Journal of Theoretical and Applied Information Technology
31st December 2022. Vol.100. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# PREPUTATION BASED TRUST MANAGEMENT SYSTEM FOR MALICIOUS FOG NODE DETECTION

**R PRIYADARSHINI[1], N MALARVIZHI[2]**

[1]Research Scholar, Department of Computer Science and Engineering , Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamilnadu, India

[2]Professor, Department of Computer Science and Engineering , Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamilnadu, India

E-mail: [1]darshini.sr@gmail.com, [2]drnmalarvizhi@gmail.com

**ABSTRACT**

Fog computing is a geo-distributed computing network; trust must be established between fog nodes for secured data communication. Decision-making can be aided by each nodes' ability to foresee the behaviours of other nodes according to trust value calculated, either directly or indirectly. Especially in indirect trust value calculation, decision to accept the recommending nodes value is critic due to malicious fog nodes which cause internal attacks like self-promotion attack, bad-mouthing attack, and on-off attack. This paper proposes a reputation based trust management system (RTMS) for malicious fog node detection among the recommending fog nodes using geometric probability distribution on multi-dimensional attributes. This RTMS keeps track of the past records of the fog node to calculate the reputation value of each recommender using weighted geometric mean in the fog environment. The proposed technique successfully detects the malicious fog nodes, that are possible among the recommending fog nodes, and allows only the trustworthy node's recommendation for indirect trust calculation, thereby eliminating malicious nodes. The simulation shows that RTMS outperforms the previous work in terms of suitability and security.

**Keywords:** *Fog Computing, Trust Management, Reputation, Weighted Geometric, Internal Attacks*

## 1. INTRODUCTION

Fog computing's main scenario is to increase the efficiency and to reduce the amount of data transferred to the cloud for storing, processing, and analysis. Also fog computing is used for security, performance and business logics. It is used for various applications and services in different industries like smart cities, smart buildings, vehicular networks, IoT and many other like so [1]. Fog computing security issues arise since there are so many devices connecting to fog nodes and at many connecting gateways. Given the number of hops, the data takes, or the number of machines it is copied to or shared with during data transfer, the risk of theft or misuse may be considerable. Although authentication is crucial in creating the initial set of connections between fog nodes in the network, it is insufficient due to the possibility of device failure or vulnerability to malicious attacks. There are different types of cryptographic-based techniques that can successfully stop external attacks, but they are useless against internal threats where rogue fog nodes are already present in the application and using actual identity. Also the flexibility nature of the fog environment complicates the whole structure and trust situation of the fog nodes.

Trust, which symbolizes the association between nodes, is essentially a view about how each node under request will behave in the future. Trust on the other hand can be direct or indirect. Direct trust of a node, deals with its own experience with the other node, whereas the indirect trust specifies the recommendation system i.e., trust is calculated based on the recommendations taken from the other connected nodes[2]. In the recommendation system involving IoT and Fog nodes numerous trust and reputation models have been used in the past, but they are unable to handle recommendations given by malicious nodes, that cause IoT devices to have a high reputation and unfair negative reviews that cause excellent IoT devices to have a bad reputation. So, as a result need a mechanism that determines the reliability of node to provide a trustworthy Quality of Service (QoS) prediction for service recommendation, IoT devices and prevent

the biased recommendations given [2, 3, 4, 5]. The term malicious fog node refers to a fog device that poses as being authentic in order to trap end users into connecting to it. Once a user joins to it, it has total control over the information transported to and from one node to the next giving it the ability to launch attacks immediately. This kind of situation gives rises of internal attacks in the trusted fog environment, where the cryptography methods fail to detect them.

The internal attacks in the trusted fog environment includes [6, 7]:

**Bad-mouthing attack:** This is an example of a collusion attack, which occurs when multiple nodes collaborate to distribute misleading information. Here, the malicious fog nodes join together and provide false information about a good fog node. The reputation of the good fog node will suffer because of this.

**Ballot-stuffing attack:** This is also another type of collusion attack. In these types of attack, a malicious fog node sends good information about another malicious fog node to increase the reputation of the malicious fog node.

**On-off attack:** A fog node, which performs both bad and good services randomly to the other fog nodes intentionally to avoid being labelled as a bad node in the environment.

**Opportunistic service attacks:** A fog node becomes a malicious node when it performs good services when it senses its reputation has dropped to regain its reputation.

