IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

Recommendation system for cloud service on Trust management services

Deepak BN[1],Anusha J[2],Krishnaveni A[3],Karthik R[4]

Assistant Professor, Dept. of CSE(DS),RNS Institute of Technology Bangalore[1]

Assistant Professor, Dept of AIML, Global Academy of Technology Bangalore[2]

Assistant Professor, Dept of CSE(DS),RNS Institute of Technology Bangalore[3]

Assistant Professor, Dept. of CSE(DS), RNS Institute of Technology Bangalore[4]

Abstract: The trust management is challenging issue in cloud computing now a days. The main obstacle for growth and adoption of cloud computing is trust. Though many works has been proposed, the determination of credibility for trust feedbacks is ignored. In this paper, the Cloud Armor, a reputation and recommendation trust management is proposed in which set of functions are provided to delivery of Trust as a Service. Cloud administration faces significant challenge. The Service Level Agreements (SLAs) are facing difficulty in finding trust between cloud service customers and cloud service providers. Buyers' input can be sensible to the cloud administration characteristic to survey.

Keywords: Trust Management,RecommendationTrust,ReputationTrust,CloudService,TrustResults.

I. INTRODUCTION

A formal trust management model is proposed to managing the trust and the properties for cloud environments' SaaS. The time based experience, reputation and recommendation based concept is used for computation of trust. The consumers will provide feedback to relevant service providers with different level of access with respect to data security, service level agreements and performances etc. The trust life cycle consists of three activities with the basic steps: establishment of trust, updating the trust and revocation of trust. It consists of two entities: trust or (i.e., Service provider),trustee(i.e., Customer)and trust model. There two kind of trust: Direct trust and indirect trust. Direct trust is based on self experience and if they there is no direct interaction between two entities then trust is based on recommendation of other entities. Defining the concept of trust is one of the challenging tasks as it consists of many applications causing to divergence in terminology. Trust in simple words can be defined as "Generally, it is said that an entity trusts second entity when the second entity withstands with expectations of first entity".

Trust model is built on certain trust properties and they are as follows:

- Asymmetry: A trust relation is a symmetric a sit does not mean that Y must trust X as X trust Y.
- Reflexivity: the trust is considered to reflexive as each entity believes it self.
- Context Dependence: trust relation will not be generalized to other a sit regarded precise object.
- Scalability: Trust is also scalable as it may change while the period of communication. This change indicates the modification in the trust level which also indicates that change in entities reputation.
- Partial Transitivity: Trust follows transitivity property. Z get recommendation from Y to X only if Y is trust worthy to X and Z is trustworthy to Y. Otherwise the property is said not to be transitive.
- Subjective: Trust is also said to be level of subjective probability.
- Uncertainty: the trust's most important characteristic is uncertainty which indicates the relationship of trust between fuzzy and stochastic entities of strangers.

Time based: time based variant property is satisfied by direct trust.

Consumes usually do the verification of service providers' trust level of before accessing data and services from the cloud. Hence the trust model guarantees cloud service providers' trust worthiness then allow the consumer to access the services and data. The main proposition of the work is trust management modeling for recommendation trust based on space variant evaluation and direct trust based on time variant evaluation. Components of the trust model:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

Trust:

Trust Degree:

Trust represents the trust degree which is evaluated using possible trust values from domain set trust or Ti views trustee Tjas and it is expressed as

$$Td_{ij}(T_i, T_j, S_k, t) \text{where} i \neq j; \qquad 0 \leq Td_{ij}(T_i, T_j, S_k, t) \leq 1 \tag{1}$$

Where kth service is represented as S k and time defined by t.Trust degree value lies between 0 and 1.Direct trust represented as T d divorce commendation trust represented evaluate the trust degree. In the case of new entity joining any cloud environment newly then ignorance value denoted by assigned.

$$\exists Td_{ij}(T_i, T_j, S_k, t) \tag{2}$$

$$Td_{ij}(T_i, T_j, S_k, t) \rightarrow \tag{3}$$

$$Td^{dir}(T_i, T_j, S_k, t) \oplus Td^{recom}(T_i, T_j, S_k, t) \oplus Td^{iv}(T_i, T_j, S_k, t) \tag{4}$$

$$Td_{ij}(T_i, T_j, S_k, t) = \begin{cases} 0, & \text{if} nd = 0, nr = 0 \\ Dt(T_i, T_j, S_k, t), & \text{if} nd \in \{1, 2, \ldots\}, nr = 0 \\ Rt(T_i, T_j, S_k, t), & \text{if} nr \in \{1, 2, \ldots\}, nd = 0 \end{cases} \tag{5}$$

The direct trust degree is represented by Dt (Ti,Tj,Sk,t) and there commendation trust degree is represented by Rt(Ti,Tj,Sk,t) of trust or Tiin the view of trustee Tj regarding the k th service Sk at time t. The values of and gives the direct trust degree number and- nr gives there commendation trust degree number,

TrustRelation:

TABLE1.Satisfactory Level

Level	Label	Trust worthiness
1	No Opinion	$Td = 0$
2	Low Distrust	$0 < Td < 0.5$
3	Medium Trust	$Td = 0.5$
4	High Trust	$0.5 < Td < 1$
5	Complete Trust	$Td = 1$

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

Trust chain In cloud computing system ,the trust chain is evaluated based on the partial transitive properties If

$$\exists T_p, T_q, T_r, T_s, T_t \in Q \tag{6}$$

and

$$Tr_{pq}\langle T_p, T_q\rangle, Tr_{qr}\langle T_q, T_r\rangle \tag{7}$$

Direct trust:

Direct trust is the relationship of trust between the entities having direct communication.In this module, direct trust table is used to maintain the trust of each entity with other entity.The direct trust measures the level of subjective probability with respect to trustee T_j and trust orT_i based on satisfaction level for the service S_k at time of interaction t.The measurement of experience of direct interaction gives the trust degree.

