Journal of Harbin Engineering University
ISSN: 1006-7043
Vol 44 No. 5
May 2023

Weighted Multi-Criteria Soft Trust offloading for Fog Computing

Ms. Shradhdha V. Thakkar [1]
Ph.d. Scholar
Computer Engineering Department
Sankalchand Patel College of Engineering
Sankalchand Patel University
Visnagar,Gujarat,India
shraddhaspce@gmail.com

Dr. Jay A. Dave [2]
Associate Professor
Computer Engineering Department
Silver Oak college of Engineering and Technology
Silver Oak University
Ahmedabad, Gujarat,India
jay.dave4u @gmail.com

Abstract
An innovative, intriguing paradigm called fog computing has the potential to solve the issues with conventional cloud computing. Fog server are used to process, manage, and store private and sensitive data, therefore security and privacy concerns need to be resolved before the fundamental of this certified technology. Putting into place a trust management system is one of these measures. A node's (or trustee's) reliability is evaluated using a set of standards decided upon by the trustor. To enable a trustor to assess the degree to which a parameter contribute the overall trust value of a trustee and if its beneficial to work with the node, it is imperative to identify and prioritise these criteria. The prioritisation of the trust parameter is a multi-task decision-making (MCDM) problem because it calls for the simultaneous consideration of several different criteria. In this study, trust parameters in fog computing are identified and given priority using a fuzzy analytics hierarchical process (Fuzzy-AHP) techniqu. The findings suggest that quality of service (QoS), quality of security (QoSec), and suggestions are the top prioritised parameters that a service requester can use to assess the amount of trust in a service provider. A service provider can use social relationships, which are ranked as the highest level of trust, to assess the degree of truthfulness of a svice requester, whereas reputation of past is least important factor.

Key words: Qos, Qosec, Trust Managment System (TMS),Multi criteria Decision Making (MCDM)

Introduction

A decentralised computing architecture or method known as "fog computing" places computing resources between data sources and cloud or another data centres.

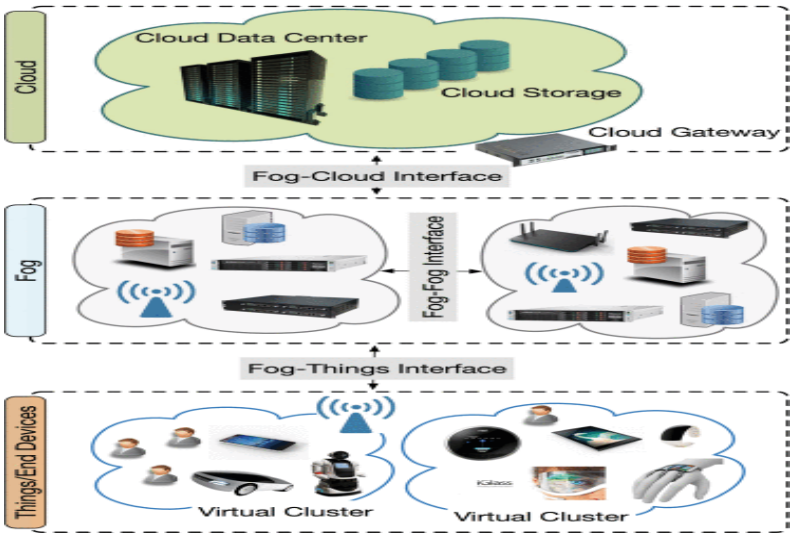

Figure 1. Working of Fog computing [11]

The Internet of Things (IoT) is a network the numerous physical object which are connected to one another via the Internet. These objects are smart because they can exchange data and communicate with one another grateful to the development of incredibly affordable sensor, actuator, and chip as well the widespread use of wireless network.

The development of IoT have significantly altered how they live and communicate with our surrounding by enabling a wide range of intelligent applications in several fields, including smart grid, smart home, transportation, health, and agriculture. Massive amounts of data are produced and transmitted by smart gadgets.