**Self-promotion attack:** A malicious fog node gives good information about itself to other fog nodes promoting itself.

The main objective of this paper is to identify the malicious node among the recommending fog nodes in the recommendation as trust management system. A novel method of calculating reputation value of each fog node to be trusted is done based on the weighted geometric mean over the QoS that takes into account both direct trust and indirect trust features including packet forward, packet delivery, packet dropping rates, etc.,. The indirect trust and direct trust are merged using the conventional weighted strategy to determine overall fog node trust. Finally, a clear analysis over the malicious node detection is done. Simulation outcomes for various trust measures with various trust thresholds are presented of this new reputation trust management strategy.

This paper further structured as follows: In Section 2 summarizes the existing and need of malicious node detection in the trusted environment. Section 3 details the proposed methodology. In Section 4 the results and discussion are specified and Section 5 concludes the paper.

## 2. LITERATURE SURVEY

Typical fog nodes in a fog-computing environment include routers, switches, set-top boxes, proxy servers, Base Stations (BS), and other conventional networking hardware. Those can be positioned in close proximity to IoT devices and sensors, which are in involved in data generation.

In [1] the author specified that only a few papers have established the use of security on data communication and storage among the fog nodes. The prerequisites for implementation for secured data include using a public key infrastructure to encrypt communications between the service requesters and service providers in the orchestration framework will be necessary. The danger of theft or misuse may be high given the number of hops the data takes or the number of machines it is copied to or shared with during data transmission. In [8], the author discusses security concerns in a fog environment. The user's information transmitted across numerous networks for analysis, computation, etc., making it vulnerable to many forms of attacks. The likelihood of an attack rises as the data approaches the end devices. Therefore, there is a significant chance that malicious users will reveal data. Trust listed by the author as one of the security concerns in the fog environment and claims that a variety of assaults can be mitigated by adopting different trust management approaches. The difficulty of making the appropriate services available in accordance with user needs has increased demand for service recommendations. The estimation of enhanced QoS values via recommendation algorithms is difficult problem given the enormous development in IoT applications. Recommendation algorithm is suggested by the author in [9] that considers probability distribution into account for collaborative filtering, emphasising the value of rated items and addressing the issue of data non-availability. A collaborative matrix factorization approach for QoS prediction is presented in [10]. Using the proper data, the suggested approach takes into account both factors that are implicitly and explicitly present in the QoS data. In [11] the author demonstrates a technique for service recommendations based on customer requirements using k means clustering. The algorithm used in this work employs distance to analyse asymmetric relationships while taking into account the influence of different item ratings. The author of [12] suggests an online service that makes use of collaborative

filtering and textual data together. The complex relationships between mashups and services are characterised by the integration of invocation communications between mashups, services, and their utilities into a deep neural network. A approach is presented by author [13] that incorporates a clustering-based algorithm with a trust-based collaborative filtering mechanism. To identify individualised clusters using text data, rating information, and implicit data, the K medoids clustering technique incorporates the task similarity computation. For the trust aware collaborative filtering approach, both local and global trust values of the clustered users are combined. Finally, all strategies are merged to personalise QoS prediction and make trustworthy cloud service recommendations. By utilising the hybrid technique described by the author in [14], which combines context-based user similarity and trust computation based on various source feedback mechanisms, IoT devices can employ fog nodes to select the service that best matches their needs. In [15] to handle trust in a fog computing environment, first the key trust criteria is determined and then rank them according to the opinions of the experts. Various sets of the defined trust criteria are applied to both client-to-fog and fog-to-fog application scenarios. In the second stage, the weights of the identified criteria and the sub-criteria are determined. A multi-criteria decision-making (MCDM) problem is thus defined as calculating the relative weighting and order of numerous criteria and their categories. In order to determine how much each of the selected criteria and their categories contribute to a trustee's overall trust score, it is also necessary to prioritise the identified criteria. This is accomplished through the fuzzyAHP method [16], which addresses ambiguity and imprecision in human judgement.

Fog computing involves two-way communication between fog nodes i.e., Fog Service Requesters(FSR) and Fog Service Provider(FSP). As a result, fog computing trust management needs to be bidirectional. Therefore, this study considering two trust management scenarios: FSR-to-FSP and FSP-to-FSR. The recommendation as trust management system is considered for calculating the trust value between both the considered scenarios. To calculate the trust value between FSR and FSP, in recommendation as trust management system, FSR get the recommendation about FSP. On receiving the recommendations, the trust value is calculated. Based on the trust value over the FSP, FSR sends request for the service or denies the request sent. However, there is a compulsion to analyse the recommender, to accept the recommendation value given by it.

