INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Ubiquo of Data Collection from Server to Mobile Device

R. Nivedha
Student, Department of Computer Science Engineering
Saveetha School of Engineering, Saveetha University, Thandalam, Chennai, India

Abstract:
This paper presents a Ubiquo of data collection from the system server to mobile. Here, we proposed an approach for accessing the network efficiently in an organization and collect data through a mobile. The common problem is that, the data that are leaked might be found in the third parties hand (in the net). Data leakage is one of the biggest challenges in front of the industries & different institutes. In order to improvise the possibilities of identifying the leakages, the data are distributed strategies among the agents. In some cases, to increase the chances of identifying the data leakages and the guilty party could be done by inserting some fake data.

Key words*: Mobile computing, Data extraction, data leakage detection, Web minning, Fake records, leakage model, data privacy, guilty agent, data distributor*

1. Introduction

Data leakages are one of the biggest issues in most of the institutions and industries. Though there is different encryption algorithm designed for data security, there is a big issue of integrity among the users. It is hard for any system administrator to track the data leaker among the system users[3]. It creates a lot of ethical problems in the Working environment. After the data is distributed among the agents, we may find those data that are found in the hands of some third parties[6] [7].Our goal is to identify the person by whom the data have been leaked[10]. Here we designed a method for estimating the "guilt" among the agents[8]. In this paper certain logical concepts have been presented to enhance the better working of the proposed model (identifying the leaker) using the existing algorithm.

2. Existing System

A broadly enabled technologies such as firewalls, encryption, access control, identity management, machine learning context based detectors and others have already been implemented for providing protection against various data leakage threat.

Traditionally the data leakage is detected using Watermarking[5] [6] [8].

Watermarking is a image or pattern where an unique code is inserted in a each copies and distributed to the users[4]. If that copy is found with an unauthorized person then the leaker can be identified easily.

2.1. Problem Definition

- To detect whether the data has been leaked by agents.
- To prevent the leakage

E.g. In a hospital the patient records can be given with the actual data along with some fake data are added and distributed[8] . Such fake data appears realistic to the agents[2]. If the fake data was leaked, then the distributor can easily identify which agent was guilty[2][9]. In the same way an organization might have a relationship with some other organization that needs agent details. So that the data must be shared with other companies [7]. This goal helps to detect by which agent the data has been leaked.

Disadvantage of watermarking are

- It is time consuming,
- Limited digital protection,
- It can be easily hacked.

3. Proposed System

By considering the above goal in our mind in this section we develop a model to find the guilty party among the agents. In this approach we present an algorithm which is used to identify the data leaker[3]. This is implemented by using client server method. The server is a computer or a computer program that manages access to a centralized resources or services in the network. A process that shares resources between client processes is called a server. For example file sharing . Here the server is a computer that controls and manages a database for sharing files. The server's function is to manipulate the data through its network. As shown in fig.1. A single system is assumed to be a server and all the client system data are frequently updated in the server database.Our goal is to detect by which agent the data has been leaked. The proposed approach is to detect the data leakage and the guilty agent who leaked the data. This could be done by implementing an algorithm, which is used to send an alert message to a mobile device when the data has been leaked. The algorithm which keeps track of the number of count the data has been sent.

When the count exceeds for more than once, the alert message is received to the mobile device.

3.1. Analysis

- Administrator (A) is a system that distributes data to the agent.
- Data (D) is a set of sensitive data.
- Agent (U) is a set of agent to whom the sensitive data is to be sent.
- Agent request the data to the administrator, admin verify the authentication and provide the access.

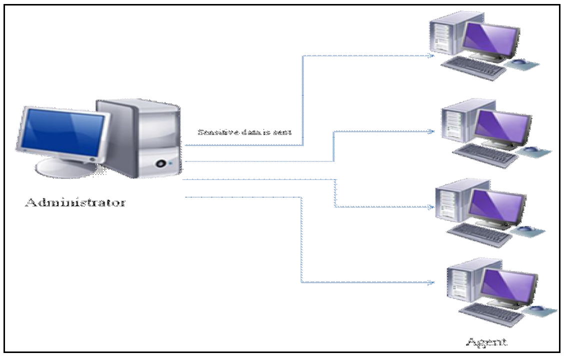


Figure 3.1: Agents requesting data for administrator

In networking the following servers are used such as application , sound , database, communication , file , name , standalone , game, proxy server. But in our approach we are going to use an application server. An application server is developed to run a software applications, here we develop an application by using algorithms for identifying the leakage of data. Data is collected from all the sources and updated in the server database.[1](sql 2008 database is used)

