International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

An Effective Design for Secure Data Storage and Access Model for Temporal Cloud Databases

K . Naga Maha Lakshmi
Assistant Professor, AAR Mahaveer Engineering College, Vyasapuri, Bandlaguda, Keshavgiri, Hyderabad, TelanganaIndia.

Abstract: - *Cloud databases are responsible for services for large scale data storage and retrieval of disseminated data. Though, the existing access control methods provided in database systems for preserving security are not satisfactory to secure the sensitive data stored in public cloud databases. In this paper, a novel protected data storage algorithm for genuine privacy preservation of personal data is proposed. To achieve storage and retrieval setups of data in the cloud data storage effectively, Cloud Map-reduce algorithms are developed in this work which performs data reduction and fast processing. In order to consider the temporal nature of documents to be retrieved, I propose a novel algorithm called Spatiotemporal Secured Cloud Map Reduced Algorithm which integrates temporal constraints with map reduce algorithms which are proposed newly in this work. The proposed algorithm leads reduce the processing time and preserve security effectively.*

Keywords: Cloud computing Temporal secured Map reduces.

1. Introduction

Cloud computing is a primitive technology plays vital role in every sector, this paper proposes a new client based security mechanism based on encryption of data to enhance the security. As clients store huge amount of data in the cloud, map reduce concept becomes the leading platform which has the flawless ability to scale-out the required client's data from the large network of machines in which the data of huge number of clients are stored. Moreover, Cloud databases enable the users to store their data in cloud servers and hence reduce the burden of local hardware and software. By this service, the users surrender their responsibility of holding their data in local databases and hence leading to new security provisions. Since map reduce provides virtualization on servers to provide multi-tenancy, it maps every node of a map reduce cluster to a virtual machine. The map reduce programs are virtually stored in every participating node which are controlled by the server. A cloud databases system consists of a group of storage servers in order to provide continuing data storage and retrieval services over the Internet. In this paper, new security features are proposed by introducing encryption of data before they are stored. The system performance is enhanced using the map reduce procedure.

The map reduce pattern is used in this work to reduce the energy consumption in cloud data storage. The runtime of a map reduce work is depending on input data size and the degree of concurrency in used in transaction processing. Moreover, the concurrency can be optimized through parallel query processing. This work uses map reduce techniques combined with temporal constraints to improve the query processing performance. Data distribution is an important functionality in cloud data storage system. In this work, we propose new techniques to securely, efficiently, and flexibly split data with others in cloud data storage. This is achieved by applying fragmentations with spatial and temporal constraints. In addition, the fragments are encrypted using a chain Hill Cipher in which the cipher text of each is used as the key to encrypt to the next block. The original key is used to encrypt only the first block of data.

2. Literature Survey

There are many existing works that discuss about data structures and algorithms for secure cloud temporal data storage (Nandlal L Sarda 1993, Abdullah UzTansel 1997, Sethukkarasi et al. 2014, Claudio et al. 1998, Burak et al. 2012). Among them, Wang et al. (2014), proposed a new scheduling

algorithm which uses weighted routing in a typical optical cloud infrastructure. In their model, energy optimization is performed at the network Level. In such scenario, energy efficiency is achieved to some extent. However, most online applications need to optimize the energy further. However, the storage and retrieval needs fast and secure algorithms.

Few works on role based access control discuss about techniques for efficient Usage of rules in cloud network. TanerCevik et al. (2012), proposed a power aware routing protocol which considers nodes with higher energy and also the shortest path for performing effective routing. Few works on temporal databases discuss about techniques for efficient storage and retrieval of temporal data from temporal databases. Tim Schlüter et al. (2010), proposed a temporal association rule mining algorithm in which the authors extended the existing apriori algorithm with time stamps and they proposed to temporal tree structures to perform effective rule mining. Chun-Hao Chen et al. (2011), proposed a fuzzy temporal rule mining algorithm in which they used membership functions for performing association rule mining with temporal decisions.