Considering the earlier research on the recommendation systems the feedback and rating are the base, which undergo the issue of trustworthiness among the recommenders. The reputation value can be calculated by various methods by direct experience or by learning about others' experiences. In literature, a number of different ways to calculate reputation scores are described, including basic summing, averaging, Bayesian systems, belief models, and flow approaches. In averaging approach, the ratings given by neighbor nodes are processed to calculate the trust value [17]. In basic summation approach, the difference between the total positive and negative scores is calculated [18]. Combining the new score with the prior rating scores used in statistical calculation is the approach used for Bayesian systems for reputation value calculation [19]. Based on the combination of the node's beliefs and uncertainty, the reputation score is calculated by the belief model approach [20, 21]. In flow approach model, the reputation scores are calculated over a series of long chains of iterations, where incoming flow increases reputation value and decreases with the outgoing flow [22, 23].

According to past research, it is clear that a combined strategy that takes into account user similarity taking co-rated products, contextual information, and reliable users that provide an honest recommendation is required for QoS prediction for service recommendation. This study makes an effort to present the pertinent characteristics and metrics necessary for trust calculation as well as their relative significance for selecting the most appropriate and trustworthy recommender node to interact or communicate by considering reputation as trust management system among the recommenders. Here, the proposed methodology helps us to share the data only with the trusted node by detecting the malicious node among the recommenders, based on the trust metrics related to past transactions of each fog node for differentiating between normal and malicious node based on the reputation value acquired for the acceptance of recommendation value given by the recommending nodes.

## 3. PROPOSED METHODOLOGY

This paper proposes a Reputation Trust Management System (RTMS) to identify the malicious fog node in the fog-computing environment, where the trustworthiness of nodes involved in the recommending network is

considered. The reputation value calculated is used to determine the nodes trustworthiness. The nodes behaviour, based on the reputation value determined by the responses to request queries sent from fog service requesting (FSR) node on fog service providing (FRP) node. The recommending nodes past transaction data are gathered using parameters based on trust metrics among the connected devices in neighbourhood are used to evaluate the reputation value of each fog node. Each fog node works as a monitor node, assessing the trustworthiness of all the neighboring fog nodes with whom it interacts. The reputation value is determined by observing the neighboring fog node activity among the recommending fog nodes. Based on the reputation value calculated the behaviour of the recommending fog nodes are classified as trusted or malicious fog node. Figure. 1 shows the fog environment data sharing among different nodes where trust management system is been implemented. Table 1. list the trust metrics considered.

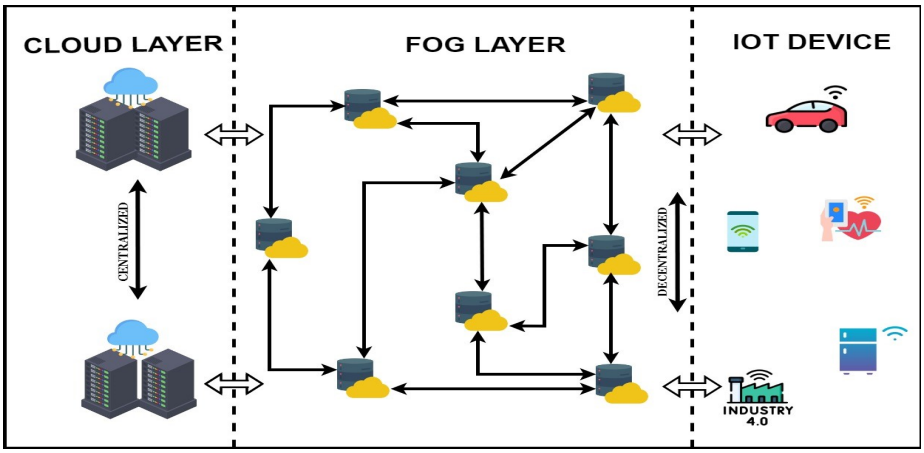



*Figure. 1 Fog Environment*

*Table 1: List of Trust Metrics*

| TRUST METRICS |
|---|
| Packet Forwarding Rate |
| Packets Delivery Rate |
| Packet Dropping Rate |
| Control Packet Generating Rate |
| Packet Sending Rate |
| Packet Acknowledgment Rate |

The proposed work is an enhancement of the existing works that uses the node's characteristic as the trust metrics to calculate the reputation value. From the existing the reputation value is calculated based on the ranks, feedbacks or ratings collected directly and indirectly. In the proposed RTMS, each trust metrics has its own importance, because a node's core functional qualities cannot be compromised. A node's trust metric levels can be used to determine its primary functionality, to maintain this trust metrics of the node should therefore to be maintained above the base value level. As a fact, if a nodes characteristic failing to produce this base value will not be properly contributing to the reputation value calculation.

