Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7766286

A CONSTRAINT-BASED ACCESS CONTROL MODEL FOR OPTIMIZING POWER AND PERFORMANCE OF CLOUD STORAGE

Mirdula S[1*], Dr Roopa M[2]

[*1]Research Scholar, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai, India.

[2]Associate Professor, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai, India.

***Corresponding author: email:** ms1093@srmist.edu.in

Abstract

Background: Cloud databases allow for the storage and retrieval of large amounts of distributed data on a massive scale. This work proposes and implements new algorithms for cloud data storage that perform data lessening and rapid processing in order to effectively perform secure storage and retrieval operations. **Methods :** Deep Belief Network (DBN) incorporates with Map Reduce techniques has been used for the enhance the cloud-security. Auditing and signature verification techniques can also help improve security. **Findings :** An audit-based security mechanism that relies on the trust of third parties has been proposed in this research. To summarise, these algorithms improve security while also speeding up computation. Based on load distribution and balancing methods, a new algorithm has been proposed to optimise power and performance in cloud computing. Such environment is also characterised by a novel algorithm for optimising power and performance based on load distribution and balancing techniques. **Novelty :**The proposed storage and retrieval methods are effectively utilised by all of these algorithms, which improves data security while also speeding up processing.

Keywords: Round-Robin Algorithm, Scheduling algorithm, Cloud Security, Deep Belief Network.

1. Introduction

Cloud computing is available 24/7, users can access resources from any location at any time as long as they have an Internet connection. Using cloud computing, data storage and retrieval features have been significantly improved. Data can be stored and used by many clients from any location at any time with the use of a distributed backup system. The cloud system can provide highly reliable and high-fidelity services with effective storage and access methods. Numerous consumers want to save their private data in the cloud, which means that existing data storage and manipulation methods must be improved with new security measures. As a result, there are additional safety concerns that have not been addressed. As a result, enhanced security requires the development of new DBN cryptographic method for securing the data. The map lowering idea is the industry standard for scaling out needed details of client information from massive network and store such information in cloud Cloud users relinquish control of their data, which introduces additional security risks for the service. Each node in a Map Reduce cluster is mapped to a virtual server that hosts a simulated computer with multi-tenancy. Each participating node has virtual copies of the Map Reduce programmes that are controlled by the server.

2. Material and methods

It is proposed in this thesis that a secure cloud data storage model be used to store and secure data effectively. An overview of cloud data storage, retrieval security, and scheduling is presented in this sections.

According to [1], the SmartX Multisec framework employs a multi-tier security architecture to provide intuitive and systematic visibility into the security of edge cloud infrastructure across multiple locations Network topologies in multi-site edge clusters are abstracted by the SmartX Multi-Security software as several onion-ring-based layers of scalable physical, virtualized, and containerized cloud nodes. For monitoring, visualising, and filtering traffic from the various levels of an abstracted networking topology, this tool set also contains automated DevSecOps tools. It is the primary goal of [2] research to present current literature on sensor-cloud architecture security issues and preventive measures. Furthermore, a number of security attacks and their innovative solutions are presented from the sensor-architectural cloud's perspective.

There are a wide range of client-specific countermeasures that can be calculated by security administrators using the [3] approach. Experiments have shown that effective security solutions for cloud applications vary depending on the threats prioritised by various clients. Additionally, this approach is not restricted to cloud-based systems but can be applied to any networked system. In addition, a software tool has been created to assist in the implementation of this strategy.

This [4] proposes a possible flow sensitive security model for a federated cloud system that assigns security levels to clouds and entities. In the next section, we introduce the concept of cloud computing system opacity—a concept that describes the safety of data flow—and discuss various approaches to quantitative opacity analysis. It's possible to measure the opacity characteristics that correspond to the different resource allocation strategies in a cloud system and see how they affect information flow.

[5] a new access control scheme that allows access permissions to be delegated. Cloud data storage was made more secure through the application of rules and cryptography, according to the authors.[6] an active approach was presented with the goal of alleviating user operation pressure and eliminating data over-collection. Finally, the results of their experiment show that their framework is both feasible and advantageous. Using a privacy-preserving model for vertically partitioned databases to outsource frequent item sets mining. Using rules, they ensured the cloud mining results' privacy.[7] a new cloud-based access control module. A new multi-layer security model for cloud databases was introduced. They used a real cloud data centre to test their system and provide security recommendations. [8] a new two-factor data security protection model for cloud databases was proposed, in which data is encrypted using the identity of a recipient. The receiver uses a combination of private and public keys to encrypt and decrypt messages.

