



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Detecting Guilty Party using Fake Object Testing and Block while Sending Original data

Y I Jinesh Melvin, K S Charumathi

Assistant Professor, Dept. of Computer Engineering, I.T., PIIT, New Panvel, New Mumbai, India

ABSTRACT: In Today's real business world more number of sensitive data has been leaked by an untrusted agent for a third party. For example Company's agreement projects, Hospital patient reports, Government Sensitive data, Military secret data, etc. These types of sensitive data are very secure by an authorized person. Water Marking is the technique to secure the sensitive data, but it has some disadvantage, Perturbation also to modify the sensitive data while sending to an agent and another technique is a fake object with original data, it makes the file size as large also the data are made less sense. It is not a proper secure because original data also transfer by distributor without any trust with an agent. In this proposed scheme to overcome these type of faults using two methods. (1) Test the agent with only fake objects. (2) Block the agent who sends the original data from the distributor.

KEYWORDS: Data Leakage, Data Leakage Model, Fake Objects, Guilty Agent, Blocking

I. INTRODUCTION

A Distributor has sent the sensitive data to his agent with proper secured, but some unauthorized person trying to leak the data, hackers also include in-between distributor and agent to attack sensitive data and to make illegal business. Data leakage in the sense of information leakage. The scope of data leakage is very wide many techniques has followed to reduce the leakage and find the guilty party. It is very useful for the distributor, but day-by-day hackers and guilty party were using loopholes from previous technique.

Watermarking is a useful technique to detect the leakage, from these the unique code is injected into all distributor copies, but it modifies the original data also it destroy and the agent doesn't get the actual data from distributor [4]. When compared with allocation strategy, the watermark is less sensitive [3]. Hackers can easily attack. In allocation strategy method distributor inject "realistic but fake" data record to improve the detecting leakage and find a guilty agent, but in "realistic but fake" method distributor add fake objects with real-data. Some intelligent hackers will fragment the original data from fake, also by using these method file size also be increased.

Today's economic world an enterprise on a daily basis sends large number of data and received through email, downloads, server and various channels. They hold only the sensitive it has been controlled from leakage [3]. In this paper our goal is to find a more accurate guilty agent, who has leaked the sensitive data from the distributor using agent testing with only fake object and block while sending original data.

II. METHODOLOGY

Sensitive data must be handed over to supposedly trusted third parties. The perturbation is a very useful technique. It moves the object which created as fake and modify the data as less sensitive. Normally leak detection is handled by watermarking [4], while distributor hides the data as an image it corrupt those data and destroy if the data is a beneficiary is malicious. In this paper the proposed unobtrusive technique for detecting leakage and block guilty agent.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

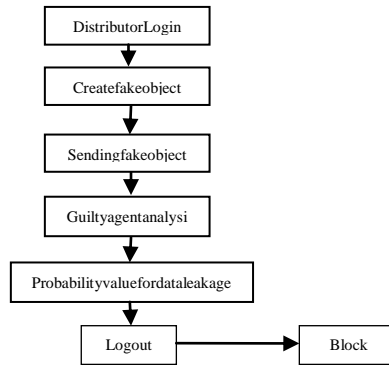


Fig. 1. Overview of New Technique

III. PROPOSED SCHEME

Distributor wants to send an original data to agent by using a fake object testing algorithm. While sending data if distributor finds any guilty party, then unauthorized party will block by distributor. Our main focus is that how the distributor intelligently give data to an agent, and how distributor choose an agent is trusted or not. In this proposed scheme two techniques to improve the chance of detecting Guilty agent.