The proposed novel RTMS trust model is a decentralized trust scheme, ie, the trust functionalities are distributed across the node. Each fog node is a monitor node, which collected required trust metrics and computes the reputation value over the collected data of the neighbouring fog nodes. Here, each fog node in the network will keep record of each of its neighbouring nodes as database. This record includes data on various trust metrics, or QoS attributes, for all of its neighbours in relation to the number of network events that have happened. This implies that the trustworthiness of each node is assessed using both direct and indirect trust. When there have been few or no direct exchanges, the indirect knowledge may be especially helpful.

The stated trust metrics data for various occurrences are crucial and can give the system useful values in order for RTMS to make the best decisions. Depending on the application, base values for all trust metrics are fixed, so that no trust metric data is blindly accepted. This is one of suggested RTMS model's key benefit over competing models. Utilizing a weighted geometric mean of all distinct trust measures for all network events that took place on that specific fog node, our trust management system determines the reputation

value. These trust measurements are different from the fog nodes in their immediate proximity in terms of trust metrics. Each fog node will subsequently have a distinct record of details about each surrounding node in various trust metrics for various network events. Based on these records, the weighted geometric mean of the QoS attributes, as shown in the equation (1), is used to calculate reputation value (Rv). Since the weighted geometric mean depicts a scenario, in which a lack of one variable will affect the overall outcome and this cannot be comprised with the presence of other variable. The weightage for the QoS metrics are specified over the priorities of the trust metrics in the application taken.

$$Rv = \left(\prod_{i=1}^{n} M_i^{w_i}\right)^{1/\sum_{i=1}^{n} w_i} \quad (1)$$

where,
M - Trust Metrics of QoS
n - Number of trust metrics
$w_i$ - Weight given for the corresponding trust metric

The likelihood that a discrete random variable, X, will exactly match some value, x, can be described as the probability mass function. The following is the formula for the geometric distribution PMF:

Comparing this model to the existing, it enables us to distinguish between trusted and malicious fog nodes in the neighborhood by determining the reputation value of all fog nodes. Using this strategy, we can prioritize the trust metrics based on the needs of the application. As mentioned in existing literature [16-23] the trust value is calculated giving importance to the feedback and ranking value given by the recommended fog node, which itself can be a victim of internal attack. Therefore, it is unable to identify the malicious nodes. However, using RTMS trust model, a different solution will be found as one of the trust metrics failed to establish a trustworthy relationship, and the node will be regarded as malicious. Only when the value of Rv for a certain trust metric is greater than or equal to the threshold value (Th), trustworthy association between two fog nodes arise accordingly. Figure. 2 gives the flow of action for accepting the recommendation from the trusted neighboring fog node only, using RTMS.

By mathematical representation (2), Direct trust of a fog node DT(FN) and Indirect trust of a fog node ITD(FN) can be specified as,

Trust (FN) = Average [DT(FN), IDT(FN)] (2)

Let us assume a set of fog nodes say A, B, C, D, E, F, G, H and I in the recommendation trust management system as in Figure. 3.

Here, we need to find the trust value of FSP done by FSR, i.e., fog node A (FSR) for its IDT evaluation over the fog node B (FSP). The fog node A collects the recommendation from its neighboring fog nodes over the fog node B. Before accepting the trust values, it checks for the reputation value (Rv) over them to proceed. In the assumed environment H,G and C are neighboring nodes. To accept the trust values of T(A,H), T(A,G), and T(A,C), for the purpose of calculating the Trust(FN). The fog node B collects the history of the recommenders, based on the QoS trust metrics. The trust metrics values gathered by each fog node on neighboring fog node in its database by checking its base value is used to calculate the reputation value, where weighted geometric mean is applied and attained value is compared with the threshold value(Th) and the malicious fog nodes are identified and their recommendations are rejected.

