

# A MODEL TO FIND THE AGENT WHO RESPONSIBLE FOR DATA LEAKAGE

Bhagwan D. Thorat<sup>1</sup>, P. R. Devale<sup>2</sup>

<sup>1</sup>Research Scholar, M-Tech Information Technology, BVDUCOEP, Maharashtra, India

<sup>2</sup>Professor, Information Technology, BVDUCOEP, Maharashtra, India

## Abstract

In this research paper, we implement the model to find the agent who responsible for data leakage system. The data leakage is one type of risk. Many times distributor sends some important data to two or more agents, but several times the information is disclosure and found unauthorized place or unauthorized person. The multiple ways to distributed important information i.e. e-mail, web site, FTP, databases, disk, spreadsheet etc. Due to this purpose information accessing in a safe way is become new topic of research and it became a contestant part to finding leakages. In this work we implement a system for distributing information to agents. In this method we add fake object to the distributed original data to the agent in such a way that improves the changes to finding a leakage. If agent sends this sensitive data to unauthorized person then distributor can receive one data leaked SMS, after that distributor can find the guilty agent who leaked the data.

**Keywords:** Significant data, fake data, guilty agent.

\*\*\*

## 1. INTRODUCTION

Information leakage detection is one of the most significant issues in corporate dealing mainly in current trend. In corporate business companies share client information with each other who are in association with that companies. In this situation information security is significant so information leakage detection will play important role. Companies send or handed over the important information to trusted agent. For example in research center some scientist can share important new research information to each other through trusted agents. Similarly another enterprise may outsource its information processing so information must be given to lots of other partner's. Usually information leakage finding is handled by watermarking. E.g. an exclusive code is embedded in each agent copy. If that copy finds an unauthorized person the guilty agent can be identified. It is very useful in certain cases, but again involves some alterations of the original data. In this model we solve the drawback of watermarking using data leakage detection system.

In this paper we develop a model to finding the agent who is responsible for data leakage detection system. We develop the model using the C sharp dot net technology to implement the model and use SQL server as database for backend support to store all information. In this model the agent send request to distributor for the data and distributor sends data back to agent by adding fake object in that data. If any one of the agents cheats the distributor by sending the data to unauthorized person, the distributor can detect who is guilty agent using guilty agent model.

## 2. PRECEDING SYSTEM

In the existing system usually information leakage detection is handled by the watermarking technology. E.g. an

exclusive code is embedded in each agent copy. If those copies find an unauthorized person the guilty agent or leaker can be identified. It is very useful technology. In watermark system one drawback is that sometimes original data can change or deleted.

## 3. PROJECTED SYSTEM

In the previous system watermarking technique is used. In this watermark technique a code is embedded in each agent copy and that code is find out to another unauthorized person then we decided the data was leaked but in watermarking system one drawback is that some time original data is changed. This drawback will be overcome to the data leakage detection system using fake object concept. In this projected system our aim is that to detect the administrator's sensitive information has been leaked by the trusted agent and possible to identify the person who leaked the information. The data leakage detection system is a very convenient method where the information is changed by adding the fake object to the original data before handover to the agent or trusted third party. Now we develop one method in this system to assess the guilty agent. We also using one new algorithm to this technique is that suppose agent send the request to the distributor for the data and distributor sends data back to agent by adding fake object in that original data and suppose any one of the agent cheats the distributors by sending the information to unauthorized person the distributor received one message that your data is leaked. After that distributor can detect who is guilty agent using guilt agent model and decide the fraud person along with the probability. A graph is used to display the probability of agent who leaked the data maximum time.

#### 4. IMPLEMENTATION PLAN

In this application we try to develop a model to finding the agent who is responsible for data leakage detection system. We develop the model using the C sharp dot net technology and Microsoft SQL server as database for backend support to store the file name, file path and fake object information for future reference when the distributor sends a file to agent. Same as when agent sends a file to unauthorized agent the sequence is store in the database and using this database the distributor received message that your data is leaked. After that we can find the guilty agent using guilt agent model.