The within limit processing, computing, and storage capacity of the smart gadgets seems unable to work upon the large volume of heterogeneous data. This has make it compulsory to depend on cloud data centres, where IoT data is upload to the cloud.

To quickly offload datas from edge to cloud, meanwhile, may not be efficient as data volume grows. Additionally, cloud might unable to provides low latency functionalities and GPS base service required by this application, as well as measure with the data produced, given the frequent delayed sensitive and mission application, such as health, vehicular systems, augmented reality, virtual reality, and internet [1].

The concerns of dynamic, resource limitations, heterogenity, and scalablity [2] in the IOT environment must be addressed immediately. In other words, a computer paradigm that brings processing and storag chores closer to end device must be implemented. Researchers and academics have recommended fog computing, which is the first popularised by CISCO, as the ideal solution to the problems stated above. In order to ensure processing, computing, networking, storag, and data management is carried out close to end user, it acts as an mediary between the end device and the cloud [3]. By permitting some processes to be carried out locally, Fog computing reduce stress on the cloud. It enhanced quality of service (QoS), supports for increased bandwith and geographical distribution, receiver, and supports the real-time environment.

Trust:

The Concerns about uncertainty can be addressed using the concept of trust.

- "The firm conviction that an entity is capable of acting dependably, securely, and reliably within a given context" - [10].
- Fog is a location bsed distributed computing network; for nodes to cooperate in a fog computing environment, trust must be established.

Trust makes it possible for node to anticipate the actions of other node, which can aid in the proces of making secure decisions.

Soft Trust : Direct and Indirect Trust

Soft trust is base on peer recommendations or third-party verification, as well as the behaviour of the trust party during past direct interaction of the trust party.

It might be risky to base decisions solely on an entity's prior behaviour as a truste or recommenders because behavior can changes over time.

As a result, Soft Trusties updated their calculations over time.

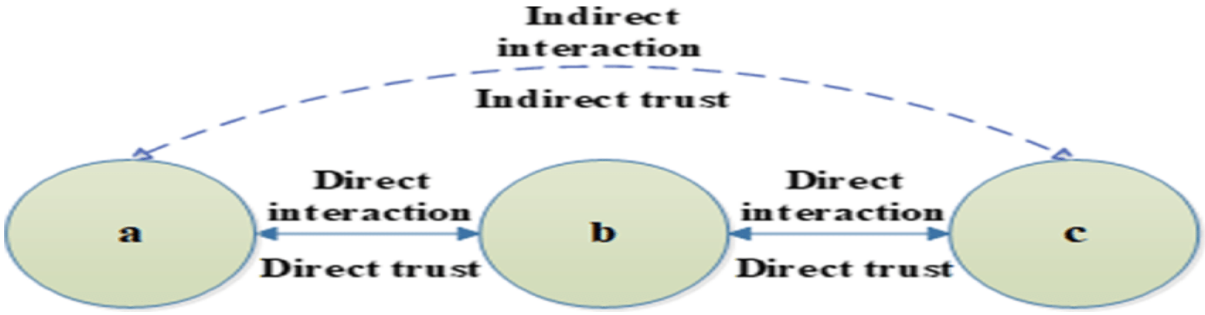

Figure 2. Direct and Indirect Trust [23]

Trust Management System

Trust composition is data used by a trustor to evaluate a trustee in trust management system (TMS). The trustor evaluates the trustee's dependability based on a variety of factors that may be either objective or subjective. The requirements for objective of the trust are that can quantified and verified, such as QoS. Contrarily, subjective criterias judgements based on the trustor's perceptions of things like honesti and recomendation. Since subjective criterias are social factors, they not measured by the equal trustor at the same time. To anticipate a node's level of dependability going forward and eliminate any unredictation, The TMS gathers valuable metrics about the node interaction in the Past and Present and recommendations from it neighbour [6].
Transmision energy, data latency, packet loss, dependability, security, integrity, availability, access control, friendlines, and cooperativenes are some of the trust characteristics used to assess a node's level of trust in fog computing. Additionally, a trustee's prior performance as well recommendation from near by node create an indirectly trust value.