Time based experience:

Direct trust always decays with time. The trust acquired by an entity at time$t$ might get changed as trust attribute at the time $t+\Delta t$.

$$D(T_i, T_j, S_k, t+\Delta t) < D_t(T_i, T_j, S_k, t) \tag{8}$$

The time t_c represents current time and t_l represents last interaction time. The definition of decay function γ is given

$$\gamma(t_c, t_l) = e^{-(\Delta t)K} = e^{-(t_c - t_l)K} \tag{9}$$

Where

$$K \in \{1, 2, 3, \ldots\}, \qquad \gamma(t_c, t_l) \in [0, 1]$$

K helps in determining the decay rate of degree of direct trust with time Δt.If RF_i is the trust ore's reputation factor, then direct trust degree is calculated at current time t_c using

$$Dt_{t_c}(T_i, T_j, S_k, t_{t_c}) = \frac{\sum_{i=1}^{N} \gamma(t_c, t_l) * Dt_t(T_i, T_j, S_k, t_t) + R}{\sum_{i=1}^{N} \gamma(t_c, t_l)} \tag{10}$$

Recommended trust:

The two entities do not have direct interactions, and then their trust relation is based on recommendation by other entity. Recommended trust is used to measure the recommenders' subjective probability set regarding the trustee $T_j$to the trust or T_i for the service S_k by single or more trust chains and represented by

$$R(T_i, T_j, S_k, t) = \frac{\sum_{m=1}^{length} W_{m,m+1}^{-1} * Dt_\gamma(T_m, T_{m+1}, S_k, t)}{\sum_{m=1}^{length} W_{m,m+1}^{-1}} \tag{10}$$

