International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I9P217
Volume 70 Issue 9, 167-175, September 2022

Original Article

Access Control in Cloud Computing using Swarm based Intelligence

Aparna Manikonda[1], N. Nalini[2]

[1,2]*Department of Computer Science, Nitte Meenakshi Institute of Technology, Karnataka, INDIA.*

[1]*Corresponding Author : aparna.subhadra@gmail.com*

Received: 14 June 2022 Revised: 22 August 2022 Accepted: 11 September 2022 Published: 17 September 2022

Abstract *- The new Cloud computing advances stand out due to their Storing ability and minimal expense administrations. The entertainers of the cloud face many issues due to virtualized and adaptable web administrations, which prompts genuine security challenges. Access control is quite possibly the main measure to guarantee distributed computing security. A large portion of the Access control models conceived for Cloud processing is cryptography-based, which leads to overhead with an increased number of users and services. Maintaining a secure, efficient system is important to improve solutions for better success and overhead. In this research, the balance of swarm intelligence and trust is the executives for implementing a novel method in cloud systems. The proposed method has articulated calculations to give better security to implement the reputation system. The outcome shows that this method can ensure better accuracy, accessibility and achievement.*

Keywords *- Cloud Computing, Access Control, Swarm Intelligence, Trust mechanism, security.*

1. Introduction

Cloud computing is an archetype that offers a computation and storage foundation over a flexible system of assets [1]. With cutting-edge technology, information is dispersed on various servers, and applications are far-off run-on servers. Cloud innovation brings dispersed information to the client's PC in a near structure. The principal thought is to make processing and infrastructure accessible for cloud clients regardless of the overall setting. There should be a mutual understanding between the parties, i.e. cloud user and cloud service provider. The vital reason for an access control framework is to uphold limitations on the general openness of an approved client over the framework [2-4].

Besides, the Cloud computing processing gives extension to the dividing of subtle data between different occupants, which thereof requires to have a strong authentication [5-9]. Most access control methods in cloud computing are either encryption or trust-based. However, using swarm intelligence (SI) to control data access in the cloud is a novel concept. The application of swarm intelligence in cloud computing is based on these three groups 1) Load Balancing [21,22], 2) Task Scheduling [23,24], 3) Intrusion Detection [18], and 4) Optimization [11].

This research uses Swarm Intelligence (SI) for access control because of its dynamism and intelligent communication that does not require intricate computations. The method uses a trust management model to avoid complex calculations and overhead in the existing systems for an effective decision-making process.

In addition, swarms (in this case, ants) are considered the most encouraging individual from gathering to be utilized in security innovation because of their cautious behaviour. Subsequently, the security system is animated by the regular way of behaving insects and all smart agents as ants with self-healing infrastructure. For example, on the off chance that any ant can identify danger, as indicated by this idea, it illuminates its province right away, and many ants merge to make a move against that danger. The scheme uses swarm knowledge to achieve trust and safeguard attacks by taking advantage of the above thoughts. The objective of this work is the applicability of SI in cloud processing for a reliable, secure system over trust value in a specific session.

2. Literature Review

This related work tries to give an idea to the reader about the implementation of access control in cloud processing using Swarm intelligence and trust. The first part of the review describes available access control methods, the second part is about the implementation of SI for intrusion detection, optimization and task scheduling and Lastly, methods about trust mechanism in cloud systems.

Access control is a significant data security innovation and has become irreplaceable for endeavors to safeguard information and assets in data frameworks. After numerous improvements, research on access control models has

accomplished recognizable advancements. Access control in cloud computing provides effective insurance to its resources. Moreover, access control in cloud computing isn't simply a specialized issue. It likewise includes a ton of angles like normalization, regulations and guidelines, implicit sets of rules, and so forth [4-8].

The idea of forwarding and backward Ants (Swarm Intelligence) alongside Honeypots to distinguish the organization interruption by following a pre-laid-out idea of the burden balancer and Intrusion Detection System. The joining of these two innovations, notwithstanding, is a non-trifling undertaking. Furthermore, while a substance-based load balancer offers many benefits over different Load Balancing and IDS arrangements, it also experiences both downsides [9].

Swarm intelligence is proposed for secure medical applications and optimization methods [28]. The information is collected and studied to direct the protection course via the 2D IIR channel. Nonetheless, the improved method for securing clinical information isn't surfaced. To triumph over this, a method based on a mystery key is created [29] for discomposed data records using Tracy Singh in the network.

Other applications include, A three-tier security structure and an effective classifier has been proposed for the cognitive and cooperative nature of nodes to reduce the overhead. In this approach, three types of Ants are considered UA, CSPA, and CDSA for data transfer authenticated and authorized data. The information about various owners is stored in legitimate honey pots (data storage) as per the degree of safety asked by the owners. They fizzled in addressing the design and evaluation of scheduling algorithms in a real-time cloud environment [15,16,18].

MTBAC [12] implements an ant colony optimization algorithm. In their approach, both client's behavioral and node behaviour are considered for the computation of trust value. The client's way of behaving is isolated into three kinds, and each sort of property has a specific weight. Nonetheless, the vulnerability in client conduct isn't considered in their methodology.

