IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: http://ijdacr.com (Volume 4, Issue 2, September 2015)

Leaker Detection In Open Network [LDION]

Remya .G .Nair
Department of Computer Science and Engineering
Cochin University of Science and Technology
Kottayam , India
nair0869@gmail.com

Mrs. Jyothis Joseph
Department of Computer Science and Engineering
Cochin University of Science and Technology
Kottayam , India
jyothisjoseph@rediffmail.com

Abstract—nowadays leakage of data is common to Industries, academic and Government Offices. Data must be shared for social purpose, research purposes and for business purposes. Data is shared among different enterprises or agents. Once the private data is shared it is not guaranteed that the data will not leak. If leakage happens it will be loss to firms. So we can detect the leaker for avoiding the loss thus occurred and thus avoid business with that agent. Leakage of data happening nowadays also but some firms will not tell their loss because of fear of loss of respect and other matters. Some companies distribute their data to trusted third parties. When Data distributers (Companies) found their some of the data in the web or somebody's laptop that is in unauthorized place. The distributor understands that the leaked data came from one or more agents. Our goal is to detect which agent leaks that data and provide the security to that data. When the distributor's sensitive data have been leaked by agents, and to identify the agent that leaked the data. We propose data allocation strategies (across the agents) that improve the probability of identifying leakages. These methods do not rely on alterations of the released data (e.g., watermarks).The Main Aim of the system can be given as follows:- Identify data leakages from distributed data using some data allocation strategies and find out the fake agent who leak that data.

In this work, we present a generic data lineage framework for data flow across multiple entities that take two characteristic, principal roles (i.e., owner and consumer). We define the exact security guarantees required by such a data lineage mechanism toward identification of a guilty entity, and identify the simplifying non-repudiation and honesty assumptions. With this model we assign a clearly defined role to each involved party and define the inter-relationships between these roles. There are three different roles in LDION: data owner, data consumer and auditor. The data owner is responsible for the management of documents and the consumer receives documents and can carry out some task using them. The auditor is not involved in the transfer of documents, he is only invoked when a leakage occurs and then performs all steps that are necessary to identify the leaker thus provide confidentiality. Whenever a document is transferred to a consumer, the sender embeds information that uniquely identifies the recipient. We call this is as fingerprinting which is cryptographically stored in the document without altering any property of the document. If the consumer or agent leaks this document, it is possible to identify him with the help of the embedded information. A key position in LDION is taken by the auditor. He is invoked by an owner and provided with the leaked data. If the leaked data was transferred using our model, there is identifying information embedded for each consumer who received it. Using this information the auditor can create an ordered chain of consumers who received the document. We call this chain the lineage of the leaked document. The last consumer in the lineage is the leaker. In the process of creating the lineage each consumer can reveal new embedded information to the auditor to point to the next consumer – and to prove his own innocence.