3. SYSTEM DESIGN

The framework proposed in this paper has eight components, as shown in Figure 1: Interface Model between the Client and User, a cloud server management system, a map reduction technique, Authentication block, and an authentication module. A constraint manager, a scheduler, a temporal information manager, a rule base, and a cloud data and

knowledge base are also included. The data on the Cloud Server can be safely stored and retrieved at any time using this system in an efficient and secure manner.

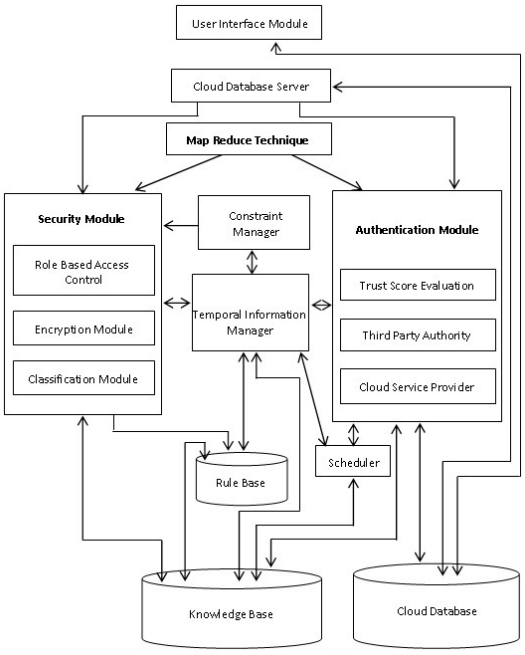

Figure 1 shows the Interface Model between the Client and User, a cloud server management system, a map reduction technique, Authentication block, and an authentication module.

3.1. SECURITIZED SCHEDULING METHODOLOGY

Performance optimization in a cloud computing environment aims to find the most efficient power allocation strategies for the server. Effective load balancing mechanisms in the cloud ensure an optimal workload. The core speed of a cloud computing platform is used to solve optimization problems. Either zero, a fixed speed, or an ever-changing rate are acceptable choices. In the cloud, terabytes of data can be stored and retrieved from a variety of automated sources. Many different types of cloud platforms exist, including public and private. However, private cloud computing is essential for most businesses. Thus, this research focuses on the improvement of cloud network security and power optimization techniques. There is a new scheduling DBN algorithm proposed in the paper as well, which aims to optimise both power consumption and scheduling.

3.2. ENERGY EFFICIENT SCHEDULING ALGORITHM (EESA)

Algorithms for improving performance have been proposed in this study using the Energy Efficient Scheduling Algorithm (EESA). Using this algorithm, roles are assigned and manipulated on a regular basis, taking into account the time constraints. Two mechanisms are included in the EESA Constraints: one with and one without temporal constraints.

There are n jobs submitted through the user interface and s servers available in cloud data storage centres that are considered in this phase. ' When a client has a task that needs to be completed, they send a request to the server. Due to aggregation, the total number of jobs is minimum than the number of servers in this phase. In this algorithm, x1, x2,... represent the n

clients, and y1, y2,... represent the m servers. The system's behaviour is defined by the formula f(x,y)=a0+a1x+a2x2+...

The +an xn. of order n. The most efficient way to use this function's energy is to find its maximum value in the interval [t1, t2].. As a final step, the values of local maxima are used to select a global maximum.

User interfacing is used to select a cloud data centre based on temporal considerations, thereby reducing the user's time complexity. As a result of that, the data center's power consumption is reduced as well. Using a one-to-one mapping between clients and servers, the cloud data centre can communicate with any one client at a time. The data centres are monitored by the temporal manager. Power consumption can be effectively reduced with the help of a nearby cloud data mapping. The proposed and existing algorithms are tested using Python programmes for effective analysis in this section. An overview of the time spent waiting for various parts of this paper is depicted in Table 1.