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

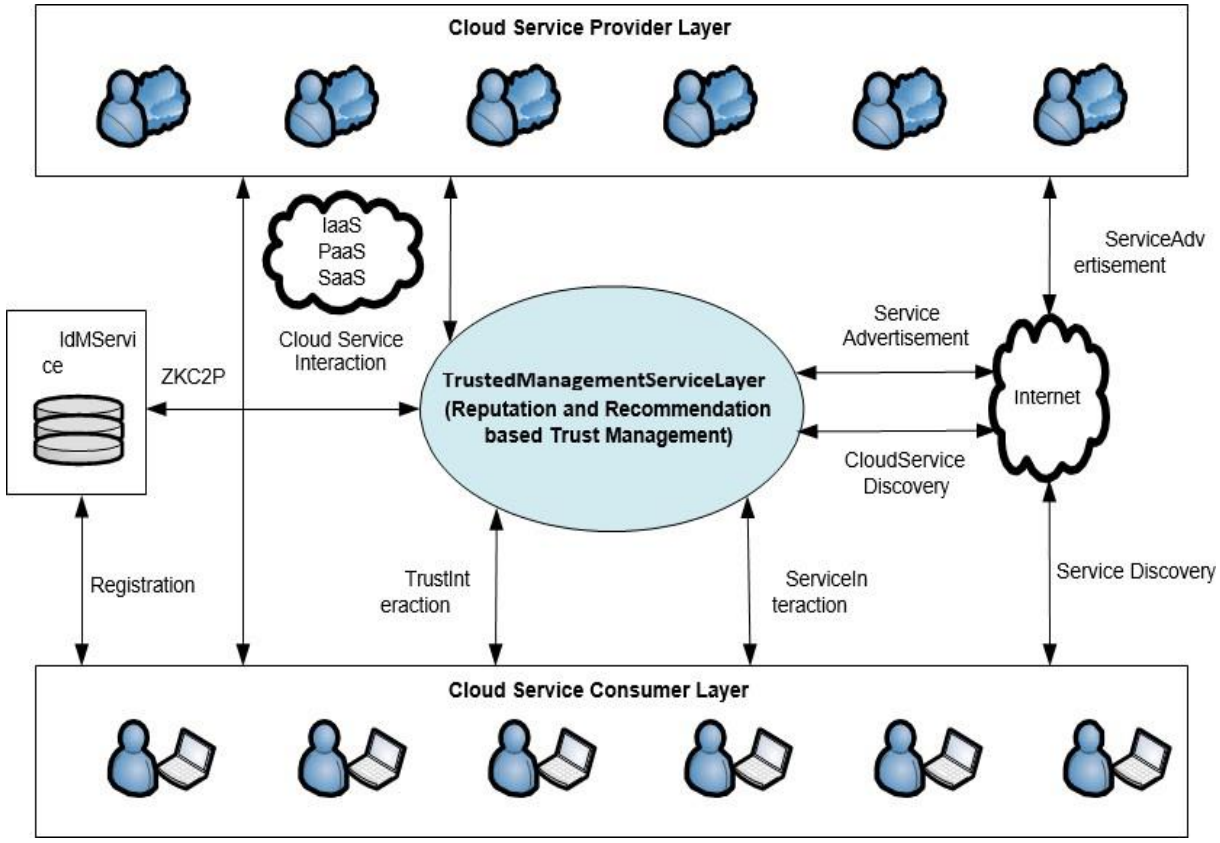

FIGURE1. System Architecture of Proposed Approach

II. METHODOLOGY

The figure shows the architecture of proposed system. The main layers of the proposed work are cloud service consumer, cloud service providers and trust management and are used for Trust as a Service (TaaS). Cloud Service Provider layer consists of cloud service providers offering one or more cloud services i.e., SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) on the Web publicly. Trust Management consists of Trust manager and cloud services. The interfaces are exposed by the trust manager by which user can provide feedback and enquire about the trust result of cloud services .Interaction for cloud service layer includes the discovery to allow users for trust assessment through internet. The trust manager publishes the users' feedback and trust of cloud service. Cloud service consumer layer has variety of users using cloud services. The interactions involved in this are service discovery by users, service and trust interactions for providing feedback and obtaining the trust results of service provider by users. Identity management helps TM for detecting the Sybil attacks. First time users using TM need to register their credentials in IDM to identity to be established. The identity record is maintained for each user. This record consists of user name, credentials attributes like passwords and postal address at the time of registration. Trust manger will assess the trust of requested service provider by the user and gets feedback from user. The trust behavior of cloud service is computed by using users' feedback. This requires user identity, cloud service identity and QoS feedbacks.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

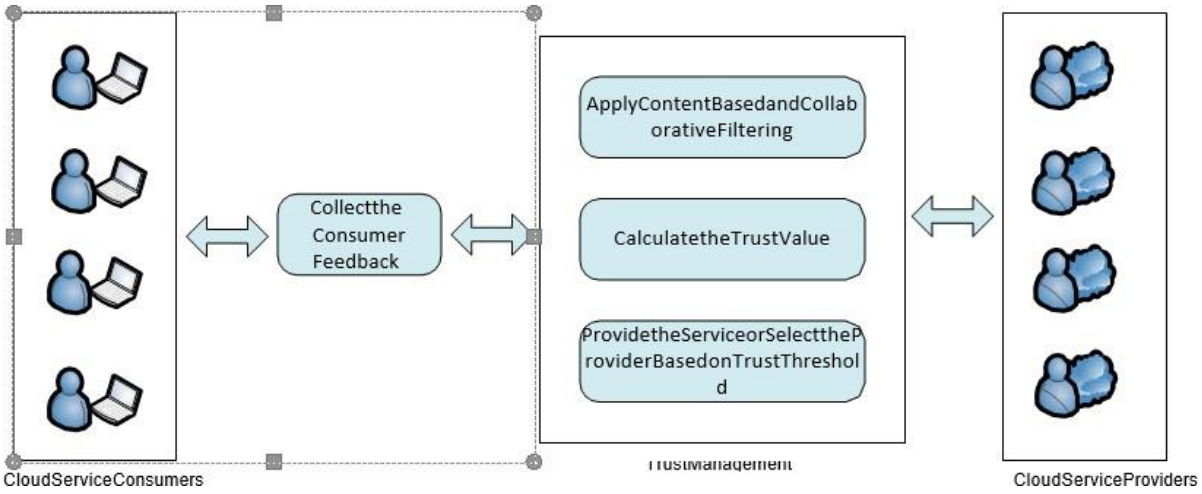

FIGURE2. System Architecture for Recommendation based Trust Management Approach

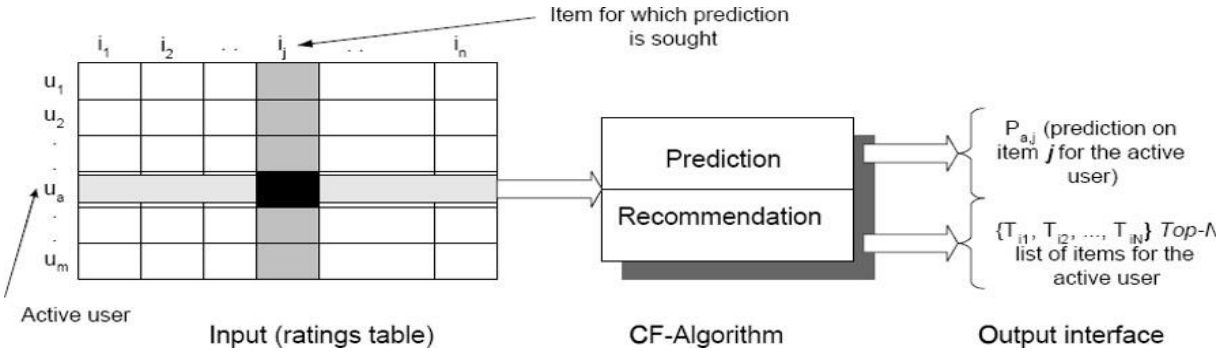

FIGURE3. TheCollaborativeFilteringProcess

The similarity rating of the user is computed as

$$U_r = \frac{A-B}{\sqrt{var(x)var(x_{i-1})}} \tag{13}$$

In the above equations ,x_I represents the rating of i^{th} service provider.