1. Test the agent with only fake object.
2. Block the agent who send the original data from distributor circle.

In Distributor circle number of agents can allow to make relation witha distributor. Consider an agent as A and the number of agents as $A = \{A_1, A_2, A_3, A_4, \dots, A_n\}$, agents wants to register and get an agent ID from the distributor. Before sending the data to agent, distributor will randomly choose agents to test where they are trusted or guilty. From [3] distributor creates some fake objects $F = \{f_1, f_2, f_3, f_4, \dots, f_n\}$ for agent A_i is a function $CREATEFAKEOBJECT(A_i, F_i, cond_i)$, it takes the input object for all objects A_i , the subset of fake object F_i that has been received to agents and $cond_i$ returns a new fake object. The Distributor can also use $CREATEFAKEOBJECT()$ function when he wants to send some fake object to a set of agents. Distributor chooses agent random order using e-optimal method [3]. This method is to improve the chance of detecting a guilty agent. Evaluating an algorithm relative to a random allocation. Distributor randomly chooses agents and send the fake object to test, so each agent's value will increase as 1. Suppose anyone agent forward those fake objects to a third party without the permission of distributors, again the value will increase in the database, it's controlled by the distributor. In this technique distributor can send number of fake objects to the agent. The total probability value for each agent is calculated as the total number of fake objects which has received or forward by a particular agent divided by the total number of fake object send by distributor.

$$\text{Agent } PA_1 = \frac{FA_1}{F}$$

- PA_1 \longrightarrow Probability of Agent A_1
- FA_1 \longrightarrow Total number of fake object receive or forward by agent A_1
- F \longrightarrow Total number of fake object

Suppose any intelligent agents identifies the received object as a fake object, then they will act as a trusted agent for their distributor, then original data has been sent from the distributor, at that situation any agent is trying to leak the sensitive data then the system will ask distributor permission. Distributor noted those agents, give black-mark and block from distributor circle.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

IV. DESIGN ARCHITECTURE

Consider D as Distributor and A as Agent, the database is common for both distributor and agent, but the database is controlled by distributor. In distributor circle number of trusted agents were allowed. The distributor sends some fake object to the agent which stores in the database. If any agent forward the fake object to any third party, then the probability value will increase for those agents. The probability value is calculated from the database shown in Fig (2).

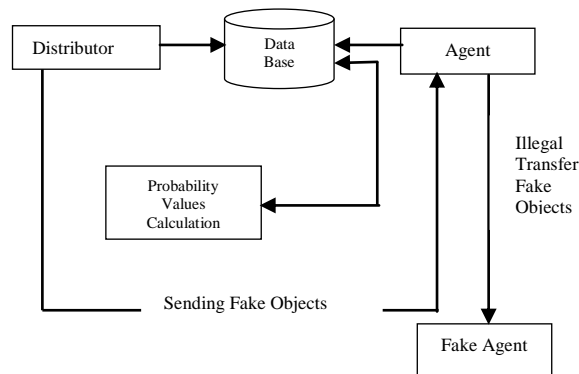


Fig. 2. Testing Guilty Agent using Fake objects

From Fig (3), suppose the intelligent guilty agent can identify that the objects are fake, then they will act as trusted. For these types of guilty agents only distributor allows the blocking system.

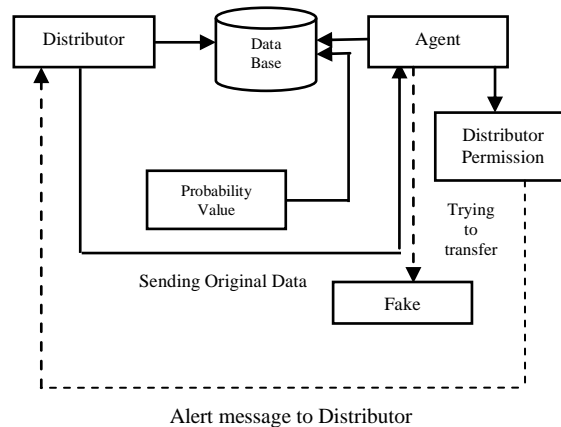


Fig.3. Blocking Guilty Agent while trying to send original data

V. ALGORITHM EXPLANATION

A. Description of the Proposed Algorithm:

- Distributor randomly select multiple agent to send data.
- Distributor creates fake objects to test selected agent.
- Consider fake objects as $(f_1, f_2, f_3, f_4, \dots, f_n)$ and send to agent in random order.
- After receiving the fake objects by all the agents, there probability value will increased as 1.
- If any agents try to send those fake objects to a third party without the permission of distributor then again the probability value also be increased.
- Probability values has been checked by distributor and take actions against the



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Guilty agent.

- After testing distributor again sends the original data to trusted agents as randomly. Unfortunately, anyone tries to send the original data to a third party, then this system will ask the distributor permission.
- Distributor got the alert messages to block guilty agent from distributor circle.

