

# Bi-directional trust management system in fog computing using logistic regression

Ramamurthy Priyadarshini, Nandagopal Malarvizhi

Department of Computer Science and Engineering, Veltech Rangarajan Dr. Sagunthala R&D Institute Science and Technology, Chennai, India

---

## Article Info

### Article history:

Received Jun 4, 2022

Revised Sep 28, 2022

Accepted Oct 14, 2022

---

### Keywords:

Fog computing

Logistic regression

Recommendation system

Subjective logic

Trust management

---

## ABSTRACT

Fog computing is a decentralised computing infrastructure that brings data, storage, computation, and communication resources closer to end users by extending typical cloud computing services to the network edge. A fog node can serve another fog node based on their processing power allowing fog-to-fog interaction. Fog nodes, being independent must be trusted for delegation because they collect sensitive data and share with other discrete fog nodes, where standard cryptographic solutions are ineffective against the internal attacks tossed by rogue fog node. This paper proposes a Bi-directional trust management system for secure transactions and fog-to-fog collaboration to address this problem in a fog environment, which allows a service requester to assess a service provider's trustworthiness and the service provider to assess the service requester's level of trust before beginning a connection. This trust management system works based on the recommendation system, which is estimated using logistic regression by fog service provider and subjective logic by fog service requester for the establishment of secured connection between them. Using quality of security parameters, the proposed work yields the result of decision making between the fog service requester and fog service provider.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



---

## Corresponding Author:

Ramamurthy Priyadarshini

Department of Computer Science and Engineering

Veltech Rangarajan Dr. Sagunthala R&D Institute Science and Technology

Chennai, Tamil Nadu, India

Email: darshini.sr@gmail.com

---

## 1. INTRODUCTION

Fog computing is a kind of edge computing that extends the cloud to devices at the edge of a network and is characterized by low latency, high mobility, geographical dispersion, location awareness, and a dynamic environment. In the three-tier design, the fog-computing environment is between the cloud and the edge. With the aid of fog computing [1], [2], the computational, storage, and control functions may be dynamically shifted among various entities. The Fog's connection between the Cloud and the Edge nodes is shown in Figure 1. In certain cases, many Fog hubs or frameworks might collaborate to provide a single application with the best possible support. Examples of this include the ability for many Fog systems to collaborate on data and processing tasks for a variety of users and programs. It is also possible for many Fog nodes or systems to cooperate to act as backups for one another. The fog, being a geo-distributed computer network consisting of numerous heterogeneous devices, requires trust among its nodes in order to ensure the safe transfer of sensitive information. To create a reliable fog environment, trust between nodes is required. With confidence, nodes in the network may anticipate the actions of other nodes, which improve the quality of decisions made by the network as a whole [3]-[6].

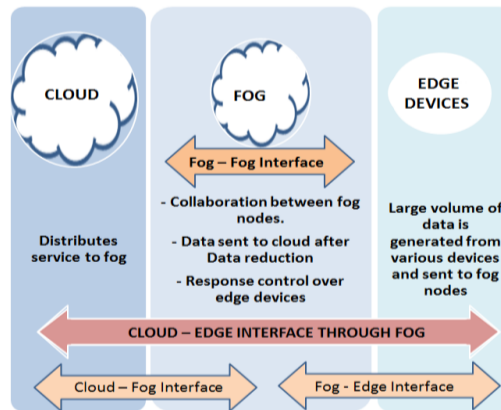


Figure 1. Fog, cloud, and things interface

Trust is the assurance one feels for other based on their behavior and interactions in the present and recent past. At the time of calculating trust values for every given element, it is necessary to verify the relevance of a set of predefined characteristics that influence how people perceive it [7], [8]. Trust are distinguished as: direct trust and indirect trust. Direct trust relations are calculated based on some underlying logic, which may be based on both historical data and present beliefs. Relationships of indirect trust are those in which the trusting party must consider offers from other entities. It is important to take any lingering uncertainty or skepticism into account when making a final determination on the reliability of a certain component. Based on policy, recommendation, reputation, and prediction, areas of information resource are crucial to trust [9].