$IDT(A,B) = \Sigma$ T(neighboring fog nodes) / No. of fog neighboring nodes (3)

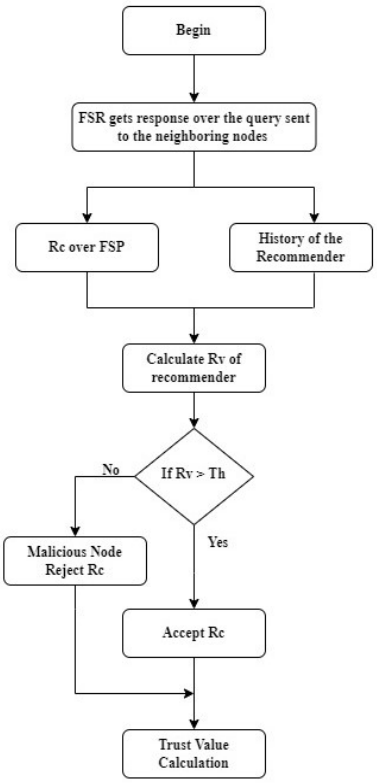



*Figure. 2 RTMS Flowchart*

This RTMS process pre-sets a threshold value Th, the acceptable behaviour levels based on the parameters considered. It is observed if these levels are exceeded or not exceeded. This mainly focus on the taken parameters under considered circumstance as normal behaviour. If the value get exceed the consideration then is called abnormal behaviour of the node, leading to the disbelief of the node.

In our assumed circumstances in Figure. 3 the fog nodes H,G and C are to be checked for their reputation before their given recommendation is accepted. Based on RTMS methodology, it checks the reputation value generated over the considered trust metrics, regarding the neighboring fog node i.e., metrics of H,G and C. Here, Rv is the reputation value evaluated by fog node A over the fog node H. If the RTMS produces the Rv with in the pre-set threshold then the fog nodes reputation is not satisfied, and its recommendation is rejected i.e., fog H recommendation over the fog node B is rejected. Suppose the generated Rv is above the threshold set then the recommendation of the fog node H over the fog node B is accepted for the IDT calculation.

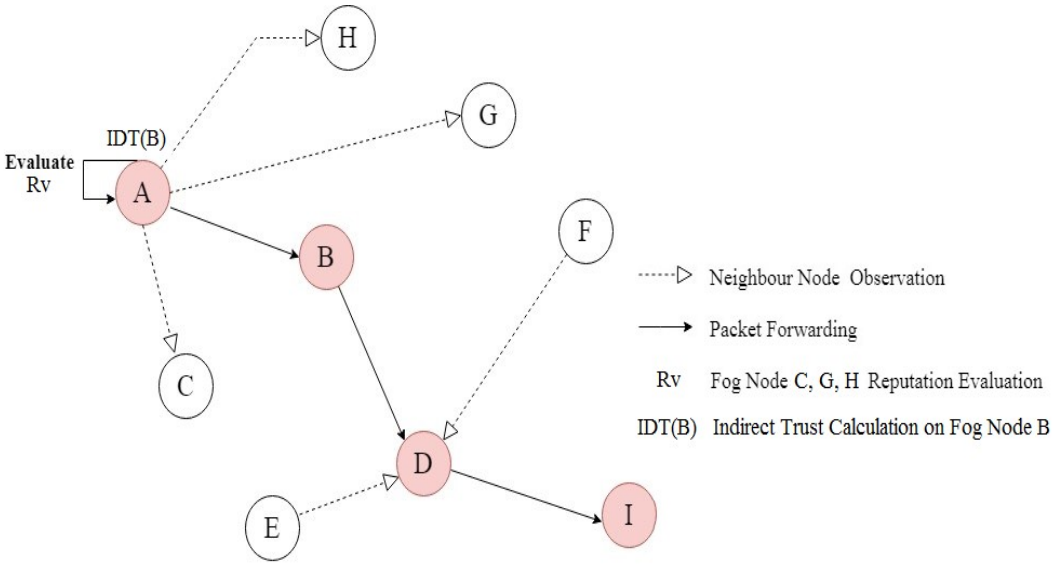



*Figure. 3 Indirect Trust Value Evaluation Process*

The below algorithm captures the details of functionality of RTMS:

```
for all neighboring fog nodes (FN)
{
    from the Metrics in the database
    Calculate Rv
    if(Rv > Tth)
{
    return: trusted fog node='Yes';
    Accept
        the recommendation from the trusted node
}
  else
  return: trusted fog node='No';
  reject
      the recommendations from the untrusted node
  Mark
      the untrusted fog node as Malicious nodes
}
Update
      the fog node database with the decision taken
Repeat
     the procedure for all the neighboring fog nodes
```