S.No	No of CPUs	RAM Size (MB)	HDD Size (GB)	EESA with Temporal Waiting Time(ms)	EESA without Temporal Waiting Time(ms)
1	2	512	10	5677	5687
2	5	1024	100	4694	4712
3	5	2048	1000	4109	4120
4	10	3072	2000	4080	4092
5	20	4096	4000	1630	1640

Table 1 shows Waiting times for various components with the comparison of with and without Temporal Waiting Time

EESA with a temporal algorithm takes less time to process than EESA without a temporal algorithm, as shown in Table 1 and the figure 2 shows the count of authorised persons throughput level that were permitted by the EESA model was lower than EESA without Temporal model. Additionally, 5% fewer users were denied access than under the previous system, indicating an increase in security. This is because the abnormal users are effectively checked using time constraints.

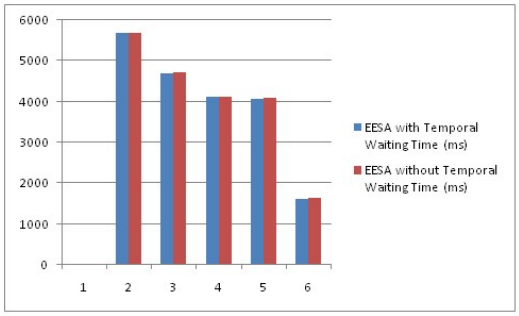

Figure 2 : Security level by number of users

3.3. DBN ALGORITHM

Power Restriction Algorithm for Temporary and Secured Use DBN is a new algorithm that has been proposed to improve the performance in this work Using this algorithm, roles are assigned and manipulated on a regular basis, taking into account the time constraints. IPCSRR (ITPCSRR) performs access control based on temporal constraints in the proposed algorithm, which categorized into three phases: the Temporal-Power-Constraint Checking (TPCC) with aggregate, TPCC without aggregate and the intelligent temporal power constraint satisfaction (ITPCSRR). Round-Robin Scheduling Algorithm for Intelligent TPCC

The Round-Robin Scheduling technique used in this algorithm enforces security constraints by applying intelligent DBN. There will be n jobs running in the user interface and m servers in the cloud data centre, so we'll use n and m as our starting points. Round-Robin Scheduling is used in this system to efficiently assign servers. ITPCSRR phase also supports M/M/C queuing system for optimal services. The following are the steps involved in this phase:

- ✓ Read m and n.
- ✓ Accept requests from the client.
- ✓ Perform the following for each of the n jobs:
- ✓ Use round robin scheduling to find out how many servers are available in the cloud data centre.
- ✓ Check to see if n > m is the case.
- ✓ Check the aggregation of the user interface and the one-to-one mapping can be done between clients and servers using a round robin scheduling mechanism.
- ✓ Perform temporal power constraint checking at the aggregate stage if you're using the user interface.
- ✓ Put a time constraint on the aggregate stage instead.
- ✓ Use the M/M/C queuing model to assign the system to round robin scheduling.
- ✓ Submit the requested information.

In this phase, the user interface selects data with aggregate mechanisms to minimize the complexity with respect to time of the processing of the user queries. This aggregation also reduces the power consumption in the data centre. A server is assigned to every client in this phase because of the M/C queuing model. Time constraints and logs are monitored by a temporal constraint manager. In spite of this, the data centre communicates with clients on a regular basis. This phase's primary benefit is the reduction in both time and energy required.

3.4. THE ANALYSIS OF EFFICIENCY

Eucalyptus noted to be a private type of the cloud has been used for this paper. The internet based DBN instantiations and protocols have been implemented in Python and windows for this purpose. The tests were performed on a Western-Digital 350 GB Serial ATA drive with a 7200 RPM Western Digital I5 processor frequency running at 2.4 GHz and utilize the memory 4 GB of RAM. Data auditing was used in this study to assess the system's performance. The simulation of the private cloud “Eucalyptus" has been installed for analysing CPU processor, memory, and disc utilities on both the user side as well as cloud service sides. Mainly Two cluster-level components have to be installed on the head node of one cluster. As a final step, each node with a supervisor was controlled by a Node Controller (NC). Tables are

used to explain the results of the experiments in this work. Round Robin and the DBN Algorithm are compared in Table 2 for the number of requests denied in five experiments, each with a different number of requests. 19:1 was the ratio of legitimate requests to malicious ones.