A trustor evaluates a trustee using trust parameters, and the truster set the weights for each parameters. The weight quantify how significant a criterion is in relation to over all trust scores. When trust parameter are mixed, the results vary depending on the circumstance. Therefore, it is crucial for the truster ascertain those parameter is adopted for a specific setting and how much each one affects each. Therefore, it is crucial for a trustor to ascertain that parameter are used in a particular situation and how much every parameter adds the trustee's over all trust. Now a days, some of the trust management solutions for fog computing have been developed [6–9]. For offloading in various IoT context, like automotive ad hoc networks, numerous another trusts and reputations model has also been developed [10,11]. The weighting of the trust criteria, however, was not taken into account because it was either done randomly or not at all. The selection of each parameter's weight and the rating of trust are hence MCDM problems since they entail many factors that must be taken into account at once.

We draw the conclusion which no attempt have made to build a method which is prioritise trust factors fog computing based on the aforementioned and the delay in the literature. This study attempts to serve a criteria that could effectively aid in the design of a TMS in an IOT environment supported by fog computing. Additionally, knowledge of the detected factors may contribute to the development of a reliable and perticular trust model, which is advantag to Fog computing services provider and end user. The main objective of it to develop a widely-accept and generalised paradigm for the decision-making in fog computing service in light of this motive. The three primary contributions of this work are as follows.

Problem formulation

An example of a decentralised computing infrastructure or process is fog computing, in which computing resources are placed halfway between the data source and the cloud or another data centre. Using edge devices, fog computing is an architecture that performs a significant amount of local processing, storage, and communication that is then routed over the Internet. The Quality of Service (QoS) is enhanced, service latency is decreased, and end users are given a better experience thanks to the fog computing strategy.
When sending only a limited amount of data to the cloud, fog computing is employed. When the data needs to be analysed quickly, or when the latency needs to be very low, fog computing is used[1][2]. Additionally, it is employed whenever a lot of services must be spread throughout a broad area at various geographical areas. Fog computing is required for equipment that performs severe computations and processing. Fog-based services are typically held by several parties in fog computing for a variety of reasons: The

deployment choice that may include the selection of service providers.

1. Companies are expanding their services to the edge to boost performance.
2. Renting out unused private cloud resources to nearby companies as fog services.

As a result, fog computing requires a higher level of security than cloud computing because data is temporarily held and analysed on local fog nodes that are located closer to the data sources. Collaboration devices may be vulnerable to internal and external attacks that compromise the performance and accuracy of the overall system due to the open environment of fog computing.Data offloading to a rogue fog node, for instance, can lead to the unauthorised gathering or modification of users' sensitive information.As a result, interactions between fog devices must be done so under controlled circumstances.

When fog nodes are already authorised and a part of a networks utilising valid identities, cryptographic (Hard Trust)[3]based solutions are useless for preventing external attacks.However, as entities in fog computing typically have limited resources, they are unable to handle the workload of cryptography-based protocols' intensive computations. Additionally, a cryptographic technique requires more time the more secure it is [4]. Additionally, authorised internal entities may offer misleading or inaccurate information. Hard trust mechanisms don't keep an eye on the behaviour of participating entities all the time. Soft security incorporates social control elements into the underlying security mechanism to enable reliable cooperation between entities [5].

Reputation [6] or the Soft Trust is an evaluation based on the behaviour of the trusted party in past contacts with the trusting party, as reported by peers through recommendations or third-party verification. To determine how much these members may be trusted for a specific service, soft trust of the entities is used. It might be risky to base decisions solely on an entity's prior behaviour as a trustee or recommender because behaviour can change over time. As a result, Soft Trust is continually updated over time.

