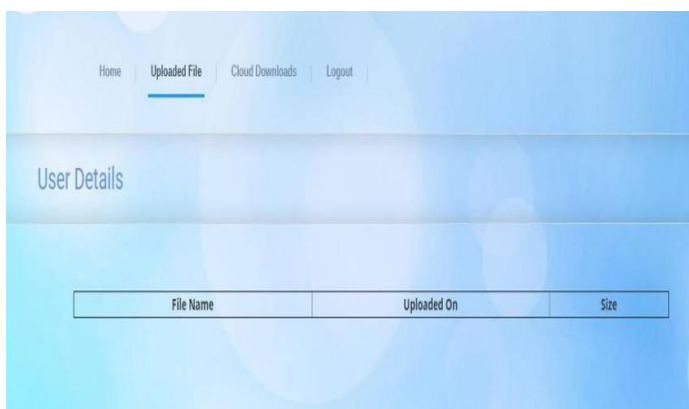
FIG: 4.6 USER DETAILS PAGE IN ADMIN

## 2. CLOUD

[14] The cloud Module is generally used to upload the files; The employee is able to upload all the files in the cloud. The files in the cloud are in the form of encryption. This will restrict the unauthorized users who are trying to access the data.

### 2.1 CLOUD UPLOAD PAGE

This is the cloud upload page where all the file details are uploaded.



| File Name | Uploaded On | Size |
|-----------|-------------|------|
|-----------|-------------|------|

FIG: 4.5 CLOUD UPLOAD PAGE

## 3. Security System

The admin will generate one unique key for each file and that is sent to the particular user who requested to access the file. The particular key is mailed to the particular user who wants to access the file. Meanwhile, there is fingerprint matching which makes the system more secure.

### 3.1 USER DETAILS PAGE IN ADMIN

This is the user's admin page of the project where user details are saved.

## 4. User

The user has to register their account along with the fingerprint upload. The fingerprint is important because if the user wants to download or they want to lock the files they have to use fingerprint matching. [15]The User can able to access the system using their credentials and they can lock the files using a fingerprint and secret key. If the particular file is locked then downloading the file is not possible. If they want to download the file, the file has to be unlocked, and using both a secret key and fingerprint the user can able to download the file.

### 4.1 USER LOGIN PAGE

This is the user login page where users and existing users can log in.

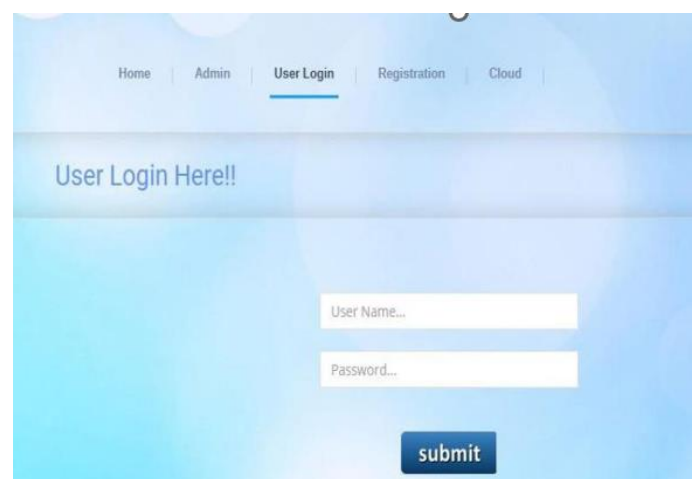
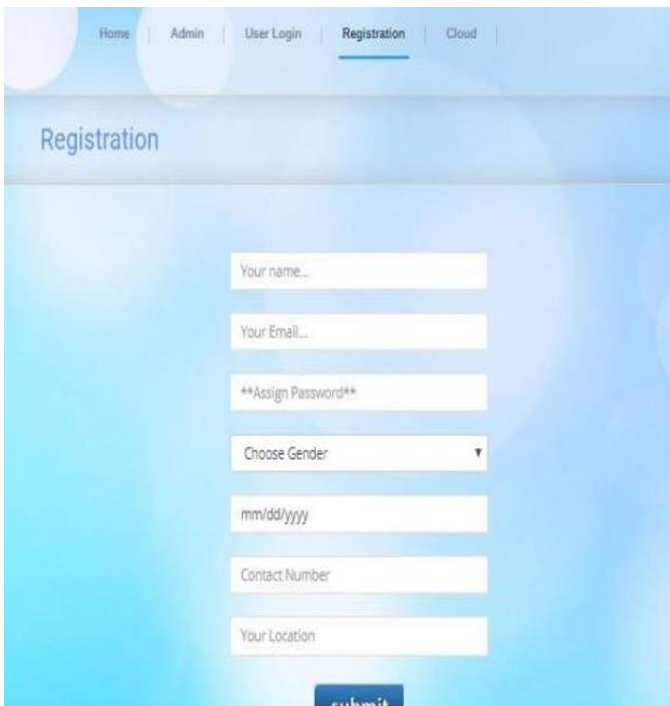