#### 5. MODULE DESCRIPTION

- A) **Login-Registration Module:**-This module is specially implemented to provide the authority to agent and distributor to access the other modules of the project and also use new registration of agent.
- B) **Data Send Module:**-This module is specially implemented to handover information from administrator to agents and same module used for transfer data from agent to unauthorized agents.
- C) **Manage Users Module:**-This module is specially designed to approve the new registered agent.
- D) **Upload Article:**-This module is specially designed to upload the new data.
- E) **Guilt Agent Module:**-This module is specially designed to identify the guilty agent. This module checks the fake object in leaked data and determines the guilty agent and decides the fraud person along with the probability. A graph is used to display the probability of agent who leaked the data maximum time.

#### Algorithm

1. Start
2. Agent send request to distributor for data.  
 $R = \{R1, R2, \dots, Rn\}$   
 $REC = \{r1, r2, \dots, rm\}$   $F = \{F1, F2, \dots, Fz\}$
3. Distributor select agent to send data.  
 $M = \{M1, M2, \dots, Mn\}$   
 The distributor select agents and gives requested data R1, R2 to agents.
4. Distributors creates fake object & allocates it to the agents randomly.
5. Now the distributor checks how many agents have already received data.
6. Distributor checks remaining agents.
7. Distributor chooses remaining agents to send data.
8. Find the guilty agent and calculate the probability for guilt agent to compute this probability we need to find by the guilty agents.
9. Stop.

