Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Advancing Trust Frameworks for Next-Generation Security in Cloud Environments via Role-Based Access Control

Kaustav Roy[1], Shivnath Ghosh[2], Amitava Podder[3]
Department of CSE, Brainware University, Kolkata
kaustroy@gmail.com, shivghosh.cs@gmail.com, amitavapodder24@gmail.com

Abstract

Making sure there are strong security measures in place becomes crucial as cloud computing continues to change the technology landscape. In this research, we introduce "Cloud Guard," a novel system that uses role-based access control (RBAC) to enhance trust paradigms in cloud environments. Through the smooth incorporation of RBAC principles, Cloud Guard not only improves security but also tackles the ever-changing issues brought forth by cloud infrastructures. In order to strengthen next-generation security measures for cloud-based infrastructures, this article examines the design, benefits, and use of Cloud Guard. The swift spread of cloud computing has highlighted how important it is to have strong trust mechanisms in place to protect sensitive data and guarantee the integrity of cloud environments. This research proposes a revolutionary technique to build a fresh trust mechanism for cloud computing, hence enhancing user trust. By utilizing the established effectiveness of Role-Based Access Control (RBAC), our suggested framework adds novel components that improve cloud environments' overall security posture. This paper explores this novel trust mechanism's architecture and implementation, explaining how it might be used to address new cloud security concerns. Through the integration of innovative components with the adaptability of RBAC, this methodology not only strengthens access control but also paves the way for increased security and trust in modern cloud infrastructures.

Keywords: Cloud Security, Trust Frameworks, Role-Based Access Control, Cloud Computing, Security Mechanisms, Next-Generation Security, Cloud Guard, RBAC Implementation, Cloud Environment, Cyber security.

INTRODUCTION:

The widespread adoption of cloud computing has ushered in unprecedented opportunities for scalability, flexibility, and efficiency in data management. However, this surge in digital transformation also brings forth a pressing need for robust security measures to safeguard sensitive information within cloud environments. One cornerstone of ensuring security in such dynamic ecosystems is the establishment of an effective trust mechanism. This paper introduces a pioneering approach to fortifying trust in the cloud by leveraging the proven principles of Role-Based Access Control (RBAC). [1]

As organizations increasingly rely on cloud infrastructure to store, process, and disseminate data, the traditional paradigms of access control are faced with new challenges. The need to accommodate diverse user roles, dynamic resource allocation, and the ever-evolving threat landscape necessitates innovative solutions. In response to these challenges, our proposed trust mechanism not only builds upon the established principles of RBAC but also integrates novel elements to adapt to the intricacies of contemporary cloud environments.

This introduction provides an overview of the escalating importance of security in cloud computing and sets the stage for the exploration of a novel trust mechanism. By combining the strength of RBAC with innovative features, our approach seeks to redefine access control in the cloud, offering a promising avenue for enhancing security, managing complexities, and instilling trust in the digital age.

A distributed computing paradigm known as "cloud computing" charges consumers for the services they utilize. The primary goal of developing a cloud computing system is to offer end customers affordable, scalable on-demand services. Users don't have to worry about installing expensive software on their computers. Additionally, consumers can use their services whenever they need them and don't have to worry about maintaining their own physical infrastructure. Infrastructure as a service (IaaS), platform as a service (PaaS),

and software as a service (SaaS) are the services offered by the cloud service provider (CSP) and are referred to as cloud services. [2]

Users may lose physical control over their data and computation when they outsource certain tasks to a cloud server. Users who lose physical control are less able to fend off some threats and attacks.

To safeguard user data and computation in cloud environments, the cloud service provider (CSP) must defend the cloud server against various risks and attacks. Users had to have mutual trust with cloud providers before outsourcing their data and processing. Thus, prior to any interaction, the users and CSP need to have mutual trust. Based on the security criteria and the level of service the CSP offers, the user has faith in the CSP.

Users must have the CSP's confidence before they may access cloud resources or services from the cloud server. The CSP's resources are impacted if any authorized user engages in harmful behavior or launches attacks against the cloud server.

As a result, the CSP is unable to fulfil the service level agreement and security objectives. The CSP only permits the trusted user to access the service in order to safeguard the resources. We must first assess the user's trust value in order to identify the trustworthy user. A user is regarded as trustworthy if their trust value exceeds the trust threshold value**.** The user behavior parameter serves as the basis for evaluating the user trust value. [4][5]

LITERATURE REVIEWS:

Introduction: As organizations increasingly migrate their infrastructure and services to cloud environments, the need for robust security mechanisms becomes paramount. "Cloud Guard: Advancing Trust Frameworks for Next-Generation Security in Cloud Environments via Role-Based Access Control" addresses this imperative by proposing a novel approach to enhancing security in the cloud through the implementation of Role-Based Access Control (RBAC). This literature review aims to explore the existing body of knowledge related to cloud security, RBAC, and trust frameworks to provide a comprehensive understanding of the context in which the proposed "Cloud Guard" framework operates. [2][3][6]