Exp.No	No of User Request Tried	No of requests denied by Round Robin	No of requests denied by DBN Model
Exp1	100	3	5
Exp2	200	6	9
Exp3	300	10	13
Exp4	400	13	17
Exp5	500	14	22

Table 2 : Number of round robin and temporal power limitation algorithm rejected user requests

Table 2 shows that the proposed DBN Algorithm model outperforms the Round Robin model when it comes to restricting access providers and providing more than 90% detection with accuracy prevention when compared to the Round Robin model. These powerful intelligent agents and password exchanging techniques are used in this model to make it possible.

Figure 3 shows the number of people who were allowed to use the DBN Round Robin Algorithm. This diagram shows that DBN Round Robin has a lower access permission than Round Robin Algorithm. 5 percent least amount of users were denied access in comparison to the previous model, so security and authenetication has been improved. This is because the abnormal users are effectively checked using time constraints.

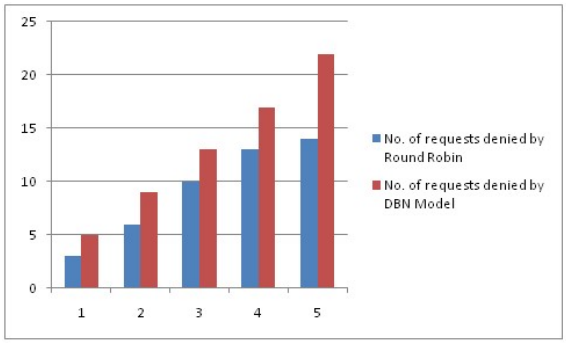

Figure 3: The number of data centres and the level of security they provide

Exp.No	No of User Request Tried	No of requests denied by Round Robin	No of requests denied by DBN Model
Exp1	100	7	8
Exp2	200	9	13
Exp3	300	12	20
Exp4	400	17	27
Exp5	500	21	34

Table 3: When identity and DBN are taken into account, the Round Robin model denies requests for access

For example, in Table 3, traditional Round Robin Scheduling Model and intelligent agent-based (TPCCRRM) Temporal Power Constraint Round Robin Model allow for a maximum of three user requests per time interval (t1, t2). In comparison to the Round Robin Scheduling Algorithm model, the total number of users who were restricting access decreased by 7% as a result of the implementation in this model. There are nine edges and seventy-one permissions for each of the ten roles, and it takes 3,384 milliseconds to assign 50 users to every role, according to the experiments conducted in this work. Each simple operation takes 68 to 120 milliseconds to complete. Time spent assigning 50 users with 10 roles is shown in Figure 4.

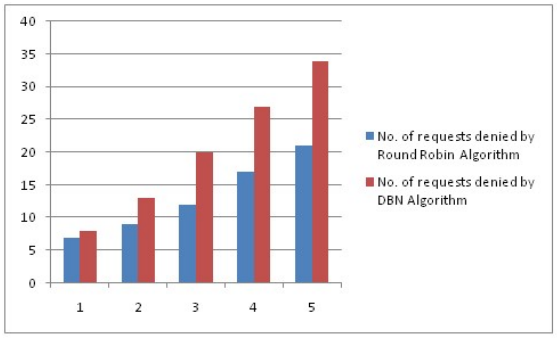

Figure 4: The maximum number of users allowed (t1, t2)

When using the Round-Robin algorithm with role-based access control or the (TPCC) Temporal Power Constraint Algorithm with Access Control, it is clear from Figure 4 that processing time is directly proportional to the size of the database. There are some advantages to using Round Robin with Access Control over Temporal Power Constraint.

4. CONCLUSION

A Constraint-Based Access Control Model has been presented for efficient power savings while maintaining safe data and cloud storage. Additionally, this work proposes a Temporal Constraints Model based on rules and intelligent agents that improvise the security of the using cloud based database system. The suggested security and storage system was validated in real-world testing in a private cloud data centre. It has been demonstrated that the

method suggested in this study is more secure and uses less energy than currently utilised algorithms. Using intelligent agents for distributed query coordination could be a future focus of this research. A trust computation model can be used in future work in this area to improve the security model even further. Rather than relying on third-party libraries and protocols to generate and transmit logs, future work will attempt to integrate log management directly into the system. Additional research will be done into secure key management techniques. To further enhance security, spatial constraints can be added in the future. A trust computation model can be used for future work in this area to improve the security model even further.