Generally in android mobiles SQ Lite database is used as the server. In this server only less data can be stored in the database. To overcome the less storage space, SQL 2008 is used. In SQL 2008 all system data can be stored in its database. It is flexible since the connection between mobile and server is easier. SQL 2008 server is comparatively secured and the storage space is more .The server database keeps track of the data that is being used by the agents. The system number and the agent details are created in the form of table and stored in the database. The multiple agents access the data simultaneously which has been allocated to them, is continuously updated in the database.

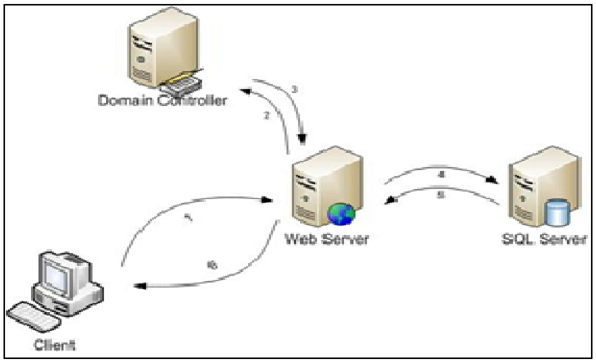


Figure 3.2 A Message From the Database mobile device is connected to the system server [1]

We get an intimation message from system server when the agent sends the reports for more than once. Pathway between the mobile and system server is developed by the use of algorithm.

4. Authenticated Users

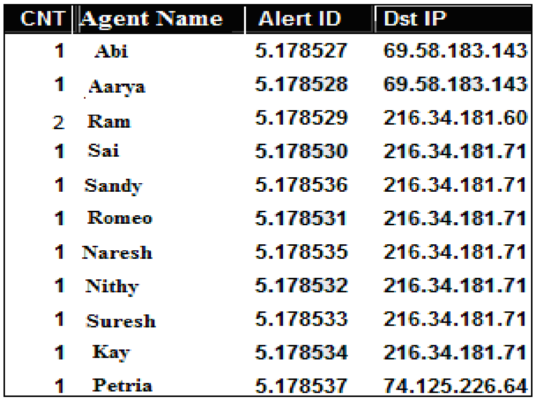
Each agent is provided with an unique id and password to verify whether they are an authenticated person or not. When an agent sign in into their user account, the agent gets the access of the data which has been allocated to them. This is done to ensure the level of authorization. By this process the data is secured from the third party.

4.1. Detection Strategies

- The algorithm keeps track of the number of count the data has been sent.
- When the count exceeds for more than once, the alert message is received to the mobile device.

4.2. Algorithm

```
Step1:  Administrator having set of data
                A=(D1, D2…)
Step 2: Agent request for data (D)
                U1=(d1)
                U2=(d2)
Step 3: After completion of project
                U1(d1) -> A
                U2(d2) ->A
Step 4:  If the data sent exceeds more than once
        [ Ux ( Dx > 1 ) ] => Alert message is sent to the admin mobile
```



CNT	Agent Name	Alert ID	Dst IP
1	Abi	5.178527	69.58.183.143
1	Aarya	5.178528	69.58.183.143
2	Ram	5.178529	216.34.181.60
1	Sai	5.178530	216.34.181.71
1	Sandy	5.178536	216.34.181.71
1	Romeo	5.178531	216.34.181.71
1	Naresh	5.178535	216.34.181.71
1	Nithy	5.178532	216.34.181.71
1	Suresh	5.178533	216.34.181.71
1	Kay	5.178534	216.34.181.71
1	Petria	5.178537	74.125.226.64

Figure 4.1: Agent reports stored in database

Here there are two people who play a vital role one is administrator and another one is agents. The administrator login into their id to perform the following functions such as who takes control of all other agents ,who approves the user privileges of other agents ,distributes the data among the agents ,edit and delete the dataset ,stores the data ,encrypt and decrypt the data. When an agent login into their account, the admin checks for the privileges and then the following functions can be performed by the agents such as register for the user privileges , access the data , store the data ,sends the report to the admin ,encrypt and decrypt the data. Check for agent’s authentication. If the agent user id and password is valid, the agent can access the data. Else the access to the data is denied. To identify the data leakage. Check the sent data count. If the count is greater than one then it is immediately updated in the database and the data is lost in the agent system.