Planning trusted security frameworks relies heavily on defining suitable trust model parameters through the use of relevant scientific equations for assessing trust values [10], [11]. Extensive studies on trust models in various contexts have been conducted by several scholars. An exhibit will be presented on coordinated cloud design for fog, with the aim of bolstering the safety and protection afforded by fog applications. Zissis and Lekkas [12] Security in the cloud was brought up as an issue that needs a fundamental view, from which security can be built on trust, increasing confidence to an outsider who can be trusted. They have typified the extraordinary difficulties of distributed computing that amplify cloud security and protection problems. Another evidentiary trust paradigm for open distributed systems is suggested in [13]. This model was predicated on the notion of a strengthened D-S evidence theory, which was presented in the form of a time productivity factor figuring capacity and a revised set of D-S fusion rules. Lightweight trust management based on subjective reasoning was developed in [14] to boost trust and security in linked clouds. The backbone of their platform is a set of SLAs that define the quality of the cloud services provided by different providers. Trust in the cloud may also be assessed by comparing rankings over fog nodes [15].

It is very efficient at identifying bad nodes and protecting them from viruses. LogitTrust was presented by Wang *et al.* [16] as a trust assessment method for use in mobile ad hoc networks (MANET). When a service consumer is aware of MANET-specific constraints, such as low energy availability or limited processing power, they may evaluate the provider's actions accordingly. In addition, the model is constructed by fusing the individual object's history with that of other objects in the network. The proliferation of Fog computing applications raises a variety of security concerns and other issues that have not yet been adequately addressed. Since fog computing is a good platform for a range of essential IoT services and applications, such as linked cars, smart grids, smart cities, and smart hospitals, researchers have concentrated on enhancing its security [17], [18]. Fog computing has inherited some security flaws from cloud computing, including the man-in-the-middle attack, which can be addressed with an authentication scheme, and physical tampering, in which data is obtained without the user's knowledge [19]-[21]. Authentication and trust are the two fundamental security concerns in fog computing [22]. This is obvious from the solutions already in place across several sectors, which show that authentication is essential for establishing a connection between fog devices and nodes. Both of these problems may be solved with a reliable trust model [23]-[25]. Using recommendations as a TM technique, this research suggests a method for bidirectional trust management. Here, establishing connections between fog nodes is decided upon by a combination of logistic regression and subjective reasoning, with the help of an intermediary node. A fog node must calculate the trust values. Along with the requested fog data, the calculated trust value is also supplied. The suggested method incorporates both a centralized and decentralized trust management mechanism. Finally, experiment was conducted to evaluate the efficacy of the suggested model in the fog environment, and a thorough analysis of

the results was completed. objective to enhance the lifetime and minimize the route detection cost. This approach using the fresher encounter algorithm to improve energy-efficiency and solves the node dead issues [26]. Multipath delay commutator fast fourier transform has been proposed for enhancing the throughput and speed [27].

## 2. METHOD

This model is a fusion of a centralized and distributed trust management framework that takes the environment variables as conditions which portrayed their characteristics of the around fog node points. These conditions can be, for instance, what is the number of fog clients it is at present fog network are been in serving, what requirements are needed by the fog clients and their recommendations over the past experience. When a fog client needs a service from a nearby fog node, the fog client takes the recommendations from the other connected nodes over the fog node service provider. Then the fog client considers these recommendations as parameters to calculate the trust value by implementing logistic regression function (1).

$$P(x) = \frac{1}{1+e^{-(x-\mu/s)}} \quad (1)$$

Where  $\mu$  is a the midpoint of the curve, where  $p(\mu)=1/2$ , and  $s$  is ascale parameter. The above equation can be rewritten as (2).

$$P(x) = \frac{1}{1+e^{-(\beta_0+\beta_1x)}} \quad (2)$$

Where  $\beta_0=-\mu/s$  and  $\beta_1=1/s$ . The best fit can be defined toykat a given  $x$   $p(x) = p(x^k)$

Trust is the element of insistence that the fog node can pass on the requested client: since the service differs in different levels, the fog service provider, on receiving the request estimates the trust over the requested node considering the uncertainty with belief and unbelief by using subjective logic [15]. Here the fog nodes gets the recommendation over the fog client, who requested for the service. Using these recommendations as the parameters the trust is estimated by the subjective binomial opinion, as in (3) about the truth of the received recommendation in the ordered quadruple.

$$\omega_x^A = b_x^A, d_x^A, u_x^A, a_x^A \quad (3)$$

Where:

- $b$  (belief): the belief value in support of parameter being true
- $d$  (disbelief): the belief value in support of parameter being false
- $u$  (uncertainty): the amount of uncommitted belief value
- $a$  (base rate): the apriori probability in the absence of committed belief value

These components satisfy  $b + d + u = 1$  and  $b, d, u, a \in [0, 1]$  (5).