Motivation

Although the devices used by fog users are frequently seen as resourceful in terms of their capabilities, they are nevertheless unable to complete some hard tasks. As a result, these responsibilities are delegated and the user's control over the data is transferred to the fog layer, where fog nodes can operate independently or jointly. Therefore, avoiding malicious fog nodes for jobs requiring teamwork and processing is still a difficulty. To be an efficient security mechanism in fog it must possess following characteristics

1. **Latency** in Computation of security parameters in fog must Low in establishing node behaviour to be either trustworthy or not.
2. Security mechanism must be **Updatable** due to collaborative and frequent changing nature of fog the security parameters must be continuously update with time.
3. Nodes in the fog must be able to **Collaborate** and inform other fog nodes about updated security parameters.
4. Security mechanism must be **Distributed** and computed via multiple nodes in real time.
5. As not all nodes in fog can possess computing facilities to compute security parameters the mechanism should have some **Offloading** Capabilities where part of computation is offloaded to centralized infrastructure or cloud.
6. Single Criteria for trust computation may not work [7] thus a **multi-criteria** trust computation must be adopted.
7. Also the security mechanism should be cap able of **adjusting weights** of various criteria in real time for added resilience and survivability.

Proposed Work

Uncertainty management issues can be addressed using the concept of trust. As was previously mentioned, trust management in the fog is very difficult because of the open environment, where the quality of information is frequently unclear because of entities' potential for misbehaviour. Also the behaviour of nodes may change with time.

In this work a hybrid trust management protocol is presented which addresses scalability and adaptability requirements of the fog computing. This work proposes new **multi-criteria trust**

mechanism for fog computing environment which can serve the nodes in the fog network to regulate the security parameters using which nodes can establish trust. The *QoS (Quality of Servies), Quality of security (QSec) [11]and social trust indicators*can be taken into account by the event-based and distributed trust management system to assess a fog node's level of trust. By dynamically combiningtrust information from the nodes and the neighbouring node suggestions to compute the final trust value. This **trust can then further be offloaded** to the cloud to be requested in real-time by other node. To compute the trust various QoS and Social behaviour parameters combined with offloaded past trust will be utilized to compute resulting trust in real time. Also a dynamic weight assignment algorithm will be implemented alongside multi-criteria decision making algorithm for continuously updating the offloaded state (Past Reputations) and Current needs.

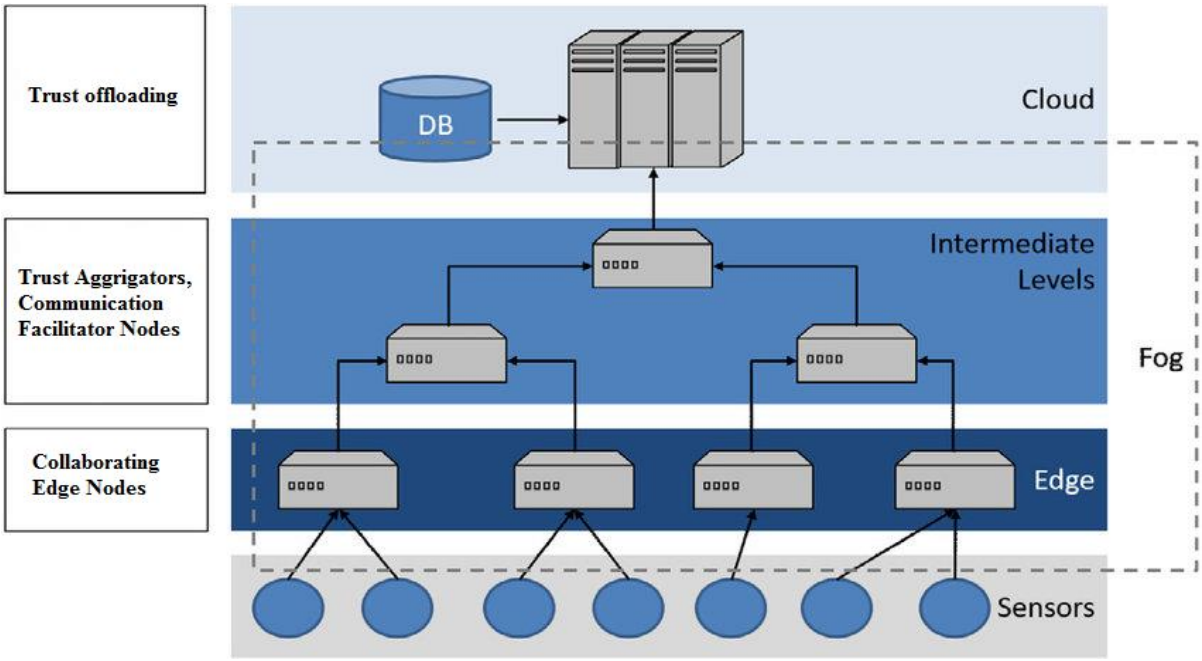

Figure 4. Proposed Trust Mechanism

In the proposed architecture the network is divided into four layers, at the lower end there are sensors which gather data and this data is pushed to the edge layer. Edge layer processes sensor data close to the logical edge of the network, far from the centralised nodes.. The computing operations are essentially pushed out to the network's edge. As these nodes collaborate in real time and are the major source of all fog attacks. The proposed trust model is intended to assess these nodes' level of trust. In the next layer i.e the fog layer the trust aggregators and communication facilitators work in real time to evaluate and update the trust of edge nodes. The fog nodes also are responsible to offload the computed trust over to the Cloud layer. The Intermediate Facilitator nodes can use various QoS, QoSec and Scocial based Trust Evaluation Parameters as mention in the following table. These parameter are further need be evaluated using multi-criteria decision making and weighing.

Trust parameter

The details required to assess a node's level of trustworthiness are known as trust parameters or criteria. The trust parameters taken into account in this work is quality of service (QoS), quality of security (QoSec), interpersonal connections, prior reputations, and recommendation.

QoS is the metrics use for assess how well the node performs in fulfilling the users requests in accordance with the service level agreement (SLA). Data Latency, transmission energies, packet loss ratios, and reliabilities are the QoS parameters. The amount of time it takes the Fog server to reply to the client request is known as latency. It is the delays in transmission, processing, and dissemination that a fog encounters which provide a service to a customers.

When a clients downloads data from a fog through a downlink connection and offloads data to a fog over an uplink network, transmission energy is consumed.. Reliability measures how well a service performs throughout a given period of time and under specific circumstances [38]. The client's prior failures and the minimum time to fail provided by the fog are used to determine it..

QoSec gauges the levels of protections a fog node offer when working with other fogs or offering a service to a client. It refers to the degree of availability, confidentiality, integrity, and access control offered by the node. If a securities measure provides a high levels of assuranse that access to data resource is limited to authorised parties, then confidentiality is guaranteed. A fog node's capacity to safeguard data from unauthorised access, usability, or disclosur while it is in transit, storaging, or processing is referred to as confidentiality. It is the access control mechanism, transmission encryption, and data encryption necessary to provide a service to the fog clients.

If a security measure provides strong assurance that the resources or data haven't changed from their initially protected state, it is offering integrity. A fog node's ability to ensure that a client's data hasn't been altered is known as integrity. copied, or otherwise tampered with. It is crucial to remember that a fog node and a fog client only need to verify each other once in order to reduce processing time .

For a fog to be available, its enabling infrastructures must be up and running and grant access to authorised users.. Access Controls should in place to preserve availability, including those that permit authorised access, a reasonable degree of performance, manage interruptions as rapidly as feasible, offer redundancy, