Chapter 25
A Novel Multi-Secret Sharing Approach for Secure Data Warehousing and On-Line Analysis Processing in the Cloud

Varunya Attasena
Université de Lyon, France

Nouria Harbi
Université de Lyon, France

Jérôme Darmont
Université de Lyon, France

ABSTRACT

Cloud computing helps reduce costs, increase business agility and deploy solutions with a high return on investment for many types of applications, including data warehouses and on-line analytical processing. However, storing and transferring sensitive data into the cloud raises legitimate security concerns. In this paper, the authors propose a new multi-secret sharing approach for deploying data warehouses in the cloud and allowing on-line analysis processing, while enforcing data privacy, integrity and availability. The authors first validate the relevance of their approach theoretically and then experimentally with both a simple random dataset and the Star Schema Benchmark. The authors also demonstrate its superiority to related methods.

1. INTRODUCTION

Business intelligence (BI) has been an ever-growing trend for more than twenty years, but the recent advent of cloud computing now allows deploying data analytics even more easily. While building a traditional BI system typically necessitates an important initial investment, with the cloud pay-as-you-

DOI: 10.4018/978-1-5225-8176-5.ch025

go model, users can punctually devote small amounts of resources in return for a one-time advantage. This trend is currently supported by numerous “BI as a service” offerings, with high economic stakes.

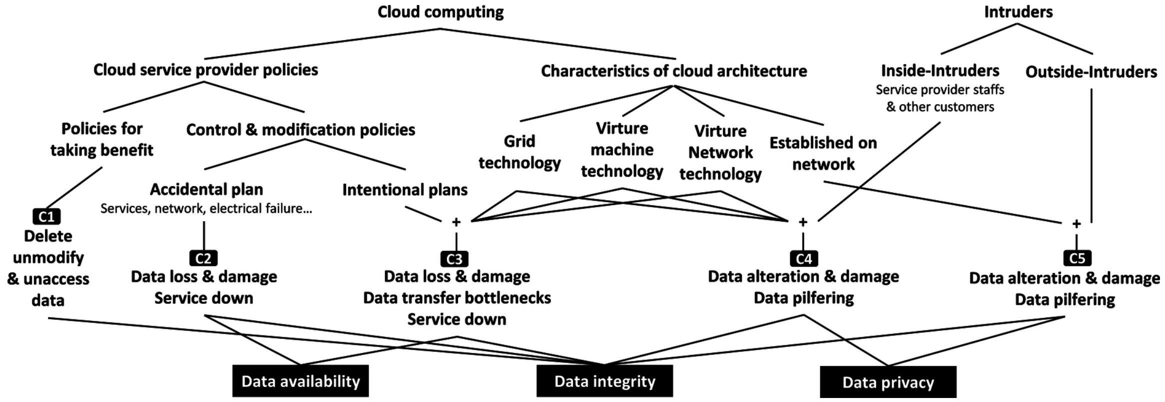
Although cloud computing is currently booming, data security remains a top concern for cloud users and would-be users. Some security issues are inherited from classical distributed architectures, e.g., authentication, network attacks and vulnerability exploitation, but some directly relate to the new framework of the cloud, e.g., cloud service provider or subcontractor espionage, cost-effective defense of availability and uncontrolled mashups (Chow et al., 2009). In the context of cloud BI, privacy is of critical importance. Security issues are currently handled by cloud service providers (CSPs). But with the multiplication of CSPs and subcontractors in many countries, intricate legal issues arise, as well as another fundamental issue: *trust*. Telling whether trust should be placed in CSPs falls back onto end-users, with the implied costs.

Critical security concerns in (especially public) cloud storage are depicted in Figure 1. User data might be deleted, lost or damaged. First, some CSPs have the policy of taking the highest profit. Therefore, unmodified or unaccessed data may be deleted to serve other customers. Second, data loss may also be caused by accidental, e.g., electrical or network failure, or intentional plans, e.g., maintenance or system backup. Moreover, virtual cloud architectures might not be sufficiently safeguarded from inside attacks. Finally, all CSPs cannot guarantee 100% data availability, although some cloud businesses must run on a 7/24 basis. Thus, data privacy, availability and integrity are major issues in cloud data security.

Encrypting and replicating data can solve most of these issues, but existing solutions are greedy in resources such as data storage, memory, CPU and bandwidth. Moreover, cloud data warehouses (DWs) must be both highly protected and effectively refreshed and analyzed through on-line analysis processing (OLAP). Thence, while CSPs must optimize service quality and profit, users seek to reduce storage and access costs within the pay-as-you-go paradigm. Thus, in cloud DWs, the tradeoff between data security and large-scale OLAP analysis poses a great challenge (Chow et al., 2009; Sion, 2007).

To address this challenge, we propose a global approach that relies on a new multi-secret sharing scheme, a family of encryption methods that enforce privacy and availability by design. Moreover, we incorporate in our approach features for data integrity verification and computation on shared data (or shares). Eventually, we minimize shared data volume. This paper expands (Attasena et al., 2013) along three axes. First, we complement the state of the art and deepen our analysis of related works. Second,

Figure 1. Cloud data security issues


Cloud computing
Intruders
Cloud service provider policies
Characteristics of cloud architecture
Inside-Intruders
Service provider staffs & other customers
Outside-Intruders
Policies for taking benefit
Control & modification policies
Grid technology
Virture machine technology
Virture Network technology
Established on network
Accidental plan
Services, network, electrical failure…
Intentional plans
+
+
+
C1
Delete unmodify & unaccess data
C2
Data loss & damage
Service down
C3
Data loss & damage
Data transfer bottlenecks
Service down
C4
Data alteration & damage
Data pilfering
C5
Data alteration & damage
Data pilfering
Data availability
Data integrity
Data privacy