B. Algorithm Steps

Step 1: Allocation for fake object request to Agent [6]

Input $A_1 \dots A_n$ $cond_1, \dots, cond_n$, f_1, \dots, f_n , F

Output A_1, \dots, A_n F_1, \dots, F_n

1. $A \leftarrow \emptyset$
2. For $i = 1, \dots, n$ do
3. if $f_i > 0$ then
4. $A \leftarrow A \cup \{i\}$
5. $F_i \leftarrow \emptyset$
6. while $F > 0$ do
7. $i \leftarrow \text{select agent } (A, A_1, \dots, A_n)$
8. $f \leftarrow \text{create fake object } (A_i, F_i, cond_i)$
9. $A_i \leftarrow A_i \cup \{f\}$
10. $F_i \leftarrow F_i \cup \{f\}$
11. $F_i \leftarrow f_i \cdot 1$
12. if $f_i = 0$ then
13. $A \leftarrow A \setminus \{A_i\}$
14. $F \leftarrow F \cdot 1$

Step 2: Agent Selection Algorithm for e-random

1. Function SELECTAGENT (A, A_1, \dots, A_n)
2. $i \leftarrow \text{select at random an agent from } A$
3. return i

VI. SIMULATION RESULTS

To overcome the existing techniques the proposed paper representation invisible those techniques and it gives more effective than previous watermarking technique. A watermark is invisible notation to identify leakage data, but our proposed techniques concentrates on identifying leakage and blocking the guilty agent from distributor circle. Various modules created for identifying the guilty agent and accessing the particular agent's probability value. The agent wants to register the account to the distributor for authentication purpose. The record may store in a database that can be visible to distribute from fig(4). Distributor creates a number of fake objects and choose the agent at random. Then the distributor sends the fake object to those agents, this is to improve his effectiveness in detecting guilty agents. Also the use of fake object is to trace the record. When the distributor gives the wrong secret key to download the files the fake file will open, and the fake details are sent to the third party. Then those agent account will increase this module fig (5).

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015



AGENT SIGNUP

Agent ID:

Agent Name:

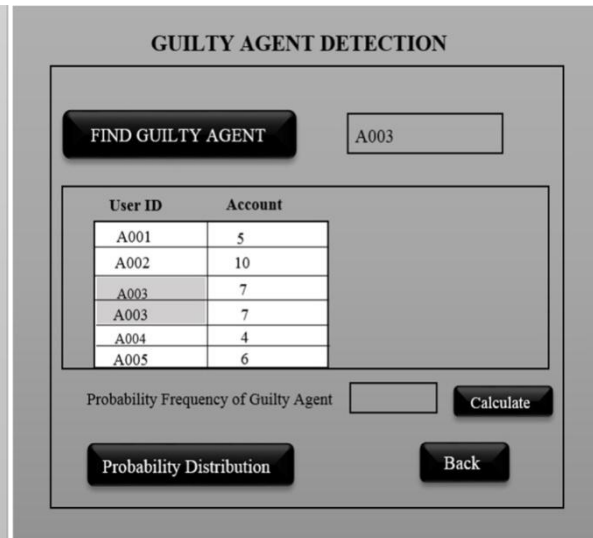
Agent Password:

Agent CPassword:

Agent Email:

Agent Contact:

Fig. 4. Registration



GUILTY AGENT DETECTION

User ID	Account
A001	5
A002	10
A003	7
A003	7
A004	4
A005	6

Probability Frequency of Guilty Agent:

Fig. 5. Guilty AgentDetection Module

From fig (6) Consider that the distributor sends total number of fake data is 20. In distributor circle five agents available. Third agent's account is increased than other four agent account, so the distributor calculate the probability of agent 003. This module is easy to identify the probability value of each agent. It can be controlled by the distributor.