A trust-based control model utilizing an AI strategy is proposed [13]. The basic idea is to give admittance to an approved client for the resource on the computed value. In this manner service provider ought to give access to the confirmed clients. They neglected to consider greater security boundaries for assessment purposes.

A dynamic authorized system was proposed for cloud computing [14], where the authorized users are identified based on trust value. The access privileges of these users are created on their behavior with the system. However, this work adds an overhead due to its various assignments and removal of permissions for malicious users.

A smart user authentication [17] was devised by combining discretionary and role-based models. The approach has client-based user authentication and consists of four main agents with cloud-based SAAS application

This paper presents an effective access control method that uses the Swarm Intelligence technique for better security arrangement, ensuring improved accuracy, availability and success rate.

3. Proposed Work

The proposed model is aimed at better performance, accuracy and availability of resources. Here, the access control policies are based on SI and the trust mechanism.

In the framework, three distinct smart ants are viewed as those are UA (User Ant), CSPA (CSP Ant), and CDSA (CDS Ant). These ants validate the user by their associated credentials and authenticate them to access the system. Further, every ant can convey trust matrices that drive effective policymaking, establishing dependable associations.

3.1. Architecture and System Design

The framework design of the proposed work is depicted in figure 1. data storage is named honey pot. A solitary individual is feeble, yet a gathering of subterranean insects who have conveyed various errands among themselves are more impressive and productive. CSPA dwells inside CSP and shares trust matrices between them that help safeguard malicious attempts if any. Similarly, is Cloud Data Storage (CDS) alongside CDSA. These Ants continuously asses the system and reconfigures it for better security. Each of the ants with various functionalities is considered and as discussed below:

Table 1. Notations

Sl.no.	Notation	Meaning
1	Δt	Gradual increase in trust degree
2	∇t	Gradual decrease in trust degree.
3	ε	Experience
4	UT_c	User Interaction with Cloud Node
5	Tp	Trust pheromone
6	P_{RR}	Prohibited Request Rate
7	V_{MAC}	MAC changes
8	A_R	Resource Accessibility
9	R	Reliability
10	Q_s	Quality of Service
11	N_B	Network Bandwidth
12	B_C	Behavior calculation
13	R_P	the reputation of the resource

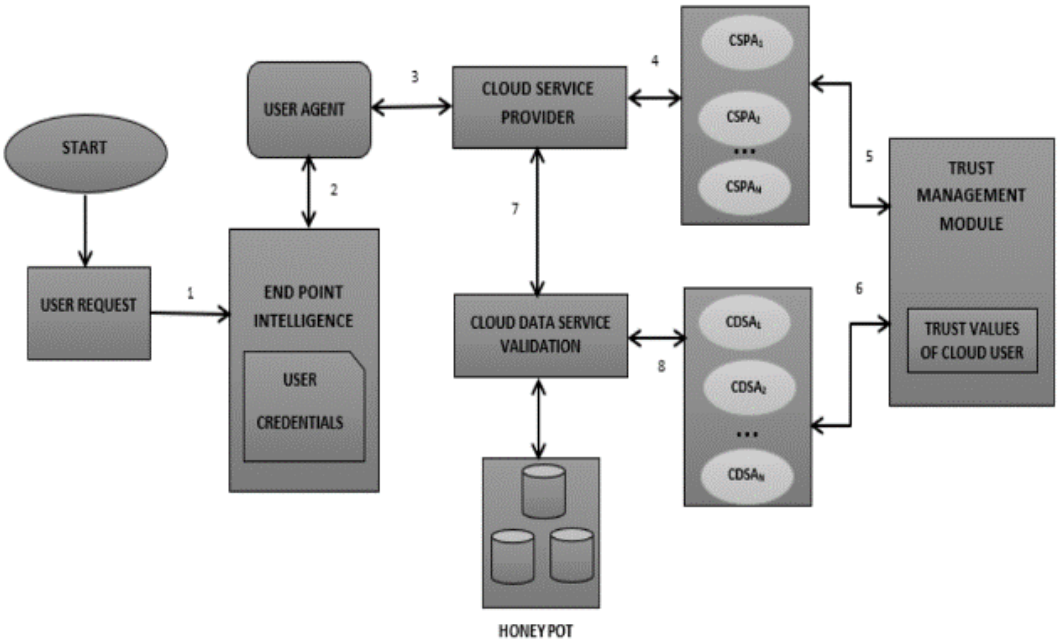

Fig. 1 System Architecture

3.1.1. User Ant (UA)

The communication history and updated trust value of the client are noted by this ant.

3.1.2. CSPA

CSPA resides inside CSP. This agent helps in finding the CDS security level for any pernicious activity

3.1.3. CDSA

CDSA resides inside CDS. Checks the trust level of owner and client and updates their related trust values accordingly. CDSA is also responsible for carrying out discussions alongside the information owner to decide the security level for the information storage.

