ABSTRACT

In the virtual and widely distributed network, the process of handing over sensitive data from the distributor to the trusted thirdparties always transpires customarily in this modern world. The company's information security depends on workers by learning the rules through training and building sessions. Sometimes authentication of data may go beyond employee knowledge and cover the following areas such as physical and logical security that is change d to fit the ne e ds of the company .It needs an up to date recorded system. To make the transaction secure, sanctioning only approved users to access sensitive data through access control policies will avert data leakage. Humans are concerned more about privacy. To safeguard the data watermarking technology can be used. Watermarking is about embedding the details so that the leaker can be detected by decoding the images or files. A idea has been proposed using data allocation strategies which increases the probability of finding the leakages.

EXISTING SYSTEM:

Traditionally, leakage detection is handled by watermarking, e.g., a unique code is embedded in each distributed copy. If that copy is later discovered in the hands of an unauthorized party, the leaker can be identified. Watermarks can be very useful in some cases, but again, involve some modification of the original data. Furthermore, watermarks can sometimes be destroyed if the data recipient is malicious. E.g. A hospital may give patient records to researchers who will devise new treatments. Similarly, a company may have partnerships with other companies that require sharing customer data. Another enterprise may outsource its data processing, so data must be given to various other companies. We call the owner of the data the distributor and the supposedly trusted third parties the agents.

Proposed System:

Our goal is to detect when the distributor's sensitive data has been leaked by agents, and if possible to identify the agent that leaked the data. Perturbation is a very useful technique where the data is modified and made "less sensitive" before being handed to agents. We develops *unobtrusive* techniques for detecting leakage of a set of objects or records.

Proposed Modules:

1. Data Distributor
   - Login
   - Send file to agent
   - View sent files
   - View Leaked file details

2. Agent/User
   - Register
   - Login
   - Send files
   - View distributor files
   - Download file

Software Requirements

Operating System	:	Windows XP/2003 or Linux/Solaris
User Interface	:	HTML, CSS
Client-side Scripting	:	JavaScript
Programming Language	:	Java(JDBC, Servlets, JSP)
IDE/Workbench	:	Eclipse with My Eclipse Plug-in
Database	:	MySQL
Web Server	:	Apache Tomcat 7.0
Technology	:	JDK 1.7

Hardware Requirements

Processor	:	Pentium IV
Hard Disk	:	40GB
RAM	:	256MB

Mini Project Coordinator **Internal Guide**