A data distributor has given a sensitive data to trusted agents. Some of the data are leaked and found in the unauthorized place. The distributor can access the leaked data any agent, as opposed to having been independently gathered by other means admin can able to view the leakage files from the agent explained in fig(7)

AGENT ID	ACCOUNT	PROBABILITY VALUE
A001	05	0.25
A002	10	0.5
A003	07	0.35
A003	07	0.35
A004	04	0.2
A005	06	0.3

Fig. 6. Calculate Probability Value

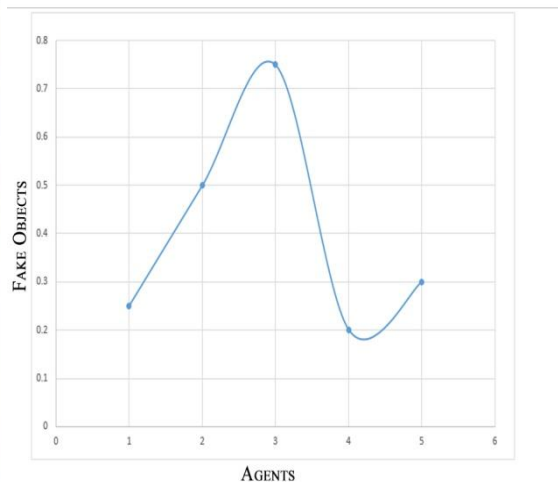


Fig.7. Probability Distribution of Agent Data



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

VII. CONCLUSION AND FUTURE WORK

Surviving of existing system, we find out some loopholes from previous techniques. Watermarking is the technique to hide the sensitive data, but it fails to make the data as sensitive and sometime it will destroy the data, also a perturbation technique in watermarking which modified the original data, but it acts as less sensitive. In “realistic but fake” technique the fake object is attached with the original, and the file size also high. Where the proposed scheme is to invisible these techniques and test the agent using fake objects and block the guilty party. Future works include the extension of blocking the guilty party and the distributor gets high priority with trusted agents and to transfer the high sensitive data between distributor and trusted agent with proper security.

REFERENCES

- [1] Sandip A. Kale, S.V.Kulkarni, “Data Leakage Detection”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, pp.668 - 678, Nov 2
- [2] Chandni Bhatt, Richa Sharma, “Data Leakage Detection”, International Journal of Computer Science and Information Technologies, Vol. 5, pp. 2556 - 2558, 2014
- [3] Lipi George, Mr.S.Vinoth Kumar, Dr.S.Karthik, “Detecting Guilty Party Using Dynamic Agents In Data Leakage”, International Journal of Scientific & Engineering Research, Volume 3, Issue 7 July - 2012
- [4] R. Agrawal and J. Kiernan, “Watermarking relational databases”, International conference on Very Large Data Bases , pp. 155 – 166, 2
- [5] Amol O. Gharpande ,V. M. Deshmukh, “Data Leakage Detection”, International Journal of Computer Science and Applications Vol. 6, pp.216 - 219, Apr 2013.
- [6] Karthik.R, Ramkumar.S, Sundaram.K, “Data Leakage Identification and Blocking Fake Agents Using Pattern Discovery Algorithm”, International Journal of Innovative Research in Computer and Communication Engineering Vol. 2 Issue 9, September 2014
- [7] P. Papadimitriou and H. Garcia - Molina, “Data Leakage Detection”, technical report, Stanford Univ., 2008
- [8] S.U. Nabar, B. Marthi, K. Kenthapadi, N. Mishra, and R. Motwani, “Towards Robustness in Query Auditing,” Proc. 32nd Int’l Conference Very Large Data Bases (VLDB ’06), VLDB Endowment, pp. 151 -162, 2006
- [9] F. Guo, J. Wang, Z. Zhang, X. Ye, and D. Li, “Information Security Applications”, An Improved Algorithm to Watermark Numeric Relational Data, pp.138 – 149, 2006
- [10] F. Hartung and B. Girod, “Watermarking of uncompressed and compressed video”, . Journal of Signal Processing” , , Vol.66, pp.283 – 301, 1998

BIOGRAPHY

Y I Jinesh Melvin is Assistant Professor in Computer Engineering Department, Pillai Institute of Information Technology Engineering Media studies and Research, Mumbai University, New Panvel, Navi Mumbai, India. He received Master of Engineering degree in 2014, Dept. of Computer Engineering in Anna University Chennai. His research interests are Data Mining, Computer Networks, Image Processing etc.

K S Charumathi is Assistant Professor in IT Department, Pillai Institute of Information Technology Engineering Media studies and Research, Mumbai University, New Panvel, Navi Mumbai, India. She Completed Master of Engineering degree in 2014, Dept of Computer Engineering, from University of Mumbai. Her Research areas are Computer Networks and Security.