Chapter 14


Reena Singh  
Manipal Institute of Technology, India

Hemant Jalota  
DeepR Analytics, Canada

ABSTRACT

Data objects having low value like insurance or data-entry forms are shared between a client and rural business process outsourcing (RBPO) organisations for tasks like translation, proofreading, and data entry. These data objects are first decomposed into smaller parts and then assigned to RBPO users. Each user in a RBPO has access to only a few parts of a complete data object which he can leak to unauthorised users. But since the value of these parts is low, there is not enough incentive for the user to leak them. Such scenarios need good-enough security models that can provide reasonable security to an aggregate number of parts of low value data objects. In this chapter, the authors study the secure data assignment and leakage in RBPO by modeling it in the form of an optimisation problem. They discuss different scenarios of object decomposition and sharing, penalty assignment, and data leakage in the context of RBPO. They use LINGO toolbox to run their model and present insights.

INTRODUCTION

Information assets such as documents, audios, or videos are often shared between users. Scenarios where data sharing is across independent organizations make the issue of preventing data leakage more challenging. In recent years, an increasing number of data security breaches have surfaced. These events can not only have legal implications but also affect the brand image or business of an organization (Coopers, 2008). Thus organizations need to have a mechanism in place to prevent exposure of shared data to unauthorized users. Furthermore, recent studies have shown that internal employees of an organization

DOI: 10.4018/978-1-5225-4053-3.ch014
can also contribute to major security breaches. Many security professionals consider insider threats as an important challenge and better organizational policies and resources are needed for their management (Insider Attacks Industry Survey, 2017).

A resource may be shared by a group of people, with each person allowed access only to a part of the complete resource. For example, a user may be allowed access to only one section of a book. Restricting user access to a part of one complete resource helps in maintaining its security. The “need to know” principle restricts user access to only those resources (or their parts) which are necessary to carry out her responsibilities (Samarati, 1994). One way to achieve this is through a process of data distribution where each resource is decomposed into parts and distributed to the users, with each user getting access to one or more of these parts, based on the assigned task and the underlying security policy. This way of sharing data to business partners after decomposition is practiced by the Rural Business Process Outsourcing (RBPO) industry (Reena Singh, 2011).

In the recent years, there has been an increased awareness in India regarding the use of Information and Communication Technology (ICT) to promote socio-economic development of the rural population (Slaymaker, 2002). The RBPO industry in India has grown from USD 1.6 billion to USD 14.7 billion over a decade and this trend is expected to continue in the years to come (DSCI-KPMG, 2010). Some of the factors driving this rise of RBPOs in India are cost benefits from availability of cheap workforce, growing workload of repetitive tasks requiring simple skills, and increasing costs in cities (The stupendous rise of rural BPOs in India, 2016; Singh, 2010). A detailed description of RBPO is given by Singh et al. (Reena Singh, 2011; Gonsalves, 2015). For clarity, we are reproducing it in the next section.

**RBPO**

Data and distribution is integral to the RBPO scenarios. The data includes documents, scanned images, associated audio files, videos etc. We refer to individual resources as data objects in the rest of the paper and use the terms resource, assets and data objects interchangeably. RBPOs distribute tasks across agents in different rural service delivery centres. The back offices of RBPO are distributed in several locations. RBPO organizations get orders from clients to perform tasks like data-entry, translation, proof-reading etc. They handle a large number of data objects (of reasonable sizes) on a daily basis. An RBPO organization has many small centres distributed in several locations and is organised hierarchically with a head office, a few regional offices and many local offices. The local office has a kiosk centre in a village or a cluster of villages, with computing and Internet facilities, shared by the operators to carry out the tasks assigned to them (Vaidyanathan, 2009).

A good-enough security measure adopted by RBPO is decomposing a data object into smaller parts before sharing with users (Reena Singh, 2011; Gonsalves, 2015). Sharing objects after decomposition has two benefits:

- Each part (or a set of parts) can be assigned to different users to carry out some task on it, independent from other users. Thus it decreases the total time required for task completion as many users can simultaneously work on different parts of the same data object.
- Each user has access to only a part (or a set of parts) of a data object. Thus, the overall object security is maintained.