Chapter 13
Intelligent Techniques for Providing Effective Security to Cloud Databases

Ar Arunarani
Anna University, India

D Manjula Perkinian
Anna University, India

ABSTRACT

Cloud databases have been used in a spate of web-based applications in recent years owing to their capacity to store big data efficiently. In such a scenario, access control techniques implemented in relational databases are so modified as to suit cloud databases. The querying features of cloud databases are designed with facilities to retrieve encrypted data. The performance with respect to retrieval and security needs further improvements to ensure a secured retrieval process. In order to provide an efficient secured retrieval mechanism, a rule- and agent-based intelligent secured retrieval model has been proposed in this paper that analyzes the user, query and contents to be retrieved so as to effect rapid retrieval with decryption from the cloud databases. The major advantage of this retrieval model is in terms of its improved query response time and enhanced security of the storage and retrieval system. From the experiments conducted in this work, proposed model increased storage and access time and, in addition, intensified the security of the data stored in cloud databases.

INTRODUCTION

Cloud databases have provided efficient storage and retrieval services to cloud users in recent years. In such a scenario, the use of cloud databases to store transactions as well as machine-generated big data pertaining to organizations is gaining traction. Owing to the volume of growth, security attacks on cloud databases have also proliferated, culminating in a need for encrypted storage in cloud databases. In the past, researchers proposed new methods to retrieve encrypted data from relational databases. However,

DOI: 10.4018/978-1-5225-8176-5.ch013

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

retrieving encrypted data from cloud databases was not considered an important research challenge. In recent years, the volume of data stored in cloud databases has multiplied considerably, and big data analytic techniques are applied on such data to ascertain interesting patterns that can help organizations in decision making.

Storage structures used in relational databases, including the B-Tree and related indexing techniques, are unsuited to the storage and retrieval of cloud databases. A cloud database stores data in the form of key and value pairs in which the value can be represented as a vector so it is possible to provide a mapping between relational databases and the Not Only SQL (NoSQL) format of cloud databases. In relational databases, users are grouped into database administrators, application programmers, query language users and end users. Each is given a set of privileges that include the right to write, read, update, delete and insert records. Database administrators are provided the highest privileges and end users the least. The chief difference between transactions in relational databases and cloud databases is that the former insists on atomicity, consistency, isolation and durability (ACID) properties, while the latter insist on BASE properties.

Big data analytics and cloud databases are two major areas of research popular among researchers in the area of cloud computing. Big data grows at enormous speed with respect to velocity, variety and volume. Therefore, tackling the challenges of the growing quanta of data with respect to secured storage and retrieval is a key task to be undertaken so big data can be stored safely in cloud databases and retrieved just as easily. The existing query languages for relational databases provide only a facility to retrieve records which are not encrypted. Certain recent works attempted to provide a facility to retrieve encrypted data from relational databases through a query language in which new keywords were introduced to enhance the SELECT statement feature of the Structured Query Language (SQL). Moreover, the GRANT and REVOKE commands of the SQL have been used to perform access control in relational databases. However, cloud databases lack such facilities and hence secured storage and retrieval call for greater attention.

In this paper, a new querying model based on a query generator through a user interface which provides an integrated feature for storage and retrieval, along with access control techniques to store data in an encrypted form and retrieve them in a decrypted form, is proposed. The query generator allows for query creation through a user interface in which database objects and user requirements can be specified either using English words or SQL queries. These queries, converted by the proposed system into cloud database queries, are executed by the cloud databases themselves. Validation is provided by the system, during database creation and insertion of new records, through the use of rules. Given that the rules systems validate tasks, the cloud database manager is relieved of the business of verifying integrity and security. In addition, authentication is carried out based on user credentials and queries. Intelligent agents are deployed in each cloud network site so the distributed cloud database system is able to coordinate and perform storage and retrieval operations - in encrypted form for storage and decrypted form for retrieval - with different types of cryptographic algorithms used for the effectual encryption of data. In this model, the Caesar cipher is used to store ordinary data, while the Advanced Encryption Standard (AES)-based encryption is used to store and retrieve valuable user data and, finally, the RSA algorithm is utilized to store the confidential data that can be accessed only by managers. The primary advantage of the proposed model is that it classifies users, data and queries suitably by applying rules and makes intelligent decisions with respect to fast and secured storage and retrieval.

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/intelligent-techniques-for-providing-effective-security-to-cloud-databases/224578

Related Content

Privacy Preserving Public Auditing in Cloud: Literature Review
Thangavel M., Varalakshmi P., Sridhar S.and Sindhuja R. (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications (pp. 2059-2083).*
www.irma-international.org/chapter/privacy-preserving-public-auditing-in-cloud-literature-review/224670

A Comprehensive Survey on Trust Issue and Its Deployed Models in Computing Environment
Shivani Jaswaland Gurpreet Singh (2018). *Critical Research on Scalability and Security Issues in Virtual Cloud Environments (pp. 150-166).*
www.irma-international.org/chapter/a-comprehensive-survey-on-trust-issue-and-its-deployed-models-in-computing-environment/195346

Evolution of Fog Computing Applications, Opportunities, and Challenges: A Systematic Review
Hewan Shrestha, Puviyarai T., Sana Sodanapalliand Chandramohan Dhasarathan (2021). *International Journal of Fog Computing (pp. 1-17).*
www.irma-international.org/article/evolution-of-fog-computing-applications-opportunities-and-challenges/284861

Analyzing the Efficacy of Machine Learning Algorithms on Intrusion Detection Systems
Swanand Arun Yamgarand Bhuvaneswari Amma N. G. (2024). *Emerging Technologies for Securing the Cloud and IoT (pp. 196-213).*
www.irma-international.org/chapter/analyzing-the-efficacy-of-machine-learning-algorithms-on-intrusion-detection-systems/343336

An Insight Into Openstack
Srinivasa K. G.and Vikram Santhosh (2018). *Design and Use of Virtualization Technology in Cloud Computing (pp. 243-259).*
www.irma-international.org/chapter/an-insight-into-openstack/188132