In this work, two new algorithms namely a temporal-B-tree data structures with manipulation algorithm and a new temporal query processing algorithm are proposed which uses temporal constraints for fast retrieval with minimum energy and higher security.

3. System Design

The architecture of the system proposed in this thesis is depicts in Figure 3.1 which consists of eight components namely Client/User Interface, Cloud Server Manager, Map Reduce Technique, Security Module, Authentication Module, Constraint Manager, Scheduler, Temporal Information Manager, Rule Base, Cloud Data and Knowledge Base. This system is used to stored the cloud data securely and to perform effective retrieval and retrieve data in a secure manner from the Cloud Server.

3.1 User Interface:

The user interface communicates to the cloud temporal database through cloud server. In this model, user interaction is performed through the user interface. It accepts user queries and validates them using a validation agent. Queries from normal users are identified by the user interface On the other hand, queries from malicious users are identified by the cloud databases manager and sent to the temporal information manager and constraint manager where they check the key provided to them and they are filtered and dropped if the key is not matched.

3.2 Cloud Database Server

A cloud database server is used in this work to support data storage and manipulation operations. The cloud database server receives queries from the user interface and passes them to the otherconstraint manager and temporal information manager for key verification if the user‘s history is doubted. Such users are subjected to checks based on temporal constraints, identity constraints and the status level of the user before accessing cloud database.

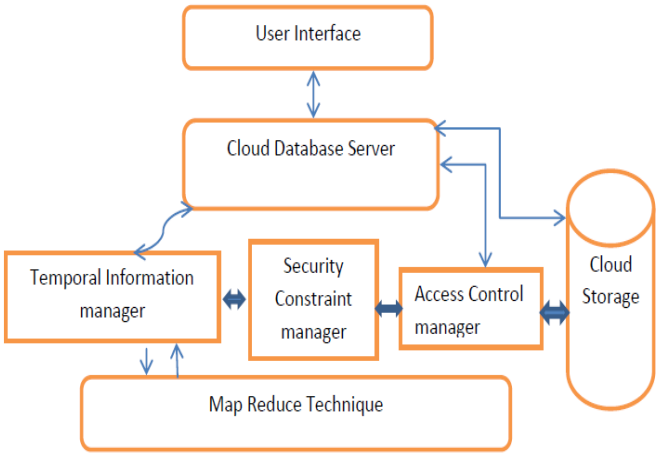

Figure 1. System architecture

3.3 Temporal Information Manager

The temporal manager is mainly responsible for managing temporal constraints and rules and to provide information about user access pattern on the cloud database during the time interval at which they are trying for data access. This manager consults rule manager and temporal information manager to assign suitable roles depending on the user requirements and status. Moreover, it uses roles from role base to decide on user role assignment and is responsible to provide various privileges to the users on tables.

3.4 Security Constraint managers

The responsibility of power constraint manager is to check the access pattern of the user in the past and the time duration for each access using temporal constraints. The rule base is used by the power constraint manager which has a collection of active and passive rules and event details. Active rules are automatically fired in response to abnormal events under the conditions defined. The power constraint manager is responsible not only for power management but also for role management activities including inserting, deleting and updating rules based on agent's feedback.

3.5 Map Reduce Technique

This component uses a new algorithm called Spatiotemporal Secured Cloud Map Reduced Algorithm (STSCMRA) for improving the performance. It is responsible for assigning and manipulating the roles periodically by considering temporal constraints in order to enhance the security. It is also responsible for temporal sorting, temporal searching and indexing, temporal classification and temporal joining which performs access control based on temporal constraints.

3.6 Cloud Database

Cloud database is connected to cloud server for storing data. In this work, the cloud database is used to store data in the form of structured, semi structured and un-structured data structures. It uses not only Structured Query Language format but also the other data structures. The cloud data is arranged in cloud data centers with identities for servers, racks, clusters, data bases and files. It can be processed effectively using map reduce functions.

4. Spatiotemporal Secured Cloud Map Reduced Algorithm

In this work, a new algorithm called Spatiotemporal Secured Cloud Map Reduced Algorithm (STSCMRA) has been proposed for improving the performance. This algorithm has been implemented to assign and manipulate roles periodically by considering temporal constraints in order to enhance the security. The proposed STSCMRA consists of three phases namely temporal sorting, temporal searching and indexing, temporal classification and temporal joining which performs access control based on temporal constraints.

4.1 Spatiotemporal Sorting

In this phase, there are n numbers of clients submitting requests to the model. Here the sorting process takes place. The inputs are a set of files which has one line assigned as one value which is used for the purpose of temporal sorting within a particular time limit (t1, t2). There are two values given to the system namely the map function key and the map value.

4.2 Temporal Searching and Indexing

In this phase, the inputs are a set of documents which are used for the purpose of temporal searching within a particular time limit (t1, t2). In this temporal time attributes also form part of the search key provided in the map reduce function. Consider F as the file name, T as the input text, P as the search pattern, M as the mapper and R as the reducer. We use the following function M = (F,T)P and if this is true then write a output file output (F, T). After the completion, the reducer is used to identify the function. Then next indexing phase consider PN as the page name, W as the word, PT as page text and V as the value. The mapper and the reducer functions are given respectively. The mapper mapping the page and text using mapping function M (PN, PT). In this algorithm for each W in PT, then do the function emit intermediate (W, PN). Finally, the results are obtained in map reducer sorting phase.

4.3 Temporal Classification

After the completion of temporal searching and indexing, the files are transferred to the temporal classification. The output files from the temporal Searching and indexing containing the Bayesian classification instances are sent to the mappers. The function M (F,I) where I is considered to be the instance is used in the Bayesian classification within the time interval of (t1, t2).

4.4 Temporal Joining Temporal joining works like nature join operator using the outputs map reduce function. However, the join condition must have a temporal component. The proposed temporal cloud chain Hill Cipher algorithm is explained in the next section.

5. Conclusions

In this paper, a novel Spatiotemporal Secured Cloud Map Reduce Algorithms has been proposed for effective cloud data storage and retrieval. In addition, temporal constraints are proposed using rules and intelligent agents in this work in order to enhance the security of the cloud database system. This system reduces the query processing time using map reduce functions. The proposed security and storage system was tested with real implementation with a private cloud data center. The performance analysis carried in this work proved that the algorithm proposed in this paper provides more security and consumes less energy. Further works in this area can be the use of a trust computation model for further enhanced in security model.

References

1. Muthurajkumar, S., Vijayalakshmi, M. &Kannan, A. Wireless PersCommun (2017) 96: 5621.
2. Wang, Q., Wang, C., Ren, K., Lou, W., Li, J., et al. (2011). Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 22, 847–859.
3. Wang, C., Wang, Q., Ren, K., Cao, N., Lou, W., et al. (2012). Toward secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing, 5, 220–232.
4. Lin, H. Y., Tzeng, W. G., et al. (2012). A secure erasure code-based cloud storage system with secure data forwarding.IEEE Transactions on Parallel and Distributed Systems, 23, 995–1003.
5. Bahga, A., Madisetti, V. K., et al. (2012). Analyzing massive machine maintenance data in a computing cloud. IEEE Transactions on Parallel and Distributed Systems, 23, 1831–1843.
6. Wang, C., Chow, S. S. M., Wang, Q., Ren, K., Lou, W., et al. (2013). Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers, 62, 362–375.
7. Zhu, Y., Hu, H., Ahn, G. J., Yu, M., et al. (2012). Cooperative provable data possession for integrity verification in multicloud storage. IEEE Transactions on Parallel and Distributed Systems, 23,2231–2244.
8. Tang, Y., Lee, P. P. C., Lui, J. C. S., Perlman, R., et al. (2012). Secure overlay cloud storage with access control and assured deletion. IEEE Transactions on Dependable and Secure Computing, 9, 903–916.
9. Yang, K., Jia, X., et al. (2013). An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 24, 1717–1726.
10. Wang, H. (2013). Proxy provable data possession in public clouds. IEEE Transactions on Services Computing, 6, 551–559.