**Data leak Detection in Networks**

**Abstract**

Statistics from security firms, research institutions and government organizations show that the numbers of data-leak instances have grown rapidly in recent years. Among various data-leak cases, human mistakes are one of the main causes of data loss. Data leakage is the big challenge in front of the industries & different institutes. Though there are number of systems designed for the data security by using different encryption algorithms, there is a big issue of the integrity of the user s of those systems. It is very hard for any system administrator to trace out the data leaker among the system users. It creates a lot many ethical issues in the working environment of the office.

**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**

The aim of this project is to detect users who have leaked the data of an organization to some other party and to detect when the distributor’s sensitive data has been leaked by users. This system will provide more amounts of hackers who are part of the data leakage and take serious actions against them. In this proposed system, there are different techniques to find out the hackers for example by generating encrypted files and watermarking.

In a perfect world there would be no need to hand over sensitive data to agents that may unknowingly or maliciously leak it. And even if we had to hand over sensitive data, in a perfect world we could watermark each object so that we could trace its origins with absolute certainty.

There are four modules:

1. Admin
2. Agent
3. Users
4. Network operator