1. Cloud Security Landscape: The evolution of cloud computing has introduced numerous benefits, such as scalability, flexibility, and cost-effectiveness. However, this shift to the cloud has also brought forth security challenges, including data breaches, unauthorized access, and compliance issues. The literature reveals a growing consensus on the necessity of advanced security measures to safeguard sensitive information in cloud environments. [7][8]

2. **Role-Based Access Control (RBAC):** RBAC has emerged as a popular and effective access control mechanism, particularly in cloud computing environments. This model assigns permissions to users based on their roles within an organization, streamlining the management of access rights and reducing the risk of unauthorized activities. Previous studies have highlighted the advantages of RBAC in achieving a fine-grained access control system and minimizing potential security vulnerabilities. [6]

3. **Trust Frameworks in Cloud Security:** Trust frameworks play a pivotal role in establishing and maintaining a secure cloud environment. Literature in this area discusses the significance of trust models, identity management, and authentication protocols. Trust frameworks contribute to building confidence among users, administrators, and stakeholders, fostering a secure and reliable cloud ecosystem. The integration of RBAC into trust frameworks enhances access control mechanisms and ensures that users are granted permissions based on their roles and responsibilities.[1]

4. Advancements in Next-Generation Security: The "next-generation security" concept emphasizes proactive and adaptive approaches to counter evolving threats. This includes leveraging artificial intelligence, machine learning, and behavioral analytics to detect and respond to security incidents in real-time. The literature suggests that incorporating RBAC into next-generation security frameworks can enhance the adaptability and responsiveness of the security infrastructure in cloud environments. [9][12][19]

5. Existing Gaps and Challenges: While RBAC is recognized for its efficacy, challenges such as scalability, dynamic environments, and policy management complexities persist. Additionally, the literature indicates a need for continuous improvements in trust frameworks to address emerging security threats effectively. "Cloud Guard" aims to bridge these gaps by proposing an advanced trust framework that incorporates RBAC, catering to the specific security demands of next-generation cloud environments.

PROBLEM DESCRIPTION:

The primary subjects of this thesis are user authorization, security, and the quality of service provided by the cloud provider. The objective is to assess the user trust value. evaluating user behavior metrics and cloud resources, in that order, to determine the trustworthiness of cloud resources.

Let's tackle the issue mathematically. We define Rj as the collection of cloud resources (j = 1, 2,....m) and Ui as the total number of cloud users (i = 1, 2.....n).

Finding the trusted user T Uk ⊆ Ui and the trusted resource T Rl ⊆ Rj based on the user behavior parameter and the quality of service, respectively, is the main goal.

SUGGESTED FRAMEWORK:

In order to complete the authorization process, the user request is routed via a number of sub modules according to our innovative trust-based access control approach. Figure displays the deployment and operation of the suggested paradigm within a cloud service provider (CSP). In the cloud environment, every resource and service is secured. There are numerous resources of both the same and distinct kinds, and each resource has a unique trust value and capability. Out of all the resources available, the suggested model chooses which user is permitted access to the service and which resources are the most reliable for the users.

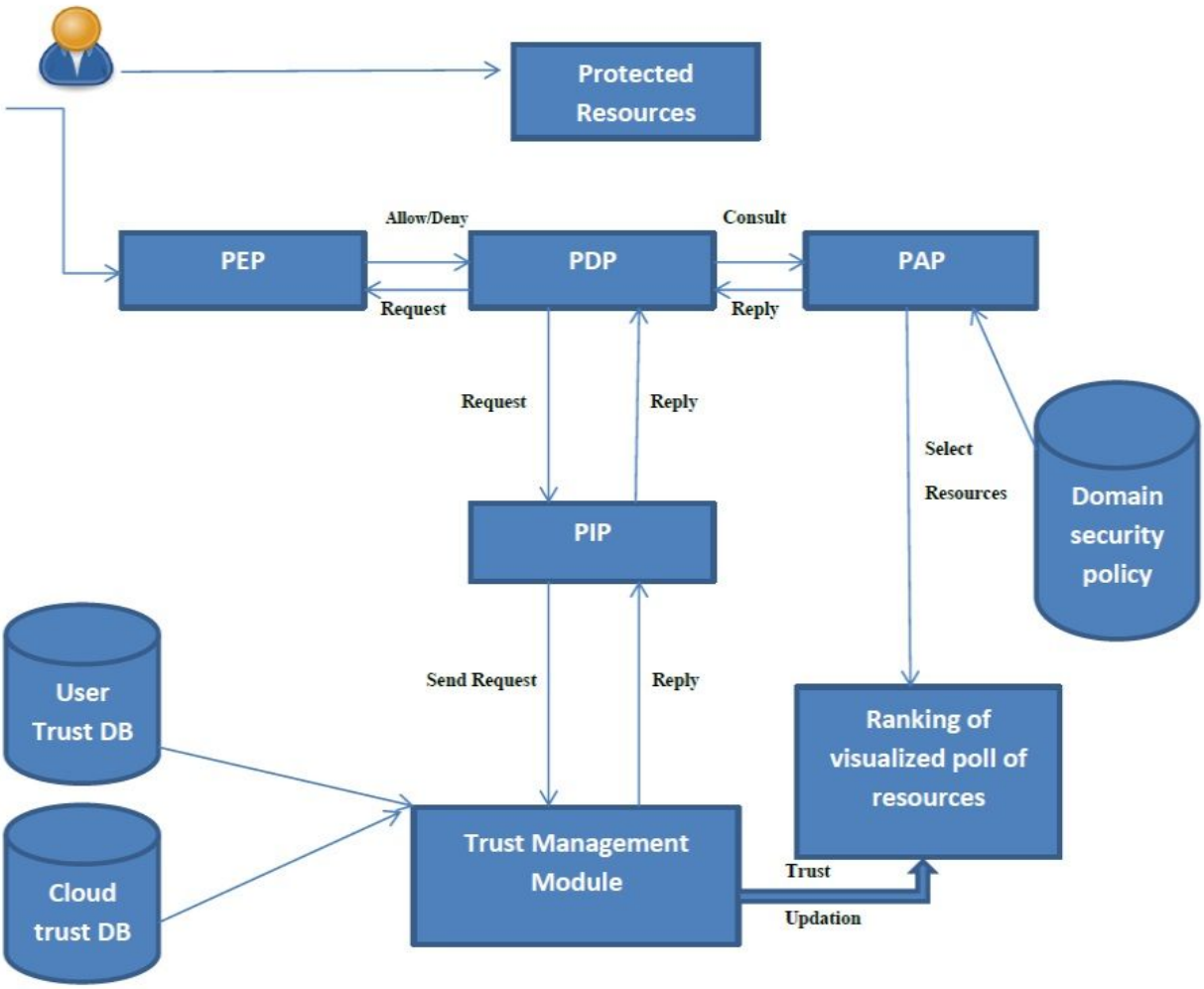


Fig.01: Suggested Framework [1]

The function of each of the suggested model's sub modules, which are covered in the following manner:

Point of Policy Enforcement (PEP): The user requests are received by PEP from the cloud clients and submit the request to the PDP for review. Following receipt of the PDP's grant or deny response, the cloud clients make sure that the necessary steps are followed.
The Policy Information Point (PIP): This module is responsible for compiling data in order to assess permission policies. PIP gets data from the trust management about the requested user, including the user trust value.
Policy Decision Point (PDP): PDP determines whether to approve or reject an access request after gathering pertinent data from the PIP and speaking with the PAP.
The Policy Administration Point (PAP): serves as a central location for authorization policies that are articulated through actions. The system allows subjects, or cloud users, to adopt different objects, or cloud resources. In essence, the authorization policies are an organization-specific implementation of the access control paradigm. [1][4][18]It serves as the center piece of the access control authorization section. PAP compares the data it receives from PDP with the cloud service provider's domain security policy before making a judgment. All user and cloud resource trust threshold value information is stored in the domain security policy.
Trust Management Module (TMM): The centrepiece of the suggested approach is TMM. The trust management module is the only source of the user's authorization. The trust value of user and cloud resources is assessed using TMM. [6][16][17] Following the assessment of cloud resource trust values, TMM assigns an average trust value to each resource category. Lastly, TMM updates the associated database with the prior trust value of users and cloud resources.

PROCESS OF AUTHORIZATION

Prior to using any cloud provider services, the user must first submit their quality of service requirements, including security, processing power, and networking speed, to the cloud service supplier. For a final agreement, the user and cloud provider may bargain among themselves over service quality. The term "service level agreement" refers to this arrangement. The method of obtaining user authorization to access the service is explained by the algorithm below. [1][7][8]

Step 1: The user request is accepted by the policy enforcement point (PEP), which then forwards it to the policy decision point (PDP).
Step 2: PDP sends the information to the Policy Information Point (PIP) after verifying that all user credentials are correct.
Step 3: PIP requests the user trust value from the Trust Management Module (TMM).
Step 4: PIP sends the necessary data to the PDP after obtaining it from TMM.
Step 5: PDP sends all information from PIP and PEP to the Policy Administrative Point (PAP) for consultation.
Step 6: In the end, PAP verifies and contrasts all of the user data it has gathered with the resource database and domain security policy. The user is granted access if their trust value above the user trust threshold; otherwise rejected.
Step 7: If the user is given permission, PAP will search for resources based on the kind of request they have received, select the most trustworthy resource from the available resources, and send it to the PDP.
Step 8: PDP provides the resource ID to PEP; in the event that it is rejected, PDP sends a deny message.
Step 9: PEP provides it to the user along with an allow or deny message.
Step 10: The user can now obtain the required serive.

MODULE FOR TRUST MANAGEMENT (TMM):

One of the most crucial components of the suggested authorization model is TMM. Figure illustrates how the TMM is made up of various sub-modules that are involved for the purpose of assessing the users and the cloud resources' trust value. This module operates continuously within the CSP to keep an eye on resource quality of service and user behaviour. Not a single module in the suggested paradigm is prejudiced toward the cloud provider, even though everything is run and distributed by the CSP. [1] [9][11] This module assesses the trust value of users and resources over a number of stages or cycles. We now move on to describe the roles and actions of each component involved in the entire life cycle for the evaluation of trust value.

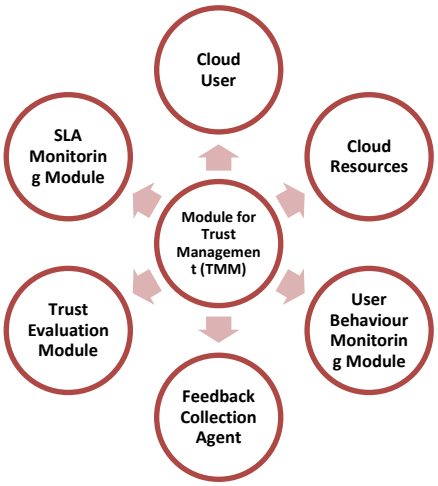


Fig.02 Trust Management Module

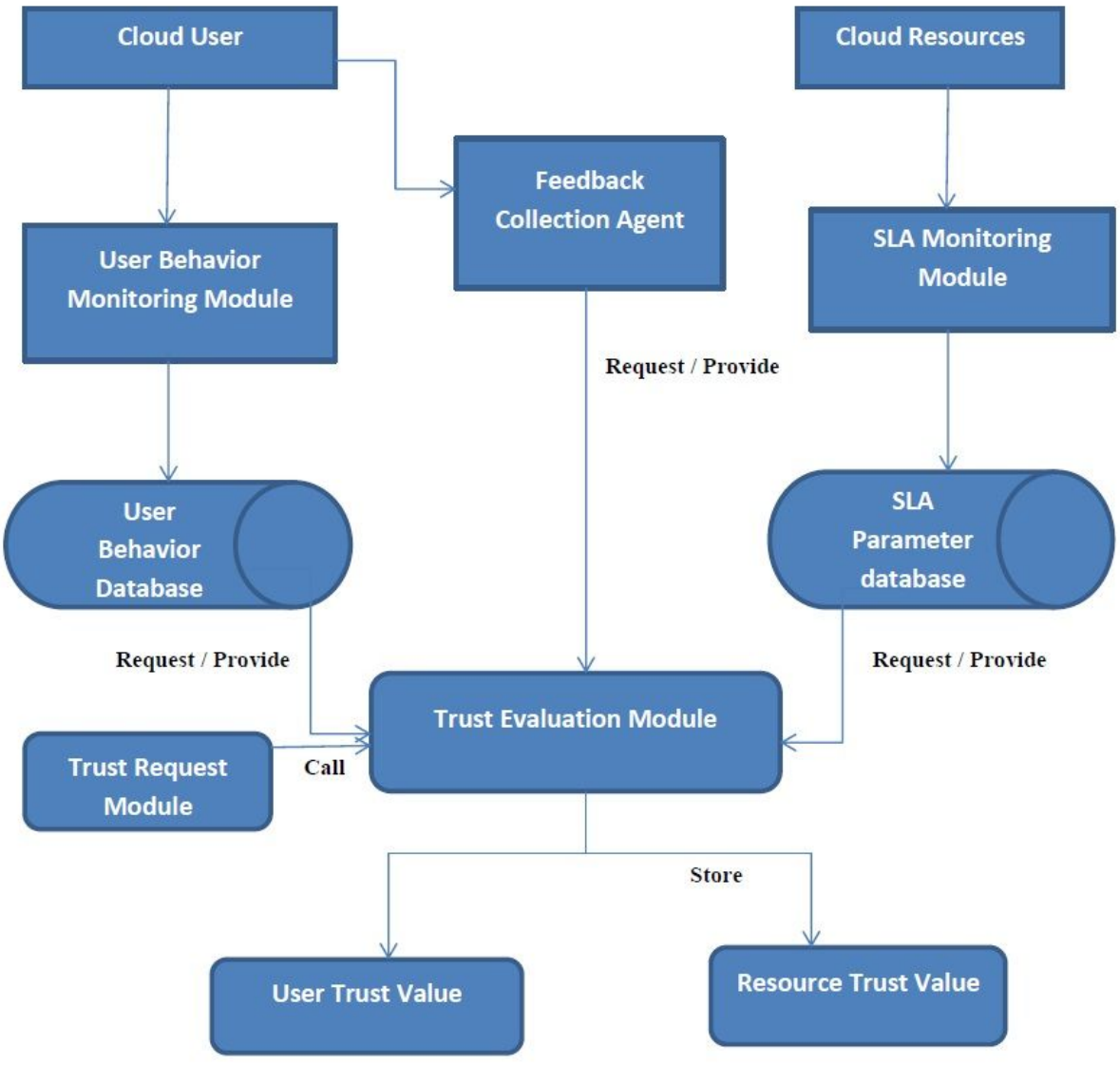


Fig.03 Module for Trust Management (TMM)

PARAMETER FOR EVALUATING TRUST:

When evaluating the trust levels of users and cloud resources, the trust evaluation parameter is taken into account. It is made up of SLA and user behavior parameters.

User behavior parameter: Users' trust value is assessed using the user behavior parameter. The resources will be impacted if the user engages in malicious activities or launches an assault on the cloud server, making it impossible for the CSP to provide the required level of service. The module for monitoring user behavior records the way a user interacts with resources and saves that information in the user behaviour database. [1][7][12]

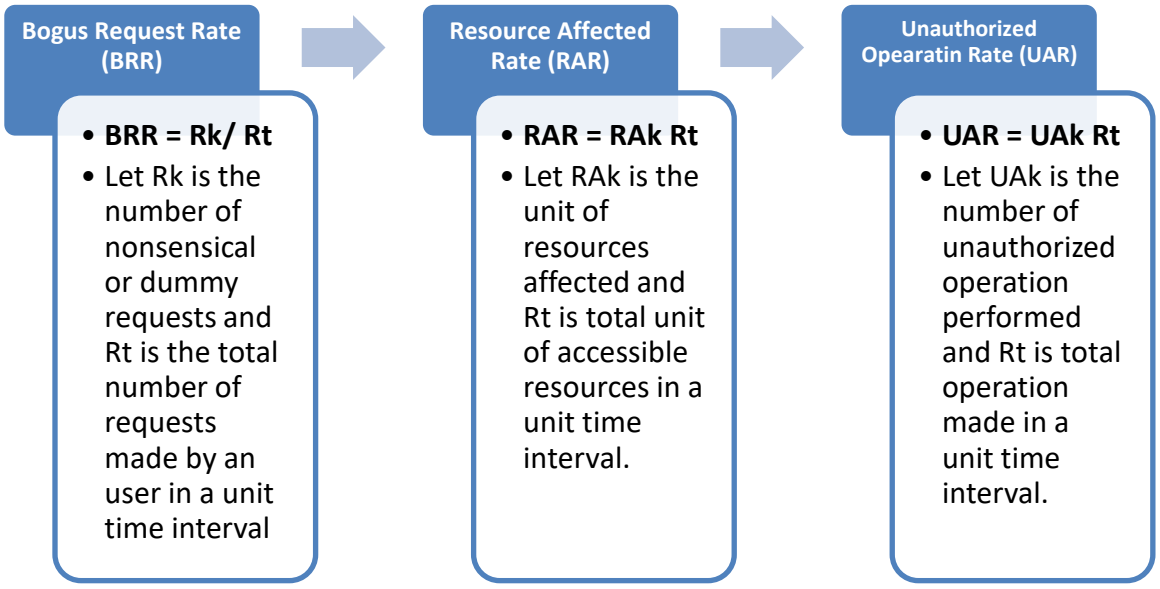


Fig.04 User behaviour parameter

SLA variable:

The SLA parameter is employed in the assessment of cloud resource trust value. Should the CSP fail to satisfy any user's security level and SLA requirements, then the CSP would lose credibility. The following is a discussion of the parameter used to evaluate the trust value of cloud resources:

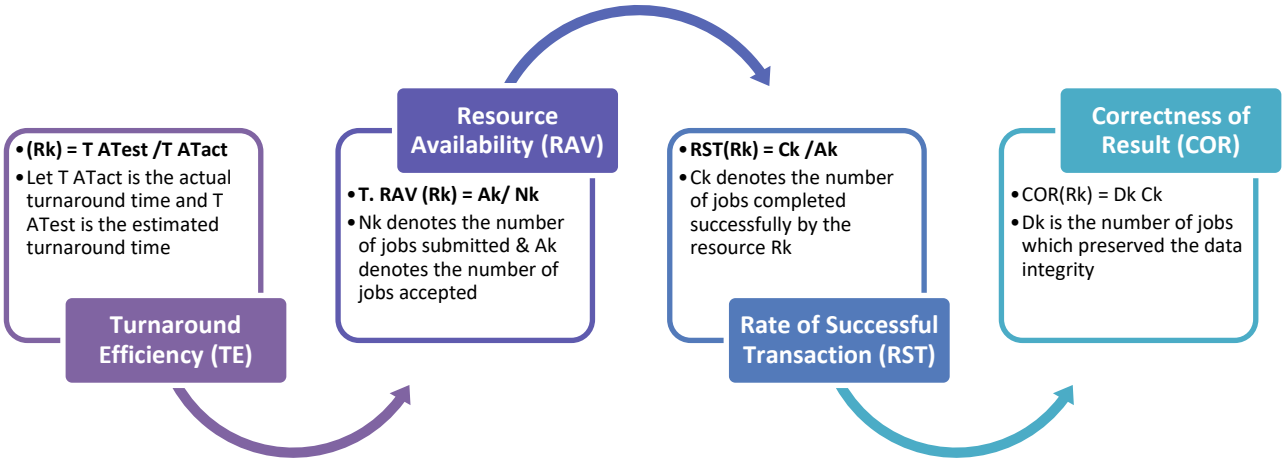


Fig.05 SLA Variables

METHOD FOR EVALUATING TRUSTS:

We evaluate the trust value of both users and cloud resources after their contact is finished in a given amount of time. Several interactions may occur during this time. We initially evaluate the trust value in the current time frame using the trust values from the present time window and the average trust value from the previous time window. The trust value evaluation timeline graphic. Let tn and tn−1 represent the time intervals for the current and previous time windows, respectively.

The following formulas are used to calculate the average user trust (AUT) and user trust (UT) values:

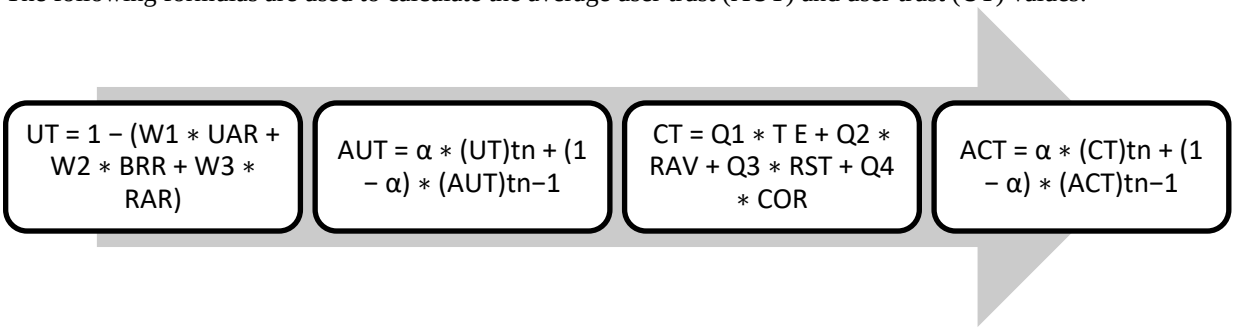


Fig.06 Formula for AUT & UT Values

Where the average resource trusts value (ACT) and the resource trust value (CT) are the respective values. Where the weight parameters [22] of TE, RAV, RST, and COR are, in turn, Q1, Q2, Q3, and Q4. The weight values for the tn and tn−1 time intervals are α and 1-α.

IMPLEMENTATION TASKS AND OUTCOMES:

Introduction: To assess the effectiveness of our suggested model, algorithm, and evaluation approach, we trust worthiness of cloud and user resources. The user and cloud resources are classified as either benign or malevolent based on the trust values.

Experimental Configuration: We build a virtual cloud environment where various capabilities' resources are defined. The user first provides the cloud provider with their quality of service specifications, including security, processing power, and networking speed. We use the following platform to put our suggested model into practice: Net Beans IDE, JDK 1.7, oracle 11g.

Based on the priority of the security requirement in our experiment, we make assumptions about the probability values of the weight parameters for the SLA and user behavior characteristics. We take into account the likelihood values for the user behavior parameter and SLA parameter, which are displayed in Tables A and B, in that order. The system that has been implemented has a Corei5 CPU with a 3.2 GHz clock speed, 4GB RAM, 500 GB HDD, and an operating system that runs Windows 8.

Weight Parameter	Probability
W-1	0.4
W-2	0.3
W-3	0.5

Table 01: For User Behaviour Parameter

METHOD OF EXECUTION:

The following describes the implementation processes needed to find the malicious users and resources:

- Service level agreement (SLA) negotiations between cloud service provider and user.
- Permission from the user.
- Allocating resources to authorized users.

- Tracking the SLA and user behavior parameters for cloud resources and users, respectively.
- The feedback gathering agent receives the feedback from users.
- Retrieve the information about the SLA and user behavior parameters from the relevant databases.
- Assess the cloud user and resource trust values as well as their average trust values.
- Revise the ACT and AUT.
- Sorting the resources based on their level of trust.
- Lastly, determine which users and resources are harmful or untrustworthy.

SIMULATION OUTCOMES:

For every unit of time, we assess the trust values of cloud resources and users. Following the assessment of trust values, we divide the resources and users into two distinct kinds, such as good and bad.

Trust value of different type of users:

Weight Parameter	Probability
Q-1	0.12
Q-2	0.21
Q-3	0.23
Q-4	0.52

Table 02: For SLA parameter

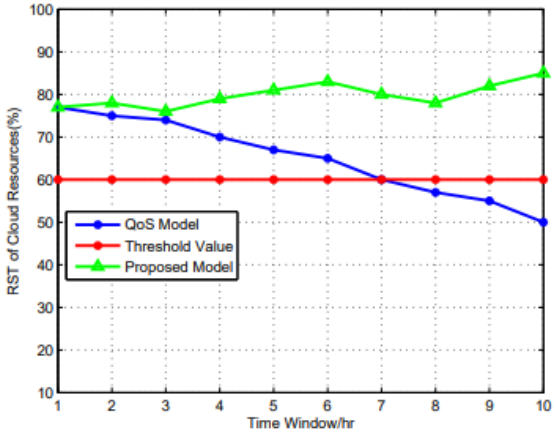
Trust value of different CSP:

	Good	Malicious
Type of User	AUT ≥ UT T	AUT < UT T
Type of CSP	ACT ≥ CTT	TACT < CT T

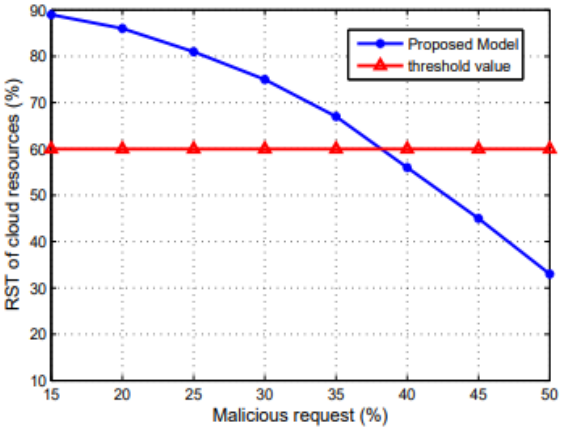
Table.03: Type of user and CSP

SUCCESS RATE OF TRANSACTIONS (RST):

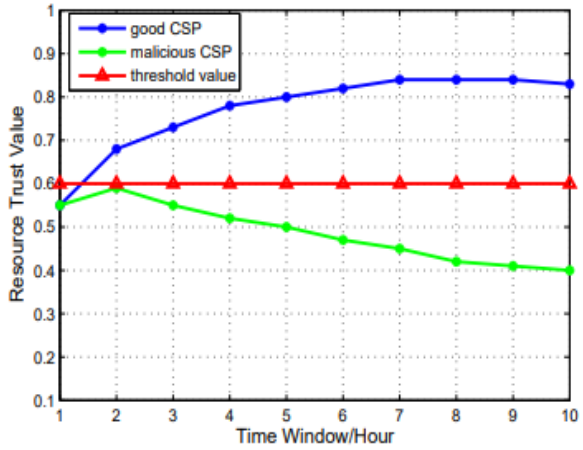
This experiment shows how successful cloud resources are. We use the percentage of malicious requests to determine the success rate of cloud resource transactions.



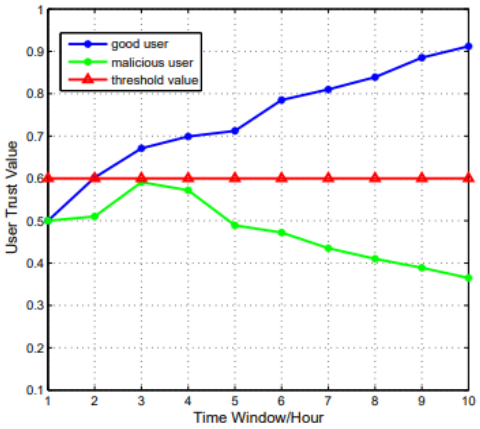
Graph-01 Trust value of cloud users



Graph.02 Trust value of different CSP



Graph.03 RST of cloud resources



Graph.04 Comparison of RST among Qos

CONCLUSION:

At the end of the day, "Cloud Guard: Advancing Trust Frameworks for Next-Generation Security in Cloud Environments via Role-Based Access Control" is a noteworthy advancement in strengthening cloud infrastructure security. The Cloud Guard framework's implementation of Role-Based Access Control (RBAC) provides a strong and scalable method for controlling access privileges, thwarting potential attacks, and guaranteeing the availability, confidentiality, and integrity of sensitive data.

Establishing trust frameworks and taking a proactive approach to security can help firms better manage the ever-changing and complicated world of cloud environments. Cloud Guard positions itself as a key element in the continuous growth of cloud security strategies by not only addressing present security issues but also foreseeing future dangers.

Additionally, by emphasizing user roles and permissions, access privileges are managed more precisely and granularly, in accordance with the idea of least privilege. This helps meet governance and regulatory compliance needs in addition to improving overall security. It is impossible to overestimate the significance of having thorough and flexible security architecture as the digital landscape changes. With its focus on RBAC, Cloud Guard not only solves today's security issues but also lays the groundwork for future enhancements and adaption to new threats. To put it simply, the deployment of Cloud Guard represents a significant stride in the direction of striking a healthy balance between security and innovation in cloud environments.

Within cloud computing, the trust-based access control paradigm is a very successful security measure. In this study, we introduced a novel trust-based access control technique. Model for cloud computing ecosystem. The main goals of this approach are to authorize the user and select the most trustworthy resource for them. Depending on the user's trust value, permission is given. We determine the trust value of each user and categorize them into different groups, such as honest and dishonest users. We evaluate the trust value of cloud resources based on the quality of service provided to users. We investigate the detrimental effects of user behavior on cloud resources and the decline in resource reliability.

REFERENCES

1. Behera, P. K. (2015). *Novel Trust Based Access Control Model for Cloud Environment* (Doctoral dissertation).
2. Farroha, B. S., & Farroha, D. L. (2010, April). Enterprise systems security management: a framework for breakthrough protection. In *Defense Transformation and Net-Centric Systems 2010* (Vol. 7707, pp. 170-181). SPIE.
3. Zhifeng Xiao and Yang Xiao. Security and privacy in cloud computing. Communications Surveys & Tutorials, IEEE, 15(2):843–859, 2013.
4. David F Ferraiolo, John F Barkley, and D Richard Kuhn. A role-based access control model and reference implementation within a corporate intranet. ACM Transactions on Information and System Security (TISSEC), 2(1):34–64, 1999.

5. Peter Mell and Tim Grance. The nist definition of cloud computing. 2011.
6. Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security, pages 199–212. ACM, 2009.
7. Amittai Aviram, Sen Hu, Bryan Ford, and Ramakrishna Gummadi. Determinating timing channels in compute clouds. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop, pages 103–108. ACM, 2010.
8. Srikanth Kandula, Dina Katabi, Matthias Jacob, and Arthur Berger. Botz-4-sale: Surviving organized ddos attacks that mimic flash crowds. In Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2, pages 287–300. USENIX Association, 2005.
9. Abraham Yaar, Adrian Perrig, and Dawn Song. Fit: fast internet traceback. In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, volume 2, pages 1395–1406. IEEE, 2005.
10. Americas Headquarters. Cisco data center infrastructure 2.5 design guide. 2007. [9] Giuseppe Ateniese, Roberto Di Pietro, Luigi V Mancini, and Gene Tsudik. Scalable and efficient provable data possession. In Proceedings of the 4th international conference on Security and privacy in communication networks, page 9. ACM, 2008.
11. Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, and Dawn Song. Provable data possession at untrusted stores. In Proceedings of the 14th ACM conference on Computer and communications security, pages 598–609. Acm, 2007.
12. Cong Wang, Kui Ren, and Jia Wang. Secure and practical outsourcing of linear programming in cloud computing. In INFOCOM, 2011 Proceedings IEEE, pages 820–828. IEEE, 2011.
13. Meiko Jensen, J¨org Schwenk, Nils Gruschka, and Luigi Lo Iacono. On technical security issues in cloud computing. In Cloud Computing, 2009. CLOUD'09. IEEE International Conference on, pages 109–116. IEEE, 2009.
14. Vyas Sekar and Petros Maniatis. Verifiable resource accounting for cloud computing services. In Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pages 21–26. ACM, 2011.
15. Bai Qing-hai and Zheng Ying. Study on the access control model. In Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011, volume 1, pages 830–834. IEEE, 2011.
16. Dewangan, O., & Sarkar, P. (2022). A Study on Network Security Using Deep Learning Methods. Advanced Engineering Science, 54(02), 6393 – 6404.
17. Sarkar, S. K., Podder, A., & Roy, P. An Analysis of the Privacy and Security Related Problem with Social Networks. ESP Journal of Engineering and Technology Advancements (ESP-JETA), 3(4), 37-43, (2023).
18. Sarkar, P., & Dewangan, O. (2022). Applying Advanced Deep Learning to Optimize Clinical Image Analysis. NeuroQuantology, 20 (21), 123–129.
19. Biswas, S. K., & Podder, A. (2021). Cost Estimation of Passive Optical Network (Pon) for Sub Optimal Deployment with Application of Path Minimization Technique and Wavelength Allocation Based of Bit Error Rate (Ber) Performance. International Journal of Innovations in Engineering Research and Technology, 8(2), 2021, 6-14.