$$\beta = \frac{OF'_s}{OR'_s} \tag{11}$$

The similarity rating of the user is computed as

$$U_r = \frac{A-B}{\sqrt{var(x)var(x_{i-1})}} \tag{15}$$

x_i represents the rating of i^{th} service provider. If users' similarity rating is found to be greater than the mean of

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

$$\alpha = \frac{OF_s}{OR_s} \tag{12}$$

The ratio of failure requested service's from i^{th}user to overall services requested by i^{th}user is the requested service failure ratio. In similar fashion, the ratio of number of other requested service failures by i^{th} user to overall number of other services than the requested by i^{th}user is

$$\beta = \frac{OF'_s}{OR'_s} \tag{13}$$

If users' trust value is found to be higher than threshold then he is assigned to cloud service, if not the user gets terminated from procedure.

Trust Computation

At the initial step, history of services and user requests are collected. Then recommendation system based filter is applied to evaluate the users' similarity rating. The following equations are used for calculation:

$$A = \sum_{i=0}^{n} x_{ii-1} \tag{14}$$

$$B = \sum_{i=0}^{n} x_i \sum_{i=0}^{n} x_{i-1} \tag{15}$$

$$va(x_i) = n\sum_{i=0}^{n} x_i^2 - \left(\sum_{i=0}^{n} x_i\right)^2 \tag{16}$$

$$va(x_{i-1}) = n\sum_{i=0}^{n} x_{i-1}^2 - \left(\sum_{i=0}^{n} x_{i-1}\right)^2 \tag{17}$$

The similarity rating of the user is computed as

$$U_r = \frac{A-B}{\sqrt{va(x)var(x_{i-1})}} \tag{22}$$

In the above equations x_i represents the rating of i^{th} service provider.

If users similarity rating is found to be greater than theme an of similarity rating, jump to next step otherwise terminate the user.

The failure ratio of requested service and others are calculated from below given equations

$$\alpha = \frac{OF_s}{OR_s} \tag{18}$$

The ratio of failure requested service's from i^{th}user to overall services requested by i^{th}user is the requested service failure ratio. In similar fashion, the ratio of number of other requested service failures by i^{th} user to overall number of other services than the requested by i^{th}user is

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

III. RESULTS

We mainly focus on trust value and credibility model to select the service provider and user. The two kinds of malicious behavior considered are Collusion and Sybil attacks. For proposed experiment, the data collected consists of five different cloud service and fifty feedbacks. The collusion attack and Sybil attack were considered and were resolved at time period 60 minutes. The trust result of all users' feedback and trust result of friends' feedback varies. The result is shown in below figure.