5. References:

1. J. -S. Shin and J. Kim, "SmartX Multi-Sec: A Visibility-Centric Multi-Tiered Security Framework for Multi-Site Cloud-Native Edge Clusters," in IEEE Access, 2021; 9(1): 134208-134222. Available from: https://doi:10.1109/ACCESS.2021.3115523.
2. R. Alturki et al., "Sensor-Cloud Architecture: A Taxonomy of Security Issues in Cloud-Assisted Sensor Networks," in IEEE Access, 2021; 9: 89344-89359. Available from: https://doi:10.1109/ACCESS.2021.3088225.
3. Armstrong Nhlabatsi et al., "Threat-Specific Security Risk Evaluation in the Cloud," in IEEE Transactions on Cloud Computing, 2021; 9(2): 793-806. Available from: https://doi:10.1109/TCC.2018.2883063.
4. Zeng and M. Koutny, "Quantitative Analysis of Opacity in Cloud Computing Systems," in IEEE Transactions on Cloud Computing, 2021; 9(3): 1210-1219. Available from: https://doi:10.26599/TST.2019.9010044.
5. W. Lei Zhang et.al., "Cryptographic Solutions for Cloud Storage and Challenges," in IEEE Transactions on service Computing, 2022; 15(1): 567-587. Available from: https://doi:10.1109/TSC.2019.2937764.
6. R. Ramkumar, M. V. Kumar and D. Sivamani, "Fuzzy Logic based Soft Switched Active Clamped Boost Converter Charging Strategy for Electric Vehicles," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020, pp. 1334-1339, doi: 10.1109/ICECA49313.2020.9297422
7. P. Bellavista, A. Corradi, A. Edmonds, L. Foschini, A. Zanni and T. M. Bohnert, "Elastic Provisioning of Stateful Telco Services in Mobile Cloud Networking," in IEEE Transactions on Services Computing, 2021; 14(3): 710-723. Available from: https://doi: 10.1109/TSC.2018.2826003.
8. S. Heidari and R. Buyya, "A Cost-Efficient Auto-Scaling Algorithm for Large-Scale Graph Processing in Cloud Environments with Heterogeneous Resources," in IEEE Transactions on Software Engineering, 2021; 47(8): 1729-1741. Available from: https//:doi:10.1109/TSE.2019.2934849.
9. R. Mendes, T. Oliveira, V. Cogo, N. Neves and A. Bessani, "Charon: A Secure Cloud-of-Clouds System for Storing and Sharing Big Data," in IEEE Transactions on Cloud Computing, 2021; 9(4): 1349-1361. Available from: https://doi: 10.1109/TCC.2019.2916856.
10. S. Sathish Kumar, R. Ramkumar, S. Sivarajeswari, D. Ramya, T. Subburaj, Martin Sankoh, "Performance Enhancement of a Three Phase Boost-Cascaded Fifteen Level Inverter Using the PI Controller", Mathematical Problems in

Engineering, vol. 2022, Article
ID 3888571, 17 pages, 2022. https://doi.org/10.1155/2022/3888571

11. S. Hosseinalipour and H. Dai, "A Two-Stage Auction Mechanism for Cloud Resource Allocation," in IEEE Transactions on Cloud Computing, 2021; 9(3): 881-895. Available from: https://doi:10.1109/TCC.2019.2901785.
12. S. Tuli, S. Ilager, K. Ramamohanarao and R. Buyya, "Dynamic Scheduling for Stochastic Edge-Cloud Computing Environments Using A3C Learning and Residual Recurrent Neural Networks," in IEEE Transactions on Mobile Computing, 2022; 21(3): 940-954. Available from: https://doi:10.1109/TMC.2020.3017079.
13. S. K. Pande et al., "A Smart Cloud Service Management Algorithm for Vehicular Clouds," in IEEE Transactions on Intelligent Transportation Systems, 2021; 22(8): 5329-5340. Available from: https://doi:10.1109/TITS.2020.3021075.
14. W. Zhang, X. Chen and J. Jiang, "A multi-objective optimization method of initial virtual machine fault-tolerant placement for star topological data centers of cloud systems," in Tsinghua Science and Technology, 2021; 26(1): 95-111. Available from: https://doi: 10.26599/TST.2019.9010044.
15. Ravindran R, Sathiasamuel CR, Ramasamy P, Balasubramanian K. MSVM-based hybrid energy-fed quasi-Z-source cascaded H-bridge inverter for grid-connected system. Int Trans Electr Energ Syst. 2021;e13139. doi:10.1002/2050-7038.13139.