The probability projection of a binomial opinion on proposition  $x$  is defined as in (4). Trust value possess the decision on accepting the requested service request for the fog client.

$$P(x) = (b_x + a_x u_x) \quad (4)$$

### 2.1. Notations used

The level of confidence in the other fog nodes in the network is represented by a logistic regression model,  $lr$ , stored in each node. The fog nodes, who have higher computing capacity, take on the work of creating the trust model instead of the fog clients, which are limited in their resources. There are a total of  $N$  fog nodes in the network, and in this case we only utilize fog node  $j$ , therefore the set of logistic regression models is  $lr = \{lr_i, i = 1 \dots N\}$ . This concept is based on a corpus of recommendations sent by individual fog clients to a central fog node  $j$ . A fog client's acquired data about a fog node in the network is represented by the formula  $RX = [pk, nk, k = T1 \dots Tm]$ , where  $pk$  is the client's suggestion and  $nk$  is the node's experience period.

Additionally, each fog node keeps a database of its previous interactions with fog clients, including the number of favorable and bad encounters with each.  $T = \{Ti, i = 1 \dots m$  is a collection of trust values for each fog node with which it has recently interacted;  $m$  is the number of fog nodes in the client's trust database. A fog client is thus defined as a resource-constrained device that requests service from the fog node. Depending on the amount of data each fog client can store, the fog nodes will be configured

differently. Each contact between a Fog server and a client is recorded in the cloud's persistent memory. The input variables into a logistic regression model are conditions.

## 2.2. Trust estimation

This section details our solution. Due to trust assessment variations, fog node and fog clients will be segregated as service provider and service requestor respectively. Each fog node in this model is in-charge of determining its own trust value for each connection establishment in the fog environment by obtaining recommendation. Each fog node contains a component of the trust management mechanism. The trust estimation is done bidirectional in order to achieve reliable and secured connection establishment. Here, the trust estimation is done by the service requester over the service provider in order to have a trustable service and secure data sharing. Also the fog service provider estimates the trust value over the requester in order to provide service for a trustable fog client. Here in this work the trust estimation is done by the fog requester in order to believe or to disbelieve the fog provider with, whereas when the estimation is done by the provider the evaluation over the trust is done with uncertainty over the requested client to trust or distrust it.

### 2.2.1. Estimation of trust between the fog client and the fog node

Fog clients utilize T to locate additional fog nodes at which to outsource their trust estimation tasks. T allows each fog client to build its own trust network from scratch using information about prior interactions. The process of evaluating trust from a fog client to a fog node consists of four stages. The stages are shown in Figure 2. Specifically,  $FC_i$ , a client in the fog, is looking to establish communication with  $FN_j$ , a fog node with higher resources. It can use T to locate reliable fog nodes and then solicit recommendation from them. In this Figure, we can see four different recommender fog nodes named  $FN_1$ ,  $FN_2$ ,  $FN_3$ , and  $FN_4$ . Algorithm 1 demonstrates an estimating client-to-node trust in the fog. What follows is a detailed description of how a fog client and fog node interact with one another.

- Step 1: Under a variety of scenarios, fog client  $FC_i$  queries fog nodes  $FN_1$ ,  $FN_2$ ,  $FN_3$ , and  $FN_4$  for recommendation on whether or not to trust fog node  $FN_j$ . For instance, the arrangement  $msg = \{FN_j, z\}$ , where  $z$  is the ecological circumstances on which the trust depends, conveys a certain message while seeking recommendation.
- Step 2: The trust model  $lr$  for fog node  $FN_j$  is based on the relapse trust models for fog nodes  $FN_1$ ,  $FN_2$ ,  $FN_3$ , and  $FN_4$ . For a given set of circumstances,  $lr$  generates a trust assessment for a fog node  $FN_j$ , which is then sent to the  $FC_i$  along with a trust suggestion and the aforementioned natural characteristics,  $FN(pk, nk)$ . To that end, the model will report how likely it is that the node can be trusted.  $TFN_{kj} = 1$  if probability is greater than 50%.  $TFN_{kj} = 0$  if the probability is less than fifty percent. This is a double-recommended change to enhance communication.
- Step 3: Fog client  $FC_i$  connects to a fog node  $FN_1$ ,  $FN_2$ ,  $FN_3$ ,  $FN_4$ , the nodes will relay the resulting trust level,  $TFN_{kj}$ .
- Step 4: Client fog  $FC_i$  calculates node  $FN_j$  trust by integrating  $FN_1$ - $FN_4$  findings. T decides  $I$ 's trust in  $FN_1$ ,  $FN_2$ ,  $FN_3$ ,  $FN_4$ .  $TFN_i FN_j = (TFN_1^{TFN_{1j}})^{(TFN_2^{TFN_{2j}})^{(TFN_3^{TFN_{3j}})^{(TFN_4^{TFN_{4j}})}}$ . This is the recommendation to the recommender. Based on this calculation, the fog client decides whether the fog node can offer the needed administration.  $TFN_i FN_j$  is delicious  $FN_j$ .  $FN_j$  application credibility.