3.2. Working Principle

1. Subject request for data or resource via a web application/interface as shown in fig. 1.
2. User-agent (UA) submits requests on behalf of cloud users. Once the request gets validated with user credentials, the CSP forwards it to CSPA.
3. CSPA validates the trust assessment module. The client's trust values are broadcasted in the remaining CSPA
4. For valid requests, CSPA checks the trust value of the subject through the Trust Management module.
5. In the trust management module, the T_{VAL} gets extracted from the log file for both resource and user.
    - The behavior value and reputation of the resource are equated to T_{TH}; if the value is less, it drops the request.
    - However, for invalid requests, all neighbor CSPAs are informed about the malevolent attempt of the user. The trust metrics are broadcasted among all possible paths to other CSPA about the inward risk.
    - CSPA validates the request according to the service level agreement to grant access to the cloud resource.
    - If any UA fails this SLA checking, CSP gets reconfigured by CSPA to control the data visibility.
6. CDSA approves the client space and updates the trust metrics with neighbor CDSA's. CDSA does additional checking on service level agreement (SLA).
7. Once the SLA requirements are satisfied, UA's permission is granted, and a channel for Data transfer is arranged between CDSA and UA.
8. The User-agent notifies the subject about access to the requested resource.

3.3. Trust Management Module

The Trust Management module is an essential piece of our approach and consists of different sub-modules. Figure 2. shows the estimation of trust for both cloud-specialist and clients. The clients need to compute trust value rapidly to identify the unhealthy client. It isn't one-sided towards any cloud-specialist co-op or client as well. It may be seen that the TMM contains a few stages for working out trust value. Each of the stages and its functionalities is explained below:

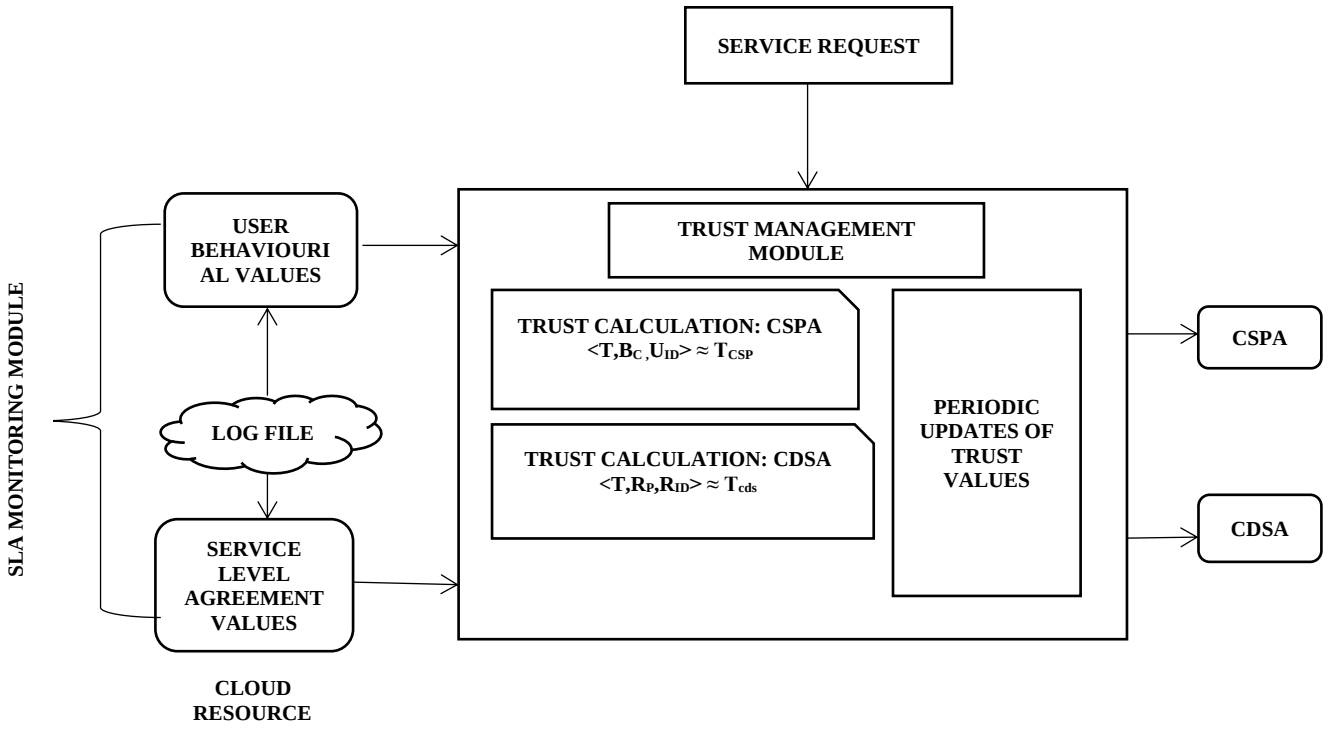

Fig. 2 Trust Management Module

(i) Cloud user: Every client must enlist before getting to the cloud administration. The personality information base contains all the approval subtleties of the multitude of clients. Whenever a client demands an asset from a cloud server, his approval must be checked by client conduct values.