## 4. RESULTS AND DISCUSSION

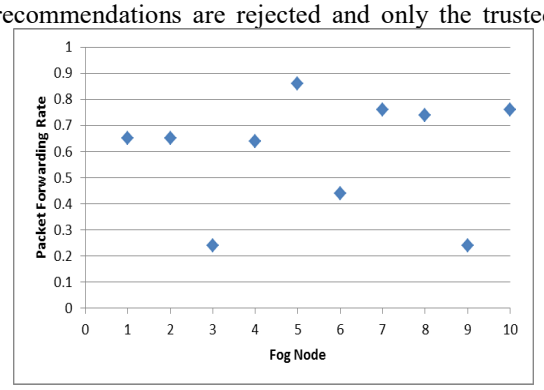
To evaluate the performance of above specified proposed model, we performed simulation experiments in OMNeT++ with FogNetSim++ simulation tool. This model was set up with various trust metrics including Packet Sending Rate, Control Packet Generating Rate, Packet Dropping Rate, Packet Forwarding Rate, Packets Delivery Rate and Packet Acknowledgment Rate for each fog node. The environment is set up with 10 fog nodes in neighborhood acting as recommender to the FSR and their packet transmitting details are considered as the primary constraints. In Figure. 4 clearly

shows the performance of the each fog node by means of packet forwarding.

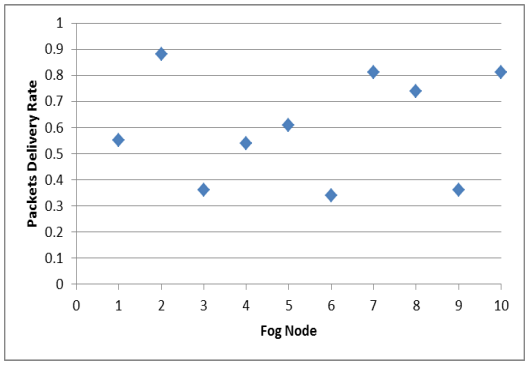
Comparison of proposed with existing method:

According to the proposed RTMS algorithm, it requires the threshold value (Th) to be pre-set according to the application adapted. The calculated Rv value based on (1) is been analysed based the Th value specified. Therefore, in the simulated environment the default threshold value is set to 0.5 with equal opportunistic of trust and distrust. Figure. 5 shows the malicious node detection based on the Rv value calculated. Figure. 6 shows comparison of with and without RTMS, which clearly specifies the detected nodes recommendations are rejected and only the trusted fog nodes recommendations are taken in consideration for the calculation of IDT(FN).

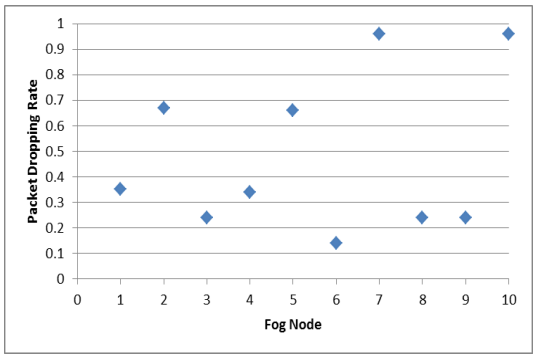
The proposed work RTMS alone analyses the history of each recommending node based on network parameters as QoS, it is plainly capable of defeating internal attacks like badmouthing attack, collusion attack, and ballot-stuffing attack. False information provided about the requesting node is the primary factor in each attack. Since each node's performance constitutes a significant portion of the input provided by a base value specified for the recommender's eligibility, RTMS adheres strictly to this requirement. The weighting assigned to each measure aids in the identification of malicious nodes.