#### Algorithm 1. Estimating client-to-node trust in the fog

**Input:** FogNode-User\_id, FogNode-Provider\_id, Recommendations, Recommendation time, Degree of Trust

**Output:** Probability based Trust Estimation

**Process:**

BEGIN

```

FCi request service from FNj {
    FCi sends query over recommendation on FNj to it's neighbourhood fog nodes FN1..FNm
    FN1..FNm {
        Calculates recommendation value about FNj using (pk,nk)
        sends the response as 0 or 1 to FCi
    } Based on the recommendation received
    FCi calculates Degree of Trust using lr
    The database reflects Fog Node FNj's estimated trust value. FCi to FNj decide on
    service requests based on trust value
END

```

### 2.2.2. Fog node-to-client trust estimation

The situation shown in Figure 3 is the same as in Figure 2, but from the point of Fog Node j. A fog node's confidence in a fog client's reliability is unrelated to the services required of the latter. For this to work, it is assumed that the fog client has polled numerous fog nodes for the same provider. To construct a

model for each fog client is questionable in this case. Only minimal data about the fog client's actions is available, and the fog node's confidence in the client is context-insensitive. The fog client then uses this assessment of the fog node's trustworthiness as a proxy for the client's own subjective beliefs and values. However, the suggestions from different nodes may be scaled using the logistic regression model created for the network's multiple fog nodes. Using subjective logic for trust value estimate has the benefit of accounting for the inevitable ignorance and uncertainties that arise while processing arguments that are themselves dubious in some respects. Algorithm 2 illustrates an estimating fog node-to-client mutual trust. The processes required for a fog node to ascertain a client's reliability are outlined in:

- Step 1: The FNj fog node communicates to other nodes in the system a request for trust propositions for the FCi fog client. If no other fog nodes on the same progressive level have interacted with FCi, FNj will ask nodes further up.
- Step 2: FN1, FN2, FN3, and FN4 react because they're connected with FCi. (aFCmi, bFCmi, cFCmi, dFCmi) = sFCmi).
- Step 3: FNj fog node scales other nodes' suggestions using a relapse model with static variables.  $TFNj = (sFN1i \wedge s1)$  is the latest FN1 fog node suggestion. FNj's trust model fog node has already stored s1, and FN1's abstract reasoning proposal is sFN1i .
- Step 4: Fog node FNj's abstract fog client tuple joins scaled recommendations (if one exists). The final equation to solve is  $TFNjFCi = sFNjFCi \_TFN1i\_ TFN2i\_ TFN3i\_ TFN4i$ . sFNjFCi, fog nodes, understand FCi's assertion. Confidence, skepticism, and exposure will double. Individual fog nodes define assurance and suspicion about fog client behavior.

**Algorithm 2. Estimating fog node-to-client mutual trust**

```

Input: FogNode-User_id, FogNode-Provider_id, Recommendations
Output: Trust estimation using probability (belief, disbelief, and uncertainty)
Process
BEGIN
  FNjto provide service to FCi {
    FNjsends query over recommendation on FCi to it's neighbourhood fog nodes FN1..FNm
    FN1..FNm {
      Calculates recommendation value about FCi using (pk,nk)
      sends the response as 0 or 1 to FNj
    } Based on the recommendation received
    FNj estimates Degree of Trust using subjective logic
    The database reflects Fog Client FCi's estimated trust valu
    Based on the calculated trust value, decision to provide service is made between FNj
  and FCi
  END
  