(ii) Cloud Asset: A little equipment or programming can be a cloud asset. Before giving admittance to the asset, the clients' approval must be checked appropriately, and all assistance layer-understanding ought to be satisfied.

(iii) Log document/file of user behavior: Log document records the movements of every sort made by the client in the cloud. This log record catches genuine client conduct through which AI calculations anticipate client trust esteem.

(iv) SLA checking module: SLA observing module catches the constant way of behaving of cloud assets. It additionally catches the presentation of the cloud assets.

3.3.1. WMA–OWA algorithm

For this approach, the scheme uses the WMA-OWA algorithm to measure the trust values of the client [19]. It is a dynamic weighted algorithm where the administrator needs to change the weights of the information associated with measuring the trust value of the client or owner. It has five distinct boundaries connected with the client where combination functions of WMA-OWA allot weights.

Definition 1. WMA model is defined as:

$$F(Q) = \sum_{i=1}^{n} w_i \, q_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \textbf{(1)}$$

where $F(Q)$ is the mass function, q_i is the definite parameter, and w_i is the mass assigned to q_i ($\sum w_i = 1$)

Definition 2. Formally, an OWA operator of dimension n is a mapping F: $Z^n \rightarrow Z$ that has connected n mass vector (w) = $\{w_1, w_2, \ldots\ w_n\}$, such that $\forall\ w_i\ \in [0,1]$ and $\sum w_i = 1$

$$F(q_1, q_2, \ldots\ q_n) = \sum_{i=1}^{n} w_i \, q_i \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

where, q_i is the i^{th} the maximum value in the set $\{q_1, q_2, \ldots\ q_n\}$

3.3.2. Behavioral Parameters

In cloud computing, the trust degree between communicated elements is like the pheromone in ant colony calculation. Cloud users will often pick highly believably elements to give assets or administrations. The parameters considered for this are as follows:

Definition 3. User Experience with Cloud ($\boldsymbol{\varepsilon}$).

It identifies the client's interaction with the framework. Too, the trust incorporates the component of time deterioration wherein the days with practically no association with the framework weaken the ongoing trust value. Δt steady increase in trust degree, ∇t steady decline in trust degree.

ε is evaluated by the following:

$$\varepsilon = \begin{cases} 0.5, \ x = 1 \\ \varepsilon + \Delta t \quad , \ x > 1 \\ \varepsilon + \nabla t, no\ iteraction \end{cases} \quad \text{….. (3)}$$

where x is the total no. of days Δt gradual increase in trust degree, ∇t gradual decrease in trust degree.

Definition 4. User Interaction with Cloud Node UT_c

This metric is a relationship built through the straight practice of communications. At time t, user $u's$ straight trust towards cloud service node c is formalizing as $UT_c(t)$.

Definition 5. Trust pheromone T_p

At time t, user u's trust pheromone towards cloud service node c is represented by $T_p(t)$. At the initial moment, the value of the trust pheromone is generally set to zero; that is $UT_c(0) = C$ (C is constant). If User Interaction with Cloud Node is initially zero, then the value of trust pheromone must be zero too.

Definition 6. Prohibited Request Rate P_{RR}

When an unauthorized user is trying to access and manipulate the resources(R) such requests are called Prohibited requests. It measured as prohibited requests to total requests.

$$P_{RR} = P_R / T_R \ \text{…………………… (4)}$$

where, P_R is prohibited request and T_R is total request

Definition 7. MAC changes V_{MAC}

It indicates the client's trust worth because of the gadget's MAC address through which the client endeavors to interface with the framework.

$$V_{MAC} = \begin{cases} 0, no\ change\ in\ address \\ V_{MAC} + \nabla t, change\ in\ address \end{cases} \text{…. (5)}$$

where ∇t steady decline in trust degree.

3.3.3. SLA Parameters

The parameters between user and service provider are service-layer-agreement, used to estimate the trust value of the resources. The QOS gets affected by security. Below are the metrics considered for SLA:

Definition 8. Resource Accessibility A_R

Resource accessibility is defined as the readiness of cloud service. During the attack, the services are inaccessible for that moment. Hence, it is the ratio between accepted and submitted tasks.

$$A_R = A_T / S_T \ \text{…………………………... (6)}$$

Where:

A_T are total accepted tasks

S_T is submitted tasks.

Definition 9. Reliability R

Reliability of a resource in a period T can be defined as the execution of successful tasks to the accepted number of tasks.

$$R = T_C / A_T \ \text{………………………... (7)}$$

Definition 10. Quality of Service Q_s

Quality of Service is an assortment of efficiency and average response time (amid 0 and 1 built on threshold value).

Definition 11. Network Bandwidth N_B

Defined as a data transfer in the network at a fixed time interval (amid 0 and 1 built on threshold value).