FIG: 4.7 USER LOGIN PAGE

### 4.2 REGISTER PAGE

This is the registration page for new users to sign up or create a new account.





Registration

Home | Admin | User Login | **Registration** | Cloud

Your name...

Your Email...

**\*\*Assign Password\*\***

Choose Gender ▾

mm/dd/yyyy

Contact Number

Your Location

**submit**

FIG: 4.8 REGISTER PAGE

#### 4.3 USER HOME PAGE

This is the user's home page.

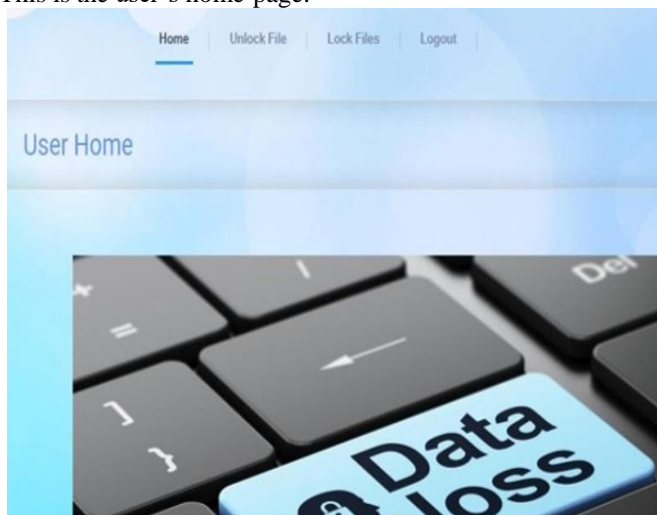
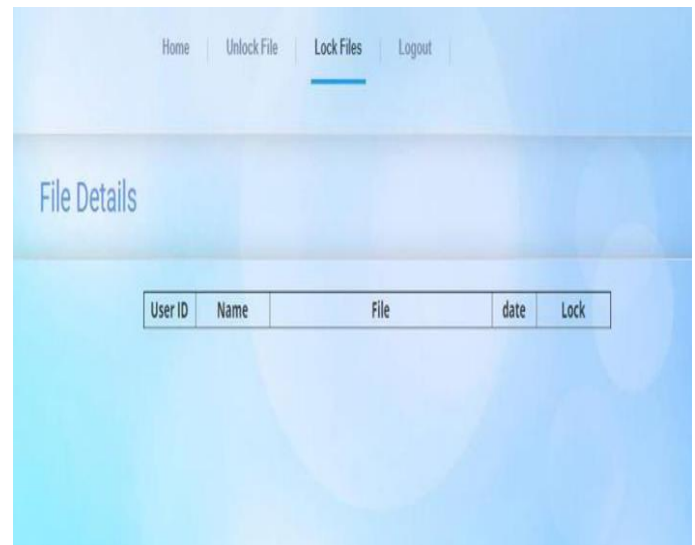


FIG: 4.9 USER HOME PAGE

#### 4.4 LOCK FILE PAGE USER

This is the lock page where the user can lock the file.