```

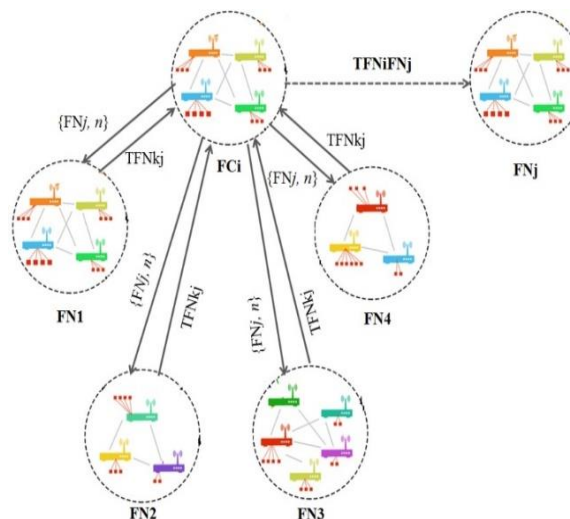


Figure 2. Estimation of trust between fog client FCi and fog node FNj

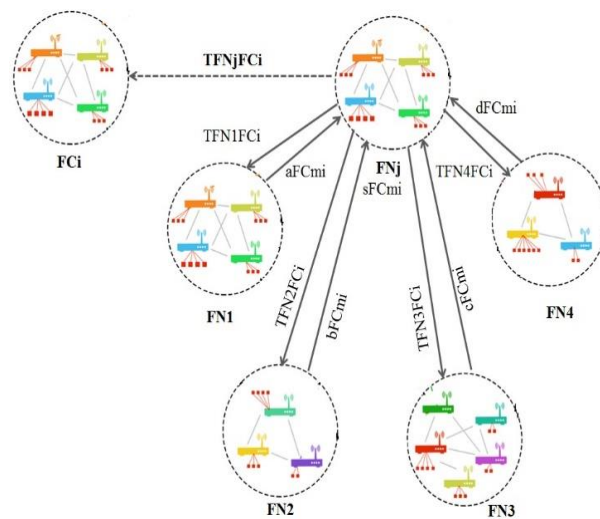


Figure 3. Estimation of trust between fog node FNj and fog client FCi

### 3. RESULTS AND DISCUSSION

The simulation tests were carried out in OMNeT++ using the FogNetSim++ tool, and the results were analyzed to see how well the aforementioned model worked. This model was constructed using a variety of parameters, the key restrictions of which are thought to be the number of fog nodes, the number of recommending nodes, and the reaction time of those nodes.

#### 3.1. Estimation of trust between the fog client and the fog node

Figure 4 shows the difference between the fog client's trust value from adjacent nodes and the fog node's computed confidence level. The fog client evaluates the fog node's reliability. The fog client accepts recommendations from neighboring nodes for the fog node it needs that shown in Figure 4(a). After receiving ideas, the proposed trust model estimates probability values based on node confidence is demonstrated in Figure 4(b). Depending on the confidence level, calculated probability values offer high and low decision-making trust is shown in Figure 4(c). Fog client trusts fog node based on recommender's trust is illustrated in Figure 4(d).

#### 3.2. Estimation of trust between the fog node and the fog client

The asking fog node chooses how much confidence to invest in the requesting fog node depending on their trust level. In this recommendation trust architecture, fog nodes seek suggestions through fog clients. Subjective logic, a probabilistic logic that combines uncertainty and source trust, doubts each provided counsel. When assessing a fog node's trustworthiness, it's helpful to conceive about opinions as a binomial (b-belief, d-disbelief, u-uncertainty, and a-base rate). Figure 5 shows the assumed uncertainty range used to compute the fog node's trust value.