The guilty agents’ details are received from the server database. Finally an alert message is sent to the administrator mobile.

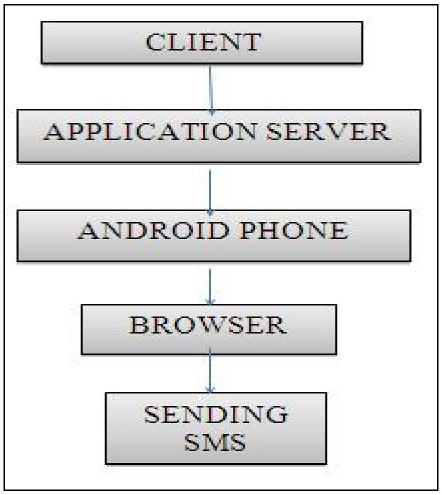


Figure 4.2 Architectural Diagram

4.3. Alert Message Algorithm

- STEP 1: Check for agent's authentication.
- STEP 2: If the agent user id and password is valid , the agent can access the data.
- STEP 3: Else the access to the data is denied.
- STEP 4: To identify the data leakage.
- STEP 5: Check the sent data count.
- STEP 6: If the count is greater than one then it is immediately updated in the database
- STEP 7: And the data is lost in the agent system.
- STEP 8: The guilty agents' details is received from the server database.
- STEP 10: Finally an alert message is sent to the administrator mobile.

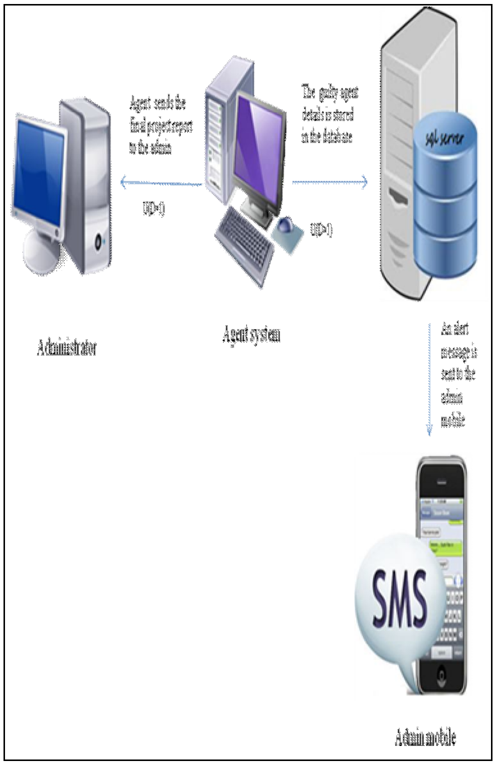

Agent sends the final project report to the admin
UID>1
The guilty agent details is stored in the database
UID>1
sql server
Administrator
Agent system
An alert message is sent to the admin mobile
SMS
Admin mobile

Figure 4.3: Alert Message

5. Guilty Agent

Guilty agent is an agent who violates the rules and tries to leak the sensitive data to the third party[2][10]. The guilty agent could be identified by using an algorithm. Here the agent can send the data only to the administrator. The algorithm keeps the track of the number of times the data has been sent. The data sent from the agents system is continuously recorded in the server database. If it exceeds the count , the data will be lost in the agent system. Since the count is increased , an alert message is sent to the mobile through the server. By this approach the guilty agent can be identified by the administrator.

- By using the traditional watermarking (which is easy to hack).The data leakage could not be contained and the guilty agent is unidentified.
- As per the proposed system the guilty agent can be easily identified by an alert message to the mobile from the system server.
- The algorithm that has been presented implements a variety of detection strategies that can improve the administrator chances of identifying a leaker.

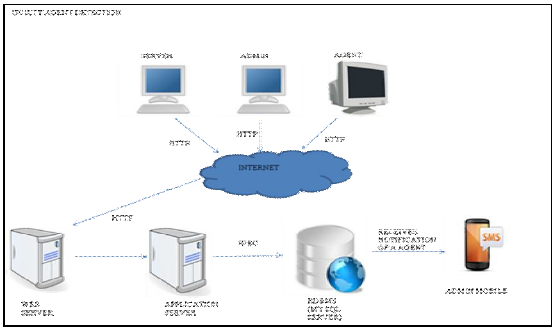


Figure 5.1: Guilty Agent Model

6. System Server to Mobile

JDBC is a driver library that connects the server and the SQL database. Java database connectivity (JBDC) defines the way in which the client access the data in the database. JTDS-1.2.5.jar is a jar file that provides a link between the mobile and the server on the linux platform. A web kit is used to connect the server to the browser. It consists of PHP language at the front end and database MYSQL at the back end. MSMTP is an SMTP client which is used to support the send mails.

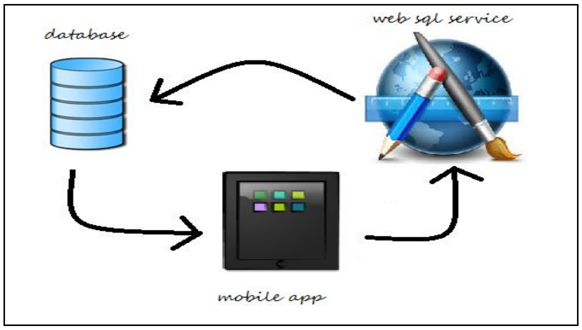


Figure 6.1: Server to Mobile

The following steps should be followed to connect to the server and the database.

String driver is assigned the following path “net.sourceforge.jtdc.jdbc.driver”.

the connecting between the database with the server could be made by the following syntax.

String connstring=”jdbc:jtds:sqlserver://server_ip_address:1433/DBNAME;

Encrypt=false;instance=SQLEXPRESS;”;

String username:”xxxxxxxx”;

String password:”xxxxxx

7. Conclusion

As seen earlier the data leakage is the biggest issues in most of the institutions & industries. To overcome this issue traditional methods like watermarking (which is easy to hack) and different encryption algorithm are used. In spite of using all these methods for protecting the data, the data leakage could not be contained and the guilty agent is unidentified. As per the proposed system the guilty agent can be easily identified by an alert message to the mobile from the system server. Based on the survey the data will be lost for both the guilty agent and the third party. In the future this idea could be implemented for the better containment of the data.

8. References

1. Krejar,o.;Janckulik,D.;Motalova,L.;Computer Engineering And Application"Optimal Data Artifact Determination For Mobile SQL Serever"Volume 1,2010
2. Umamaheswari .S, Geetha,H.A Dept. Of Comput. Sci., Coimbatore Inst. of Eng. & Technol.; Tamilndau, Coimbatore, India. "Detecting guilty agent".
3. Sandip A. Kale 1, Prof. S.V.Kulkarni2, Department Of CSE, MIT College of Engg, Aurangabad, Dr.B.A.M.University, Aurangabad (M.S), India1,2." Data Leakage Detection". Vol. 1, Issue 9, November 2012
4. Rudragouda G Patil,Dept of CSE,The Oxford College of Engg, Bangalore." Development of Data leakage Detection Using Data Allocation Strategies".
5. Unnati Kavali, Tejal Abhang, Mr. Vaibhav Narawade "DATA ALLOCATION STRATEGIES IN DATA LEAKAGE DETECTION".Vol. 2, Issue 2,Mar-Apr 2012
6. Panagiotis Papadimitriou, Student Member, IEEE, and Hector Garcia-Molina, Member, IEEE ." Data Leakage Detection". VOL. 23, NO. 1, JANUARY 2011
7. Detection Sridhar Gade1, Kiran Kumar Munde2, Krishnaiah.R.V.3 1Department of CSE, DRK Institute of Science & Technology, Ranga Reddy, Andhra Pradesh, India."Data Allocation Strategies for Leakage "
8. Mr. V.Malsoru, Naresh Bollam "REVIEW ON DATA LEAKAGE DETECTION"
9. Ming Li Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE."Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption"
10. Rohit Pol, Vishwajeet Thakur, Ruturaj Bhise, Prof. Akash Kate "Data leakage Detection"