File Details

Home | **Unlock File** | Lock Files | Logout

| User ID | Name | File | date | Lock |
|---------|------|------|------|------|
|---------|------|------|------|------|

FIG: 4.10 FILE LOCK PAGE USER

#### 4.5 UNLOCK PAGE USER

This is the unlocking page of the project where the user can unlock the files.



File Details

Home | **Unlock File** | Lock Files | Logout

| User ID | Name | File | date | Lock | Download |
|---------|------|------|------|------|----------|
|---------|------|------|------|------|----------|

FIG: 4.11 UNLOCK PAGE USER

#### V. CONCLUSION

Nowadays the number of internet users has increased and protected the data from others is a big challenge. The delicate information spillage on computer systems makes a genuine threat to organizational security. As indicated by measurements, ill-advised encryption of records and correspondences because of human blunders is the primary driver of information misfortune. The danger currently reaches out to our own lives: a ton of individual data is accessible to informal organizations and cell phone suppliers who by implication move the information to dishonest outsiders. It is not needed to deliver sensitive data to the perfect world. There is a chance, knowingly or unknowingly, data may get leaked, and even if the sensitive data needs to be handed over, in an actual world, each entity could be watermarked. So that origins could be traced with absolute certainty. The proposed

system algorithm conferred a variety of data distribution strategies such as binomial distribution; it will be used to identify the probability of leaking the data from the system. This will help identify the number of leakers using data distribution. Distributing objects wisely can make a significant distinction in recognizing guilty agents.

#### REFERENCES

- [1] P. Papadimitriou, H. Garcia-Molina "Data Leakage Detection", Knowledge And Data Engineering, 51-63.
- [2] Data Leakage: What You Need to Know by Faith M. Heikkila, Pivot Group Information Security Consultant. P.P (1-3).
- [3] Asaf Shabtai, Yuval Elovici and Lior Rokach, "A Survey of Data Leakage Detection and Prevention Solutions", SpringerBriefs in Computer Science.
- [4] Subhashini Peneti and B. Padmaja Rani, "Data Leakage Prevention System With Timestamp", International Conference on Information Communication and Embedded Systems,
- [5] Rudragouda G Patil Dept of CSE, the Oxford College of Engg, Bangalore. "Development of Data leakage Detection Using Data Allocation Strategies"
- [6] IOSR Journal of Computer Engineering ISSN: 2278-0661 Volume 1, Issue 6(July-Aug 2012), PP 32-35
- [7] Xiaokui Shu and Jing Zhang, Danfeng Daphne Yao and Wu Chun Feng, "Fast Detection of Transformed Data Leaks, on Information Forensics and Security", 528-542.
- [8] The Who, What, When & Why of Data Leakage Prevention/Protection Presented by: Archie Alimagno California Department of Insurance P.P (2-7)
- [9] Michael Backes, Niklas Grimm and Aniket Kate "Data Lineage In Malicious Environments, on Dependable and Secure Computing", 178-191.
- [10] Yin Fan, Wang Yu, Wang Lina, Yu Rongwei, "A Trustworthiness-Based Distribution Model for Data Leakage Prevention", Wuhan university journal of natural sciences, 2010, Vol.15 No.3, 205-209.
- [11] A Handbook on Information Security Management, Harold F. Tipton, Micki Krause, Fifth Edition.
- [12] Information technology – Security technical - Code of practice for information security management. ISO/IEC 27002, 2005.
- [13] Data Leakage: Affordable Data Leakage Risk Management by Joseph A. Rivela Senior Security Consultant P.P (4-6)
- [14] Gilad Katz, Yuval Elovici, and Bracha Shapira, "Coban A context-based model for data leakage prevention", Information science on Springer.
- [15] Veronika Stamati Koromina and Christos Ilioudis, "Insider Threats in Corporate Environments: A Case Study for DLP", in Proc. ACM