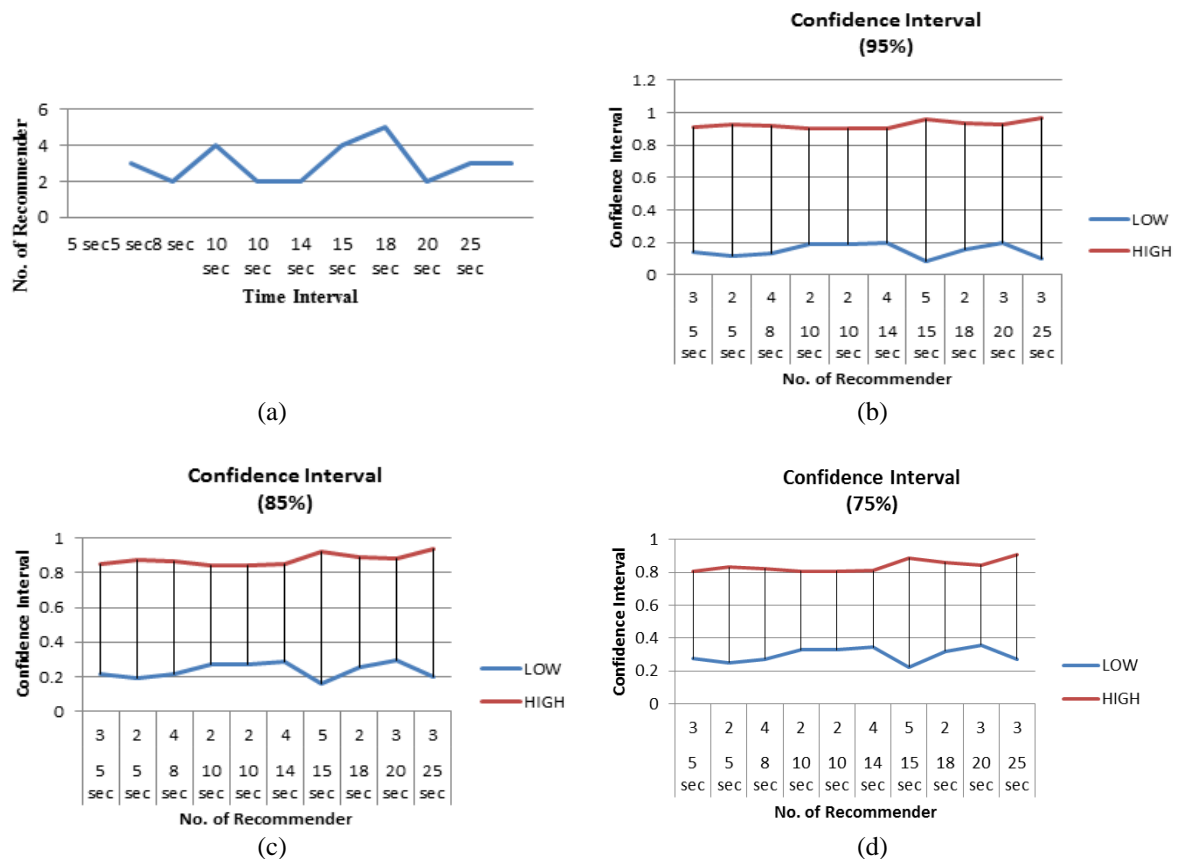


Figure 4. Difference between the fog client's and the fog node's compute confidence level by (a) trust recommender response time, (b) trust estimation using logistic regression with 95% confidence, (c) trust estimation using logistic regression with 85% confidence, and (d) trust estimation using logistic regression with 75% confidence

