Chapter 11
Secure System Model for Replicated DRTDBS

Pratik Shrivastava
Madan Mohan Malaviya University of Technology, India

Udai Shanker
Madan Mohan Malaviya University of Technology, India

ABSTRACT

Security in replicated distributed real time database system (RDRTDBS) is still explorative and, despite an increase in real-time applications, many issues and challenges remain in designing a more secure system model. However, very little research has been reported for maintaining security, timeliness, and mutual consistency. This chapter proposes the secure system model for RDRTDBS which secures the system from malicious attack. To prevent the request/response from malicious attack, authors have extended the system model with a cryptographic algorithm. In the cryptographic algorithm, a key must be secretly known only to the sender and receiver. Thus, in this chapter, authors have used the key generation algorithm to generate a key using an image. This secure system model maintains the confidentiality of the replicated data item and preserves its data integrity. It performs better in terms of malicious attack compared to other non-secure system models.

DOI: 10.4018/978-1-7998-0373-7.ch011

INTRODUCTION

The confluence of real time systems, communication network, and database systems is creating a real time database system (RTDBSs). Real time application processing in such an RTDBSs requires timely completion of real time transaction (RTT) such that temporal consistency of real time data item can be maintained. Failing to meet such a demand of real time data item cause heavy economic loss. Thus, the primary focus of RTDBSs is timeliness irrespective of logical consistency. Recently, the demand of RTDBS is expanding rapidly, a large number of real time applications such as stock management system, banking system, business information system, and air traffic control system generates a massive amount of data. A distributed real time database system (DRTDBS) has been specifically designed to satisfy the timeliness demand of RTT such that temporal consistency of such huge amount of data can be maintained. However, due to distributed processing of RTT and following strict consistency criteria has resulted in an increased research effort in this area. The research area includes concurrency control protocol (CCP), commit protocol (CP), replication technique (RT) and buffer management (BM) to maximize majority of RTTs to get successfully complete within their deadline. RT in DRTDBS is usually used to increase the performance of the system in terms of scalability, reliability, availability, and fault-tolerance.

In RDRTDBS, the main concern is to maintain the mutual consistency between data replicas despite a malicious attack from unauthorized users and compromised replicas (Zhao, 2014). This is accomplished via totally ordering the request deterministically, and simultaneously propagating this request to all the master sites or slave sites (Zhang, 2011). Replication protocol (RPL) (i.e. replica concurrency protocol or replica control technique) is used to maintain the mutual consistency between data replica present in such a master sites or slave sites. Existing research has been conducted mainly on designing an effective and efficient RPL (Gustavsson, et al., 2004; Gustavsson, et al., 2005; Haj, et al., 2008; Kim, 1996; Mathiason et al., 2007; Peddi & DiPippo., 2002; Salem et al., 2016; Shrivastava & Shanker, 2018; Shrivastava & Shanker, 2018; Shrivastava & Shanker, 2019; Shrivastava & Shanker, 2018; Son & Kouloumbis, 1993; Son & Zhang, 1995; Son et al., 1996; Syberfeldt, 2007; Xiong et al., 2002). Additionally, these RPLs were following different correctness criteria such that one copy serializability (1SR) or weaker than 1SR can be satisfied (Ouzzani et al., 2009).

Although existing work (Gustavsson et al., 2004; Gustavsson et al. 2005; Haj et al., 2008; Kim, 1996; Mathiason et al., 2007; Peddi & DiPippo, 2002; Salem et al., 2016; Shrivastava & Shanker, 2018; Shrivastava & Shanker, 2018; Shrivastava

A Survey on Applied Cryptography in Secure Mobile Ad Hoc Networks and Wireless Sensor Networks

Jianmin Chenand Jie Wu (2010). *Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice (pp. 262-289).*
www.irma-international.org/chapter/survey-applied-cryptography-secure-mobile/41119