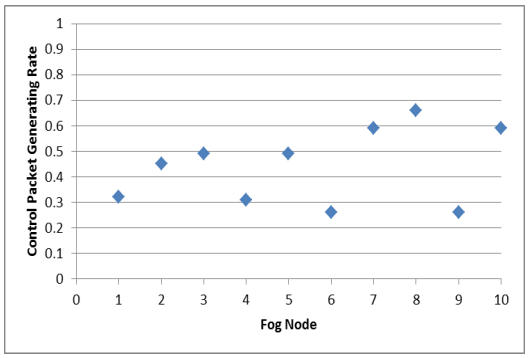

*a) Packet Forwarding Rate*



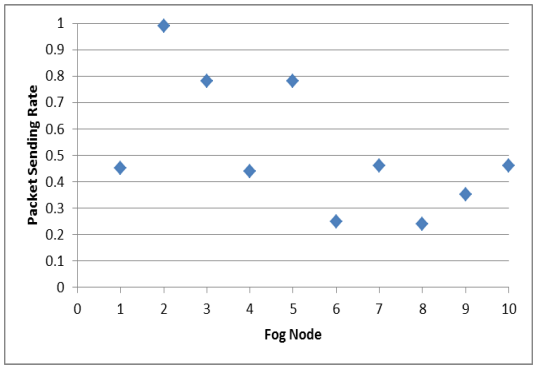

*b) Packet Delivery Rate*



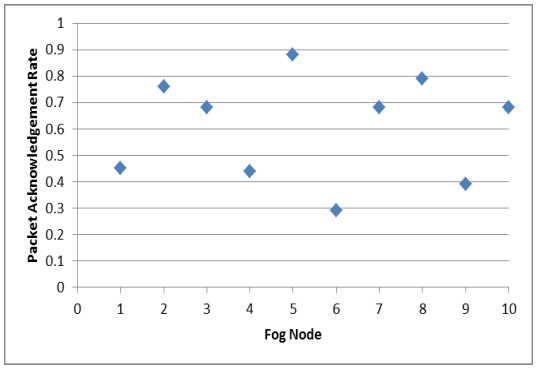

*c) Packet Dropping Rate*




*d) Control Packet Generating Rate*




*e) Packet Sending Rate*




*f) Packet Acknowledgement Rate*

*Figure. 4 Trust metric of Recommender Fog Nodes*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

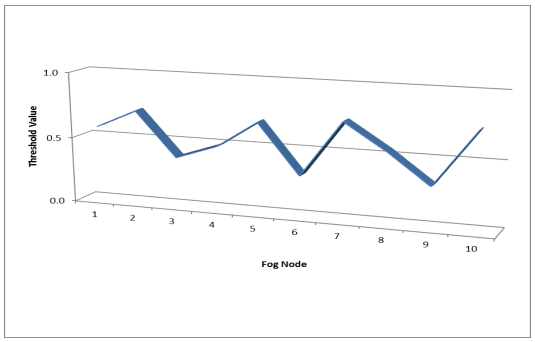



*Figure.5 Malicious Node Detection using RTMS*

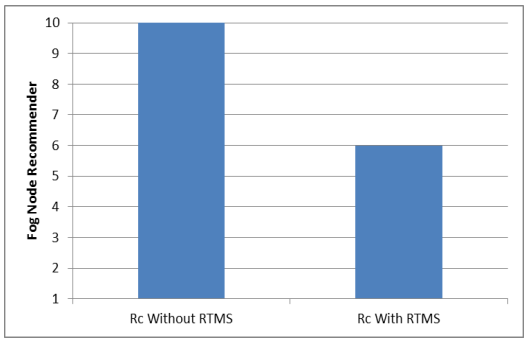



*Figure. 6 Comparison with and without RTMS*

## 5. CONCLUSION

The trust management system proposed in this paper in fog computing environment to provide trust among the recommending fog nodes depending on the QoS characteristics in the fog network. This approach is suggested as a solution to this problem because the recommendation-influenced trust management system must be capable of detecting internal attacks. The proposed RTMS is used to detect malicious fog nodes, which are already in trusted network, to reject its contribution for indirect trust value calculation. The weighting of several trust metrics on QoS features, the base value determined for each metric, and the aggregate threshold value over the estimated reputation value are used to determine each fog node's reputation. By changing the trust metrics, the base value, and the overall reputation threshold, the RTMS have focused on how the trusted relationships vary among the fog nodes. In future, the enhancement of the work will focus on assessing the effectiveness of this trust management model over various other internal attack, and model comparisons. We will also compare the security and privacy solutions of the Fog with those of other similarly distributed environments, such as mobile computing and edge computing, and present these security issues and appropriate solutions for the Fog. We will also look into and categorize the threat models and Blockchain technology usage in fog computing.

## REFERENCES:

[1] Costa, Breno, Joao Bachiega Jr, Leonardo Rebouças de Carvalho, and Aleteia PF Araujo. "Orchestration in fog computing: A comprehensive survey." ACM Computing Surveys (CSUR) 55, no. 2, 2022, 1-34.

[2] Ogundoyin, Sunday Oyinlola, and Ismaila Adeniyi Kamil. "A trust management system for fog computing services." Internet of Things 14, 2021, 100382.

[3] Rathee, Geetanjali, Rajinder Sandhu, Hemraj Saini, M. Sivaram, and Vigneswaran Dhasarathan. "A trust computed framework for IoT devices and fog computing environment." Wireless Networks 26, no. 4 2020, 2339-2351.