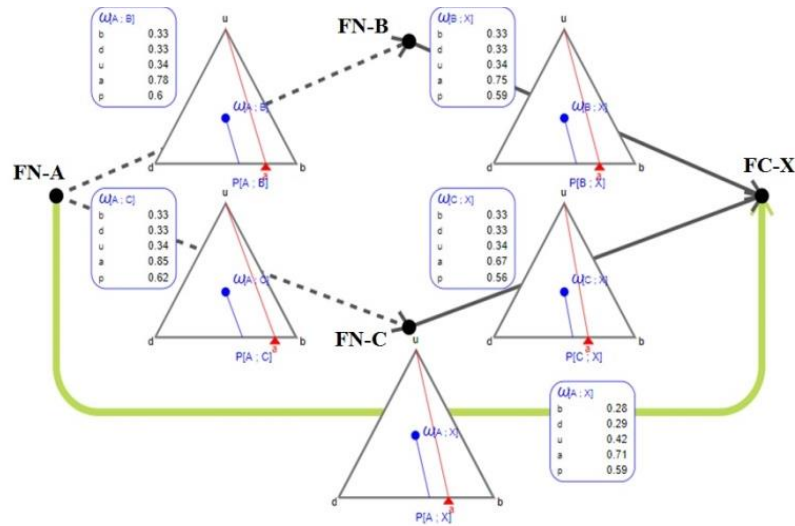


Figure 5. Estimation of reliability based on the use of subjective logic

#### 4. CONCLUSION

All of the planned labor Our bidirectional trust management method uses input from other nearby fog nodes to carry out both centralized and decentralized trust management. This paper presents a trust evaluation model for communicating between fog service providers and fog service requesters, with the goal of identifying and selecting trustworthy and dependable fog nodes for fog-to-fog communication. Logistic regression is used by the requester of a fog service to choose the most reliable fog node to provide the requested service based on the recommendations of other nearby fog nodes. The calculated value is then applied to the question of whether or not to have faith in the fog service provider. When determining the quality of the requested fog node, the fog service provider employs a subjective logic, factoring in surrounding nodes' suggestions and the inherent ambiguity in the situation. The Bi-directional trust management system incorporates both QoS and social trust information, allowing fog nodes to avoid connecting to uncertain nodes and ensuring secure data transfer with only reliable nodes based on the calculations of trust levels of fog nodes using an adaptive combination of direct observation and recommendations. Detailed experiments on the trust management system have shown that it converges rapidly, is highly accurate, and can withstand trust-based assaults with ease. As the trustworthiness of fog node recommenders is assessed, future work will need to take this into account.





#### REFERENCES

- [1] M. Chiang and T. Zhang, "Fog and IoT: an overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, Dec. 2016, doi: 10.1109/JIOT.2016.2584538.
- [2] R. Priyadarshini, N. Malarvizhi, and E. A. Neeba, "A study on capabilities and challenges of fog computing," in *Novel Practices and Trends in Grid and Cloud Computing*, 2019, pp. 249–273.
- [3] W. B. Daoud, M. S. Obaidat, A. Meddeb-Makhlouf, F. Zarai, and K. F. Hsiao, "TACRM: trust access control and resource management mechanism in fog computing," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, p. 28, Dec. 2019, doi: 10.1186/s13673-019-0188-3.
- [4] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Networks*, vol. 26, no. 5, pp. 3169–3182, Jul. 2020, doi: 10.1007/s11276-019-02129-w.
- [5] M. Momani, "Bayesian methods for modelling and management of trust in wireless sensor networks," Phd. Thesis, University of Technology, Sydney, 2008.
- [6] M. Al-khafajiy *et al.*, "COMITMENT: A fog computing trust management approach," *Journal of Parallel and Distributed Computing*, vol. 137, pp. 1–16, Mar. 2020, doi: 10.1016/j.jpdc.2019.10.006.
- [7] S. O. Ogundoyin and I. A. Kamil, "A trust management system for fog computing services," *Internet of Things*, vol. 14, p. 100382, Jun. 2021, doi: 10.1016/j.iot.2021.100382.
- [8] E. Alemneh, S. M. Senouci, P. Brunet, and T. Tegegne, "A two-way trust management system for fog computing," *Future Generation Computer Systems*, vol. 106, pp. 206–220, May 2020, doi: 10.1016/j.future.2019.12.045.
- [9] S. S. Babu, A. Raha, and M. K. Naskar, "Trust evaluation based on node's characteristics and neighbouring nodes' recommendations for WSN," *Wireless Sensor Network*, vol. 06, no. 08, pp. 157–172, 2014, doi: 10.4236/wsn.2014.68016.
- [10] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, May 2015, doi: 10.1109/TPDS.2014.2320505.
- [11] C. Marche and M. Nitti, "Trust-related attacks and their detection: a trust management model for the social IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3297–3308, Sep. 2021, doi: 10.1109/TNSM.2020.3046906.