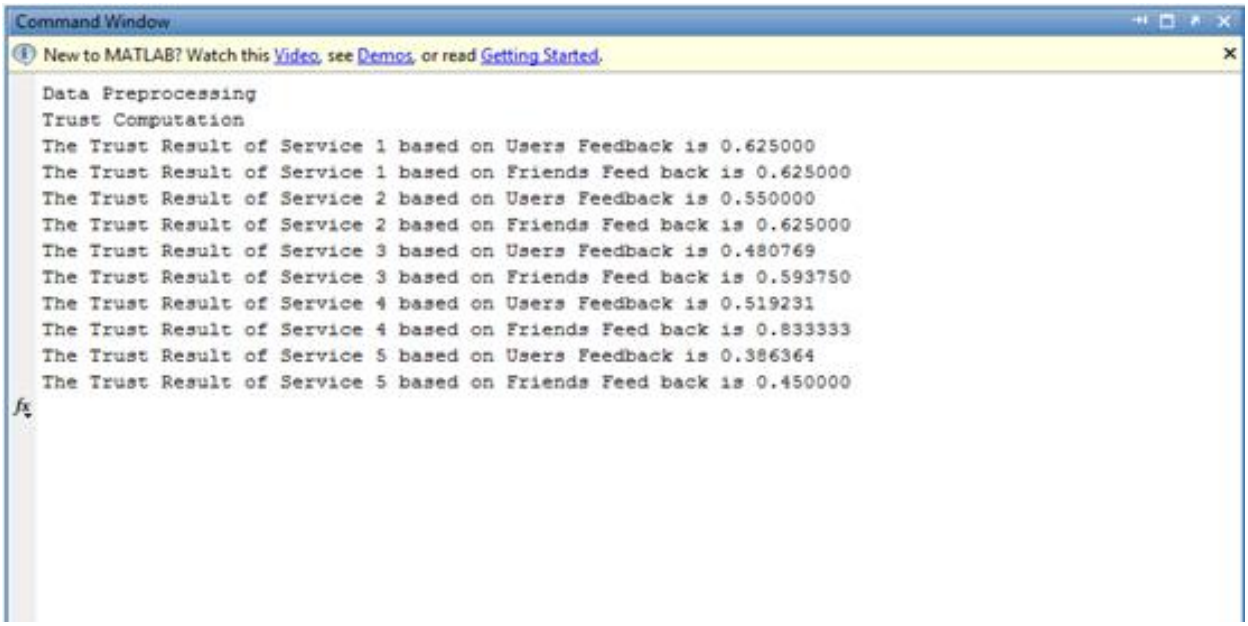

FIGURE4. TrustResultofServiceProviders

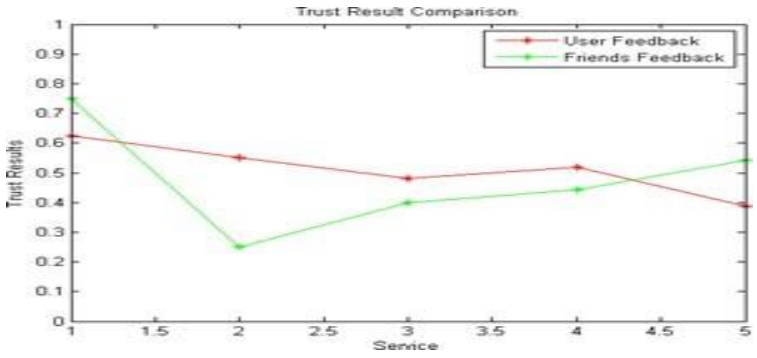

FIGURE5. Reputation and Recommendation based Trust Results

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

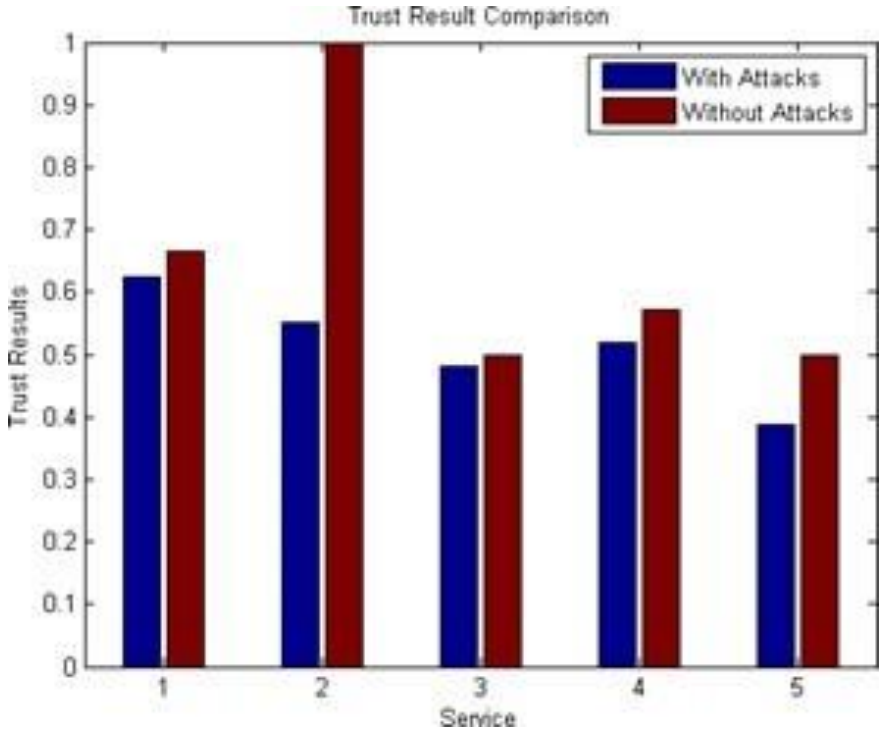

FIGURE6. TrustResultComparison

The result comparison of reputation and recommendation based trust result for service providers is shown in figure 5.The trust results in presence of attacks and in the absence of attacks in the figure6.The analysis of trust management result of service provider is shown in figure 7.

Then the trust assessment for the user is done and result is given to the service providers and is as shown below in figure. The graph in figure shows the credibility of users. The user behavior in the form of trust value and credibility is shown in figure 9.

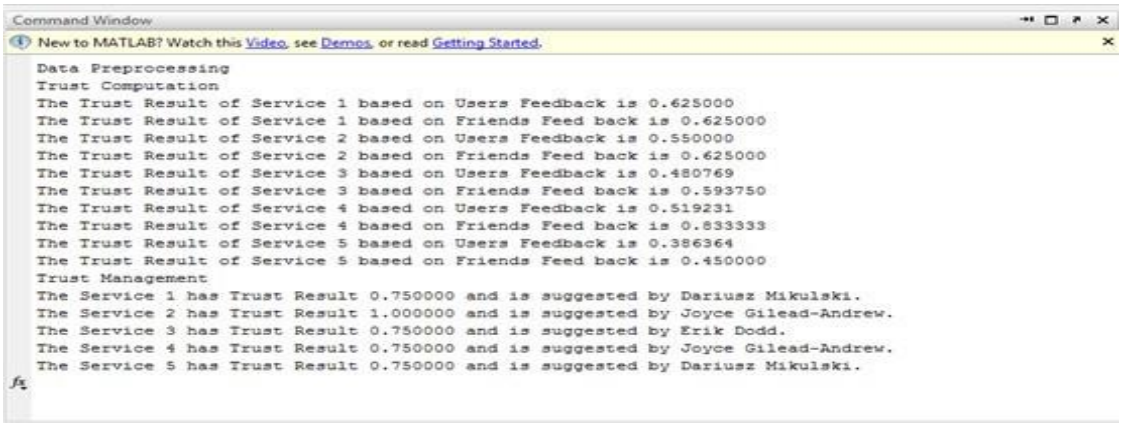

FIGURE7. Reputation and Recommendation based Result

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

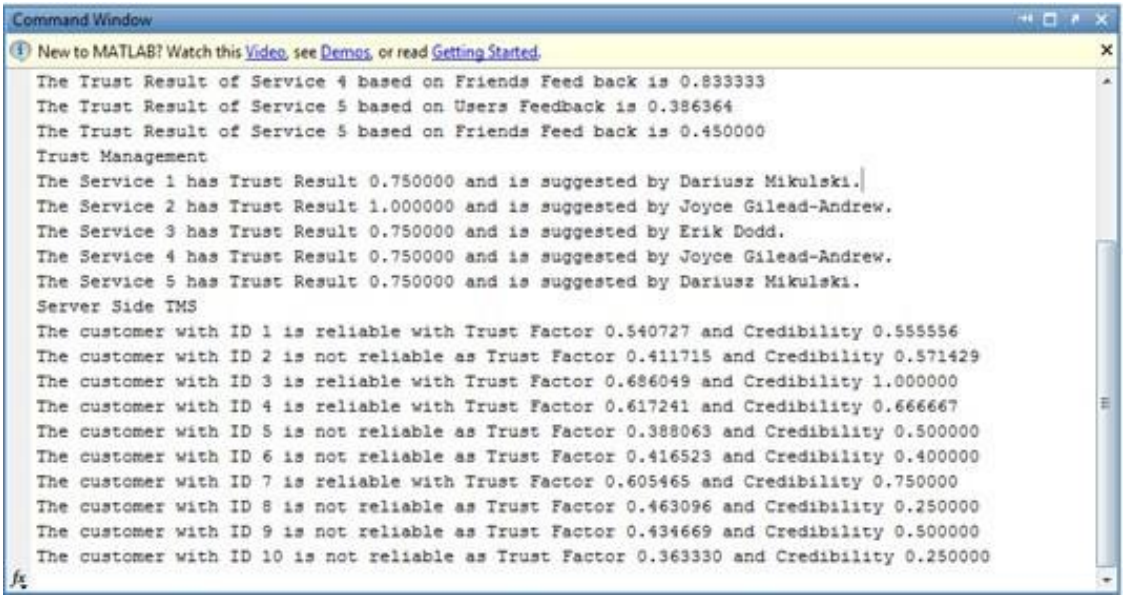

FIGURE8. Users' Trust Result

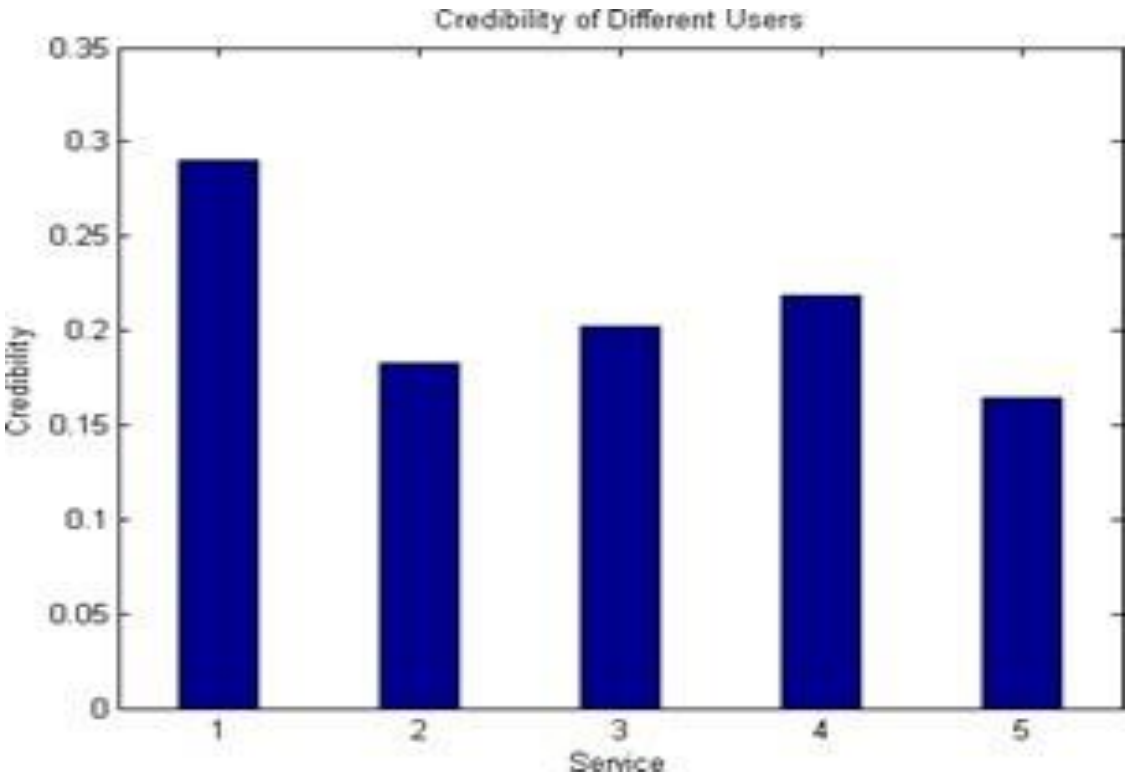

FIGURE9. Credibility of Different Users

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15584

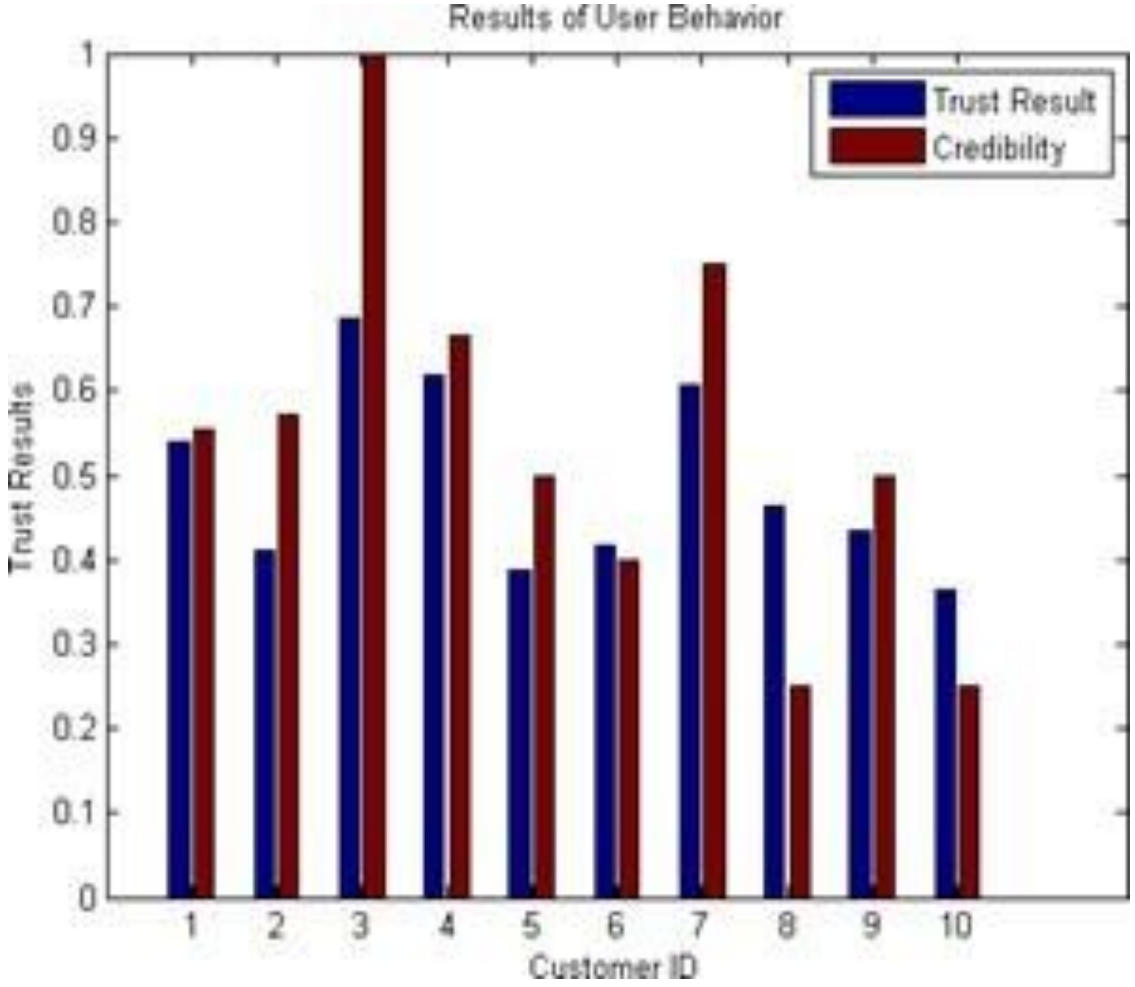

FIGURE10. User Behavior Result

IV. CONCLUSION

From various journal studies, it is concluded that trust-aware recommendation systems improve the accuracy, reliability, and transparency of cloud service selection. These systems help users identify dependable cloud providers while reducing risks associated with malicious feedback, fake ratings, and uncertain service performance. Techniques such as collaborative filtering, fuzzy logic ,machine learning, block chain integration, and reputation-based models are widely used to enhance trust evaluation mechanisms.

Furthermore, trust management frameworks contribute to better decision-making by dynamically updating trust values based on real-time service performance and user experiences. This increases user satisfaction and strengthens confidence in cloud environments. Researchers also highlight that combining trust metrics with QoS parameters provides more effective and personalized cloud service recommendations compared to traditional methods.

DOI: 10.17148/IJARCCE.2026.15584

REFERENCES

1. Talal H. Noor, Quan Z. Sheng, Lina Yao, Schahram Dustdar and Anne H.H. Ngu, "Cloud Armor: Supporting Reputation-based Trust Management for
2. SuganyaandD.Selvam,"CloudArmor Cloud Services", IEEE Transactions on Parallel and Distributed Systems, Volume 0, Issue 0, 2014.:SupportiveandTrustworthyCloudServices",InternationalJournalof Innovative Research in Computer and Communication Engineering, Volume 4, Issue 2, 2016.
3. T. Sandeep and G. Priya, "Reputation Based Trust Management for Cloud Services", International Journal of Pharmacy & Technology (IJPT), Volume 8, Issue 3, pp. 15541–15551, 2016.
4. Muhammad Yasir Siddiqui and Alam Gir, "An Integration of policy and reputation based trust mechanisms", School of Computing, Blekinge Institute of Technology, Master's Thesis, Computer Science Thesisno: MCS-2011-08, January 2011.
5. Subramanian Anbazhagan and Dr.K. Soma sundaram, "CTRAC: A Combined Trust and Recommendation based Access Control Approach for Cloud Computing", Asian Journal of Research in Social Sciences and Humanities, Volume 6, Issue 6, pp. 1824–1841, 2016.
6. S. Nagalakshmi and Dr. Rakesh Poonia, "Towards A Secure And Dependable Credibility-Based Trust Management System In Cloud", International Journal For Technological Research In Engineering, International ConferenceonEmergingTechnologiesinEngineering,Biomedical,MedicalandScience,pp. 162–166,2016.
7. T. Sandeep and G. Priya, "Reputation Based Trust Management for Cloud Services", International Journal of Pharmacy & Technology, Volume 8, Issue 3, pp. 15541–15551, 2016.
8. SriB.LakshmanaRaoandSriB.Veerendra,"SupportingReputation-basedTrustManagementforCloudServices",IJCSIET–InternationalJournalofComputerScienceInformationandEngineeringTechnologies,Volume 2, Issue 5, 2015.
9. Saket Maskara, Mudit Saraf and Priya G, "Trust Management in Cloud Computing", International Research Journal of Engineering and Technology, Volume 03, Issue 11, 2016.
10. KommineniMadhaviandM.VijayKumar,"CloudArmor:ATrustySupportingReputation-basedManagement forCloudServices", International Journal of Applied Sciences, Engineering and Management, Volume04, Issue 01, pp. 20–24, 2015.
11. Badrul Sarwar, George Karypis, Joseph Konstan, and John Ried, "Item Based Collaborative Filtering Recommendation Algorithms", ACM, 2015.
12. Song Jie Gong, "A Collaborative Filtering Recommendation Algorithm Based on User Clustering and Item Clustering", Journal of Software, Volume 5, Issue 7, 2010.
13. T. Sandeep and G. Priya, "Reputation Based Trust Management for Cloud Services", International Journal of Pharmacy & Technology (IJPT), Volume 8, Issue 3, pp. 15541–15551, 2016.
14. Muhammad Yasir Siddiqui and Alam Gir, "An Integration of policy and reputation based trust mechanisms", School of Computing ,Blekinge Institute of Technology, Master's Thesis, Computer Science Thesisno: MCS-2011-08, January 2011.
15. Subramanian Anbazhagan and Dr.K. Somasundaram, "CTRAC: A Combined Trust and Recommendation based Access Control Approach for Cloud Computing", Asian Journal of Research in Social Sciences and Humanities, Volume 6, Issue 6, pp. 1824–1841, 2016.

DOI: 10.17148/IJARCCE.2026.15584

16. S. Nagalakshmi and Dr. Rakesh Poonia, "Towards A Secure And Dependable Credibility-Based Trust Management System In Cloud", International Journal For Technological Research In Engineering, International ConferenceonEmergingTechnologiesinEngineering,Biomedical,MedicalandScience,pp. 162–166,2016.

17. T. Sandeep and G. Priya, "Reputation Based Trust Management for Cloud Services", International Journal of Pharmacy & Technology, Volume 8, Issue 3, pp. 15541–15551, 2016.

18. SriB.LakshmanaRaoandSriB.Veerendra,"SupportingReputation-basedTrustManagementforCloudServices",IJCSIET–InternationalJournalofComputerScienceInformationandEngineeringTechnologies,Volume 2, Issue 5, 2015.

19. Saket Maskara, Mudit Saraf and Priya G, "Trust Management in Cloud Computing", International Research Journal of Engineering and Technology, Volume 03, Issue 11, 2016.

20. KommineniMadhaviandM.VijayKumar,"CloudArmor:ATrustySupportingReputation-basedManagement for Cloud Services", International Journal of Applied Sciences, Engineering and Management, Volume04, Issue 01, pp. 20–24, 2015.

21. Badrul Sarwar, George Karypis, Joseph Konstan, and John Ried, "Item Based Collaborative Filtering Recommendation Algorithms", ACM, 2015.

22. Song Jie Gong, "A Collaborative Filtering Recommendation Algorithm Based on User Clustering and Item Clustering", Journal of Software, Volume 5, Issue 7, 2010.