#### 6. RESULT

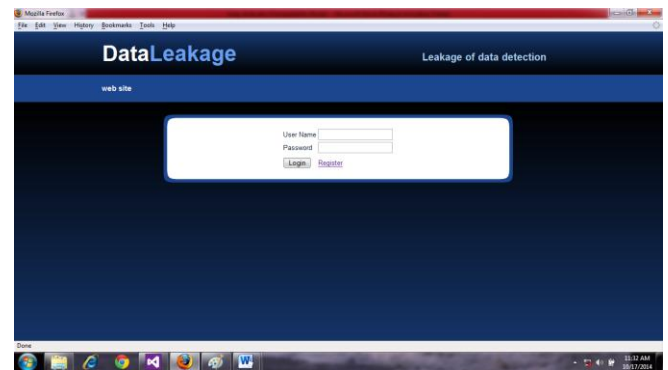


Fig1. Login Page



Fig2. Home Page

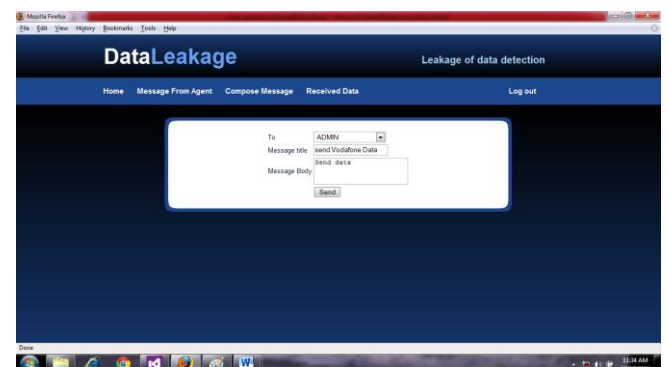


Fig3. Send Request page

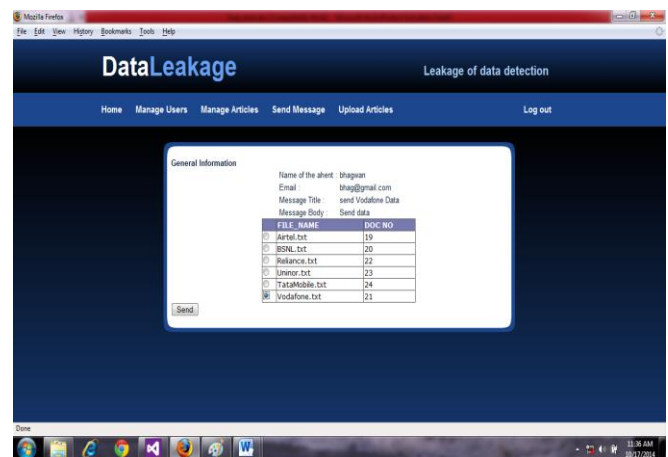


Fig4. Send Data Page

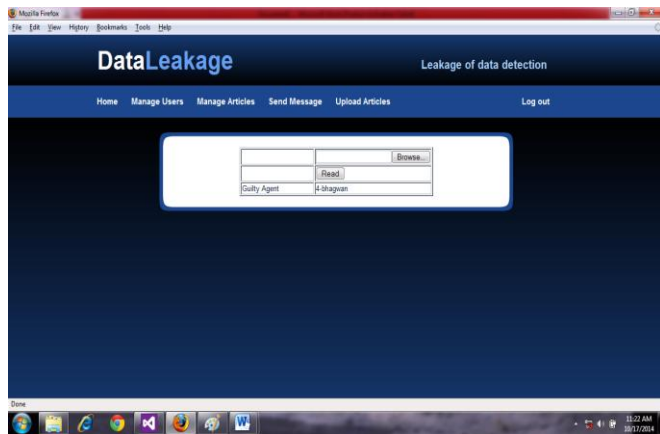


Fig5. Guilty Agent Detection Module page

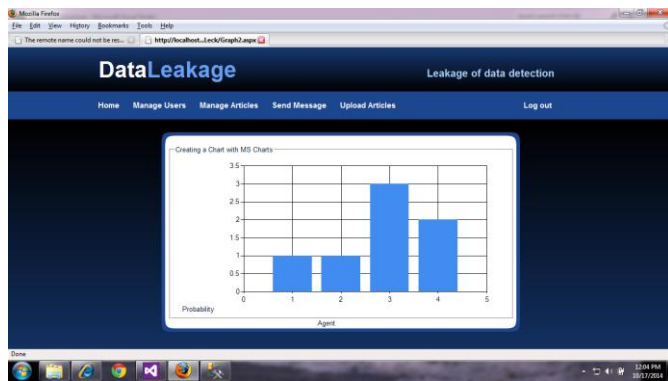


Fig-6. Calculate probability for Guilty agent

## 7. CONCLUSION

When a distributors necessity to send sensitive information to a trusted agents, it is needed to monitoring on the distribution process. When sensitive information has to be send through trusted agents the chances to leak the data is increased. In this research paper we try to solve this problem using fake object method. In this method when agent send request to distributor for the data and distributor send data back to agent by adding fake object in that original data. If any one of the agent cheats the distributor by sending the data to unauthorized person the distributor can detects who is guilty agent using guilty agent module. In this module distributor can browse the leaked data and find out the guilty agent ID and name by using fake object. We implement algorithm that are having data allocation method for enhancing the probabilities of distributor can identifying the leaker.

## REFERENCES

- [1]. Panagiotis Papadimitriou, Hector Garcia-Molina "A Model for Data Leakage Detection." Stanford University 353 serra street, Stanford, CA 94305, USA.
- [2]. Bhagwan D. Thorat, P. R. Devale "Identifying Guilty Agent for Data Leakage Detection System." International Journal of Advance Research in Computer Science and Management Studies. Volume 2, Issue 3, March 2014.
- [3]. Shreyta Raj, Ravinder Purwar, Ashutosh Dangwal "A Model for identifying Guilty Agents in Data Transmission."

International Journal of Advanced Research in Computer Engg. & Technology. Vol. 1, Issue 4, June 2012.

[4]. Y. Jagadeesh Kumar, M Chinna Rao. "Unauthorized Data Access Detection by Insertion of Duplicate Data Records." IJRCCT, Vol. 1, Issue 7, December 2012.

[5]. Sridhar gade, Kiran Kumar Munde, Krishnaiah R. V. "Data Allocation Strategies for Leakage Detection." IOSR Journal for Computer Engg. Vol 5, Issue 2, Sep-Oct. 2012.

[6]. R. Arul Murugan, Kavitha. E, Nivedha. M, Subashini. S "Data Leakage Detection and Prevention Using Perturbation and Unobtrusive Analyzes." International Journal of Communications and Engineering. Vol 4, Issue 3, March 2012.

## BIOGRAPHIES



**Bhagwan D. Thorat**, B.E. Computer Engineering, Pursuing M-Tech Information Technology in Bharati Vidyapeeth Deemed University College of Engineering, Pune, Maharashtra, India.



**Prakash R. Devale**, M.E. Computer Engg, Pursuing Ph. D in Bharati Vidyapeeth University, Pune, Maharashtra, India. Currently working as Professor in the Department of Information Technology, Bharati Vidyapeeth Deemed University College of Engineering, Pune, Maharashtra, India.