- [12] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, Mar. 2012, doi: 10.1016/j.future.2010.12.006.
- [13] L. Jiang, J. Xu, K. Zhang, and H. Zhang, "A new evidential trust model for open distributed systems," *Expert Systems with Applications*, vol. 39, no. 3, pp. 3772–3782, Feb. 2012, doi: 10.1016/j.eswa.2011.09.077.
- [14] H. Kurdi *et al.*, "A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments," *Journal of Supercomputing*, vol. 75, no. 7, pp. 3534–3554, Jul. 2019, doi: 10.1007/s11227-018-2669-y.
- [15] P. Kochovski, P. D. Drobintsev, and V. Stankovski, "Formal quality of service assurances, ranking and verification of cloud deployment options with a probabilistic model checking method," *Information and Software Technology*, vol. 109, pp. 14–25, May 2019, doi: 10.1016/j.infsof.2019.01.003.
- [16] Y. Wang, Y.-C. Lu, I. Chen, J. Cho, A. Swami, and C. Lu, "LogitTrust: A logit regression-based trust model for mobile Ad Hoc networks," in *6th ASE International Conference on Privacy, Security, Risk and Trust*, 2014, pp. 1–10.
- [17] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing - MCC '12*, 2012, p. 13, doi: 10.1145/2342509.2342513.
- [18] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018, doi: 10.1109/COMST.2017.2762345.
- [19] O. Bouachir, M. Aloqaily, L. Tseng, and A. Boukerche, "Blockchain and fog computing for cyberphysical systems: the case of smart industry," *Computer*, vol. 53, no. 9, pp. 36–45, Sep. 2020, doi: 10.1109/MC.2020.2996212.
- [20] A. Rauf, R. A. Shaikh, and A. Shah, "Security and privacy for IoT and fog computing paradigm," in *2018 15th Learning and Technology Conference, L and T 2018*, Feb. 2018, pp. 96–101, doi: 10.1109/LT.2018.8368491.
- [21] A. A. Lisbon, "A study on cloud and fog computing security issues and solutions," *International Journal of Innovative Research in Advanced Engineering*, vol. 03, no. 4, pp. 2349–2163, 2017, [Online]. Available: <http://ijirae.com/volumes/Vol4/iss03/03.MRAE10083.pdf>.
- [22] I. Stojmenovic and S. Wen, "The fog computing paradigm: scenarios and security issues," in *2014 Federated Conference on Computer Science and Information Systems, FedCSIS 2014*, Sep. 2014, pp. 1–8, doi: 10.15439/2014F503.
- [23] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," in *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, Mar. 2017, pp. 1169–1176, doi: 10.1109/AINA.2017.161.
- [24] H. Hellaoui, A. Bouabdallah, and M. Koudil, "TAS-IoT: trust-based adaptive security in the IoT," in *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, Nov. 2016, pp. 599–602, doi: 10.1109/LCN.2016.101.
- [25] R. Priyadarshini and N. Malarvizhi, "Secured Data transfer between fog nodes using blockchain," in *Lecture Notes in Networks and Systems*, vol. 215, 2021, pp. 417–422.
- [26] A. Unnikrishnan and V. Das, "Cooperative routing for improving the lifetime of wireless Ad-Hoc networks," *International Journal of Advances in Signal and Image Sciences*, vol. 8, no. 1, pp. 17–24, Jan. 2022, doi: 10.29284/ijasis.8.1.2022.17-24.
- [27] M. M. Ismail, M. Subbiah, and S. Chelliah, "Design of Pipelined Radix-2, 4 and 8 based multipath delay commutator (MDC) FFT," *Indian Journal of Public Health Research & Development*, vol. 9, no. 3, p. 765, 2018, doi: 10.5958/0976-5506.2018.00380.7.

## BIOGRAPHIES OF AUTHORS



**Ramamurthy Priyadarshini**     is Research Scholar in the Department of Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, Tamilnadu, India. She holds Master of Technology in Computer Science and Engineering. She has more than 12 years of teaching experience. She is member of IAENG and life member of ISTE. Her areas of research interests include fog computing, cloud computing, network and information security. She can be contacted at email: [vtd398@veltech.edu.in](mailto:vtd398@veltech.edu.in).



**Nandagopal Malarvizhi**     is Professor in the Department of CSE at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, Tamilnadu, India. She holds a Ph.D. degree in Computer Science and Engineering with specialization in Cloud Computing. She is having more than 20 years of teaching experience. She has supervised and co-supervised more than 25 masters and 8 Ph.D. students. She has authored or coauthored numerous papers in International Conferences and Journals. She serves as a reviewer for many reputed journals. She is a life member of CSI, ISTE, IARCS and IAENG. She is a Senior Member of IEEE and IEEE Women in Engineering (WIE). She is a Member of ACM IET. Her area of interest includes parallel and distributed computing, grid computing, cloud computing, big data analytics, internet of things, computer architecture and operating systems. She can be contacted at email: [drnmalarvizhi@veltech.edu.in](mailto:drnmalarvizhi@veltech.edu.in).