3.3.4. Request Metric for CSP

The request metric for CSP is defined as $< \boldsymbol{T}, B_C, U_{ID} > \approx T_{csp}$

Where:

- T is an ordered set of values $[t_1\ to\ t_n]$ between the current time and threshold time.
- B_C is Behavior calculation. It is the combination of the general client Behavior esteem with the assistance of WMA-OWA calculation. It is acquired by weighted normal assessment involving the various margins/parameters as determined previously.
The method needs to quantify every one of the margins/parameters further as per their commitment to deciding client trust value. The value is calculated as:

$$B_C = \varepsilon * w_1 + UT_c * w_2 + Tp * w_3 + P_{RR} * w_4 + V_{MAC} * w_5 \ \text{……………... (8)}$$

$\{w_1, w_2, ... w_n\}$ are weighing coefficients such that $\forall\ w_i \in [0,1]$ and $\sum w_i = 1$. Here each of the metric descriptions is represented in table 1.

3.3.5. Request Metric for CDS

The request metric for CDS is defined as $< T, R_P, R_{ID} > \approx T_{cds}$

Where:

T is an ordered set of values $[t_1\ to\ t_n]$ between the current time and threshold time.

R_P is the reputation of the resource. CSPA receives this value from CDS and decides to continue with the request after negotiating with UA. The value is calculated as:

$$R_P = Q_1 * A_R + Q_2 * R + Q_3 * Q_s + Q_4 * N_B \text{… (9)}$$

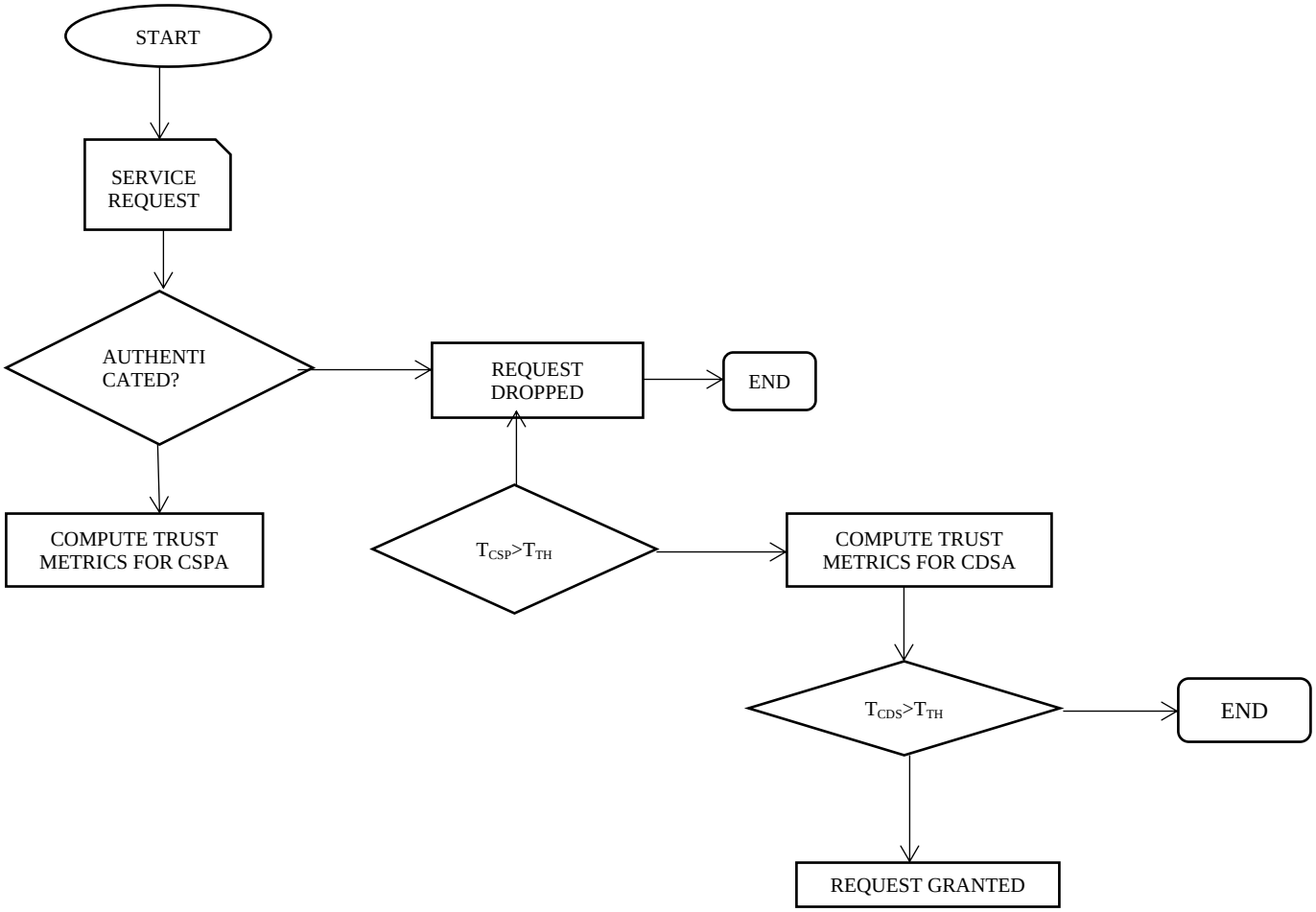

Fig. 3 Flow Chart for Trust Evaluation

Algorithm 1: Authorization

1. Input: Trust Valuation Parameters of Requested User
2. Output: Updated trust values and access to the resource.
3. Begin
4. for each user $u_i \in u$ do
   Compute weights w_1 to w_n Wma-Owa
   Compute B_c (u_i) using eq. 8
   Broadcast (T_{csp});
5. if (T_{csp} (u_i) > 0.5) then
6. Compute T_{cds} (u_i) using eq.9
7. Broadcast (T_{cds});
8. if (T_{cds} (u_i) >0.5) then
9. UA ↔CDSA
10. else
11. Decrement the trust degree;
12. else
13. Return request failed;
14. end for

Algorithm 2: Authentication

1. Input: User Request, User Credentials
2. Output: Request Is Accepted or Rejected.
3. Begin
4. The user sends r_q for accessing data resource
5. If (User Credentials is, ok?)
6. then
7. Request redirects to User_Agent(UA)
8. User_Agent (UA) submits the request to CSP
9. end if
10. else
11. Drop (User Request);
12. end

4. Performance Evaluation

CloudSim3.0 [20] is used to simulate the proposed method. An eclipse editor is an operating environment for simulation, the language used is JAVA, and 64-bit Operating System is Ubuntu18.04. An order of 100 requests ranging from 0 to 100 with a step size of 20 is used in this

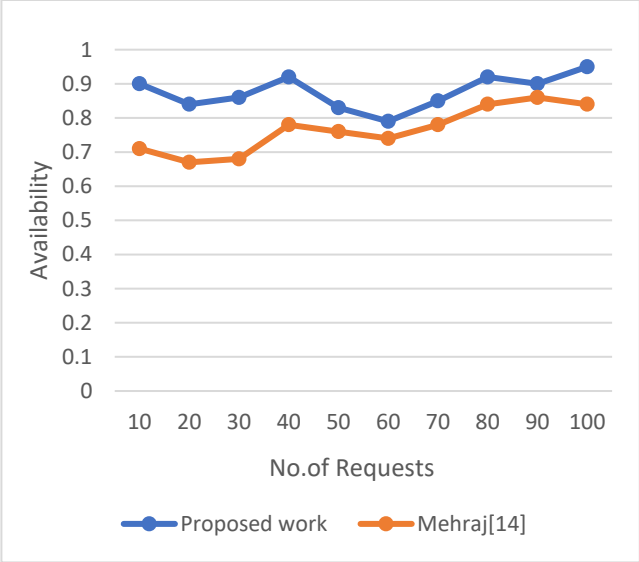

Fig. 4 Availability of cloud resource

experiment, along with some malicious attempts to analyze the proposed system's performance in terms of accuracy, success rate and availability.

Figure 4 depicts a declining availability rate with the increase in requests due to user behavior and its credibility for literature [14]. Behavior value of users changes along with the variation in numerical values. The proposed method has a higher availability rate, and the value changes because of distributed nature of swarms. Hence, the values shown ensure that the proposed work has better availability of the resources in comparison with the existing one.

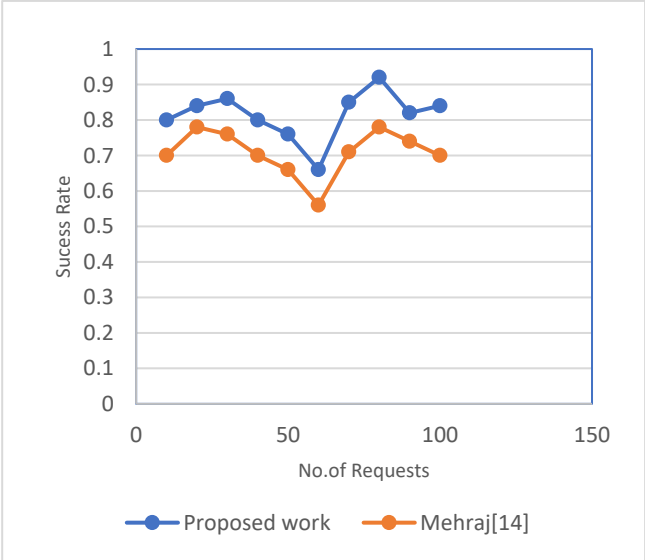

Fig. 5 Rate of successful transactions

The simulated result shown above is the rate of successful transactions. Users whose trust value does not match the threshold have no access to cloud services. Hence, there is a sharp decline in RST at 40 and 60. In both works. Because of the vulnerability of the client's way of behaving, the impact of the client's trust limits isn't quite as steady as cloud service nodes. However, the proposed work has a success rate of 10% more than the existing methodology.

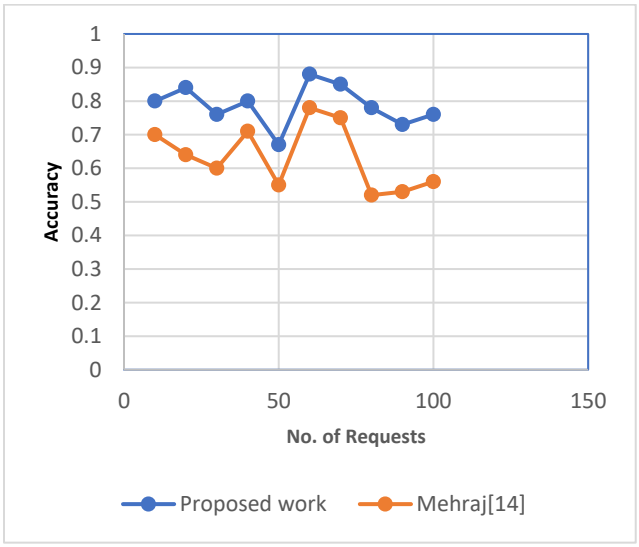

Fig. 6 Accuracy of the system

Fig. 6 Showcases the accuracy and depends on users' credibility. The result clearly shows that the proposed work has better accuracy than the existing one. The accuracy values are linear with the parameters used to calculate the trust value. However, there is a decline in accuracy as CSP create a communication channel based on User trust value.

5. Conclusion

The proposed framework is to build an access control method based on swarm intelligence, i.e., dynamic and swarms work together to maintain a secure and efficient data storage protection system. CSP and CDS trust metrics empower effective information sharing and guarantee a stronger security structure. This approach can efficiently protect the unauthorized access of any malicious attempts, which is evident from the results. In future work, the proposed model can be hybridized with different methodologies to improve the system's efficiency.

References

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," *in Proc. of Iwqos'09*, 2009.

[2] Dillon, T., Wu, C., Chang, E, "Cloud Computing: Issues and Challenges," in: 2010 24th IEEE International Conference on Advanced Information Networking and Applications (Aina). IEEE, pp. 27–33 , 2010.

[3] Krutz, R. L., Vines, R. D, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing," *Wiley Publishing*, 2010.

[4] Cai, F., Zhu, N., He, J., Mu, P., Li, W., Yu, Y, "Survey of Access Control Models and Technologies for Cloud Computing," *Clust.Comput*. vol. 22, pp.6111–6122, 2019. Https://Doi.Org/10.1007/S10586-018-1850-7

[5] Ghaffar, Z., Ahmed, S., Mahmood, K., Islam, H., Hassan, M., Fortino, G, "An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical–Socialsystems," *IEEE Access*, vol.8, pp.47144–47160 , 2020. Https://Doi.Org/10. 1109/Access.2020.2977264

[6] Ilankumaran, S., Deisy, C., "Multi-Biometric Authentication System Using Finger Vein and Iris in Cloud Computing," *Clust. Comput*, vol.22, pp.103–117, 2019.Https://Doi.Org/10.1007/S10586-018-1824-9

[7] Indu, I., Anand, R., Bhaskar, V, "Identity and Access Management in Cloud Environment: Mechanisms and Challenges. Eng. Sci. Technol," *Int. J*, vol.21, no.4, pp.574–588, 2018.Https://Doi.Org/10.1016/J.Jestch.2018.05.010

[8] Joseph, T., Kalaiselvan, S.A., Aswathy, S.U., Radhakrishnan, R.,Shamna, A.R, "A Multimodal Biometric Authentication Scheme Based on Feature Fusion for Improving Security in Cloud Environment," *J. Ambient Intell. Humaniz. Comput*, 2020.Https://Doi.Org/10.1007/S12652-020-02184-8

[9] Kaur, Gurdip & Khurana, Meenu & Sethi, Monika, "Intrusion Detection System Using Honeypots and Swarm Intelligence," 2011. 10.1145/2007052.2007060.

[10] V.Meena, N.Dhivya, "An Access Control System in Cloud Storage With Scalable User Revocation for Sharing Data," *SSRG International Journal of Computer Science and Engineering*, vol.3, no. 9, pp.6-11, 2016. *Crossref*, Https://Doi.Org/10.14445/23488387/Ijcse-V3i9p102

[11] Reddi Narendra Kumar, Behara Vineela, "An Efficient Multi Authority and Privacy of Data Access Control in the Cloud Storage Systems," *SSRG International Journal of Computer Science and Engineering*, vol.3, no. 12, pp.10-13, 2016. *Crossref*, Https://Doi.Org/10.14445/23488387/Ijcse-V3i12p104

[12] Khilar, P., Chaudhari, V., Swain, R, "Trust-Based Access Control in Cloud Computing Using Machine Learning," in: Das, H., Barik, R., Dubey, H., Roy, D. (Eds) Cloud Computing for Geospatial Big Data Analytics, vol.49, pp. 55–79, 2019. Springer Https://Doi.Org/Https://Doi.Org/10.1007/978-3-030-03359-0_3

[13] G. Lin, D. Wang, Y. Bie and M. Lei, "Mtbac: A Mutual Trust-Based Access Control Model in Cloud Computing," in *China Communications*, vol. 11, no. 4, pp. 154-162, 2014, Doi: 10.1109/Cc.2014.6827577.

[14] Mehraj, Saima & Banday, M. Tariq, "A Flexible Fine-Grained Dynamic Access Control Approach for Cloud Computing Environment," *Cluster Computing*, vol.24, pp.1-22. 10.1007/S10586-020-03196-X.

[15] M. Rafiqul Islam and M. Habiba, "Collaborative Swarm Intelligence Based Trusted Computing," *2012 International Conference on Informatics, Electronics & Vision (Iciev)*, pp. 1-6, 2012. Doi: 10.1109/Iciev.2012.6317341.

[16] Md. Rafiqul Islam, Mansura Habiba, "Agent Based Framework for Providing Security to Data Storage in Cloud", Computer and Information Technology (Iccit) 2012 15th International Conference on, pp. 446-451, 2012.

[17] Hajivali, Mostafa & Fatemi Moghaddam, Faraz & Alrshdan, Maen & Alothmani, Abdualeem, "Applying An Agent-Based User Authentication and Access Control Model for Cloud Servers," *International Conference on Ict Convergence*, pp. 807-812. 10.1109/Ictc.2013.6675484.

[18] S. Kalaivani, A. Vikram and G. Gopinath, "An Effective Swarm Optimization Based Intrusion Detection Classifier System for Cloud Computing," *2019 5th International Conference on Advanced Computing & Communication Systems (Icaccs)*, 2019, pp. 185-188, Doi: 10.1109/Icaccs.2019.8728450.

[19] Li, X., Zhou, F., Yang, X, "A Multi-Dimensional Trust Evaluation Model for Large-Scale P2p Computing," *J. Parallel Distrib. Comput*, vol.71, no.6, pp.837–847, 2011.Https://Doi.Org/10.1016/J.Jpdc.2011.01.007

[20] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. De Rose, and R. Buyya, "Cloudsim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms," *Softw.,Pract. Exper.*, vol. 41, no. 1, pp. 23-50, 2010, Doi: 10.1002/Spe.995.

[21] Elmagzoub, M.A.; Syed, D.; Shaikh, A.; Islam, N.; Alghamdi, A.; Rizwan, S, "A Survey of Swarm Intelligence Based Load Balancing Techniques in Cloud Computing Environment," *Electronics*, vol.10, pp.2718, 2021. Https://Doi.Org/10.3390/ Electronics10212718

[22] Pan, I., Elaziz, M.A., & Bhattacharyya, S. (Eds.), "Swarm Intelligence for Cloud Computing (1st Ed.)," Chapman and Hall/Crc, 2020. Https://Doi.Org/10.1201/9780429020582

[23] Lulwah Alsuwaidan, Shakir Khan, Riyad Almakki, Abdul Rauf Baig, Partha Sarkar, Alaa E. S. Ahmed, "Swarm Intelligence Algorithms for Optimal Scheduling for Cloud-Based Fuzzy Systems", Mathematical Problems in Engineering, vol. 2022, Article Id 4255835, pp.11, 2022. Https://Doi.Org/10.1155/2022/4255835

[24] G. Rjoub and J. Bentahar, "Cloud Task Scheduling Based on Swarm Intelligence and Machine Learning," *2017 Ieee 5th International Conference on Future Internet of Things and Cloud (Ficloud)*, pp. 272-279, 2017. Doi: 10.1109/Ficloud.2017.52.

[25] Marcel Chibuzor Amaechi, Matthias Daniel, Bennett E.O, "Data Storage Management in Cloud Computing Using Deduplication Technique," *Ssrg International Journal of Computer Science and Engineering*, vol.7, no. 7, pp. 1-7, 2020. *Crossref*, Https://Doi.Org/10.14445/23488387/Ijcse-V7i7p101

[26] V. A. Lepakshi and C. S. R. Prashanth, "Efficient Resource Allocation With Score for Reliable Task Scheduling in Cloud Computing Systems," *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (Icimia)*, 2020, pp. 6-12, Doi: 10.1109/Icimia48430.2020.9074914.

[27] Pushkar G. Dhande, Dr. Bandu B. Meshram, "Extending Uml to Define Access Control," *Ssrg International Journal of Computer Science and Engineering*, vol. 6, no. 6, pp. 10-16, 2019. *Crossref*, Https://Doi.Org/10.14445/23488387/Ijcse-V6i6p102

[28] Sinkar Yogita Deepak; C. Rajabhushanam, "Privacy Preservation in Cloud Using Glowworm Swarm-Based Whale Optimization Algorithm (Gwoa) With 128 Key Size in Cleveland Database," *International Journal of Advanced Research in Engineering and Technology (Ijaret)*, vol.11, no. 3, pp.410-415,2020-03-31,

[29] Thanga Revathi, S., Ramaraj, N. & Chithra, S, "Brain Storm-Based Whale Optimization Algorithm for Privacy-Protected Data Publishing in Cloud Computing," *Cluster Comput*, vol. 22, pp.3521–3530, 2019. Https://Doi.Org/10.1007/S10586-018-2200-5.