[4] Anakpa, Manawa, Yuyu Yuan, and Ghazaros Barseghyan. "A modified Bayesian trustworthiness evaluation method to mitigate the effect of unfair ratings." Mathematical Problems in Engineering, 2018.

[5] Vithanwattana, Nattaruedee, Glenford Mapp, and Carlisle George. "Developing a comprehensive information security framework for mHealth: a detailed analysis." Journal of Reliable Intelligent Environments 3, no. 1 2017, 21-39.

[6] Priyadarshini, R., N. Malarvizhi, and E. A. Neeba. "A study on capabilities and challenges of fog computing." Novel Practices and Trends in Grid and Cloud Computing. IGI Global, 2019. pp. 249-273.

[7] Abidoye, Ademola Philip, and Boniface Kabaso. "Energy-efficient hierarchical routing in wireless sensor networks based on fog computing." EURASIP Journal on Wireless Communications and Networking 2021.1, 2021: 1-26.

[8] Kaur, Jasleen, Alka Agrawal, and Raees Ahmad Khan. "Security issues in fog environment: a systematic literature review." International Journal of Wireless Information Networks 27.3 2020, pp. 467-483.

[9] Deng, Jiangzhou, Junpeng Guo, and Yong Wang. "A Novel K-medoids clustering recommendation algorithm based on probability distribution for collaborative filtering." Knowledge - Based Systems 175, 2019, 96-106.

[10] Wu, Hao, Kun Yue, Bo Li, Binbin Zhang, and Ching-Hsien Hsu. "Collaborative QoS

prediction with context-sensitive matrix factorization." Future Generation Computer Systems 82, 2018, pp. 669-678.

[11] Guo, Liangmin, Kaixuan Luan, Xiaoyao Zheng, and Jing Qian. "A service recommendation method based on requirements for the cloud environment." Journal of Control Science and Engineering 2021.

[12] Xiong, Ruibin, Jian Wang, Neng Zhang, and Yutao Ma. "Deep hybrid collaborative filtering for web service recommendation." Expert systems with Applications 110, 2018, 191-205.

[13] Liu, Jian, and Youling Chen. "A personalized clustering-based and reliable trust-aware QoS prediction approach for cloud service recommendation in cloud manufacturing." Knowledge-Based Systems, 174, 2019, pp. 43-56.

[14] Hallappanavar, Vijay L., and Mahantesh N. Birje. "Prediction of quality of service of fog nodes for service recommendation in fog computing based on trustworthiness of users." Journal of Reliable Intelligent Environments 8, no. 2 (2022): pp. 193-210.

[15] Hallappanavar, Vijay L., and Mahantesh N. Birje. "Prediction of quality of service of fog nodes for service recommendation in fog computing based on trustworthiness of users." Journal of Reliable Intelligent Environments 8, no. 2, 2022, pp. 193-210.

[16] Ogundoyin, Sunday Oyinlola, and Ismaila Adeniyi Kamil. "A Fuzzy-AHP based prioritization of trust criteria in fog computing services." Applied Soft Computing 97, 2020 106789.

[17] Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43, no. 2, pp. 618–644, 2007.

[18] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system," in The Economics of the Internet and E-Commerce, ser. Advances in Applied Microeconomics, M. R. Baye, Ed. Elsevier Science, 2002, vol. 11, pp. 127–157.

[19] Mui, Lik, Mojdeh Mohtashemi, and Ari Halberstadt. "A computational model of trust and reputation." In Proceedings of the 35th annual Hawaii international conference on system sciences, IEEE, 2002. pp. 2431-2439.

[20] Whitby, Andrew, Audun Jøsang, and Jadwiga Indulska. "Filtering out unfair ratings in bayesian reputation systems." In Proc. 7th Int. Workshop on Trust in Agent Societies,2004.

[21] Josang, "A logic for uncertain probabilities," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, vol. 9, no. 3, pp. 279–212.

[22] Whitby, Andrew, Audun Jøsang, and Jadwiga Indulska. "Filtering out unfair ratings in bayesian reputation systems." In Proc. 7th Int. Workshop on Trust in Agent Societies, vol. 6, 2004. pp. 106-117.

[23] L. Page, S. Brin, R. Motwani, and T. Winograd, "The pagerank citation ranking: Bringing order to the web," in Proceedings of the 7th International World Wide Web Conference, Brisbane, Australia, 1998, pp. 161–172.

[24] K. Kurbel and I. Loutchko, "Towards multi-agent electronic marketplaces: what is there and what is missing?" Knowledge Eng. Review, vol. 18, no. 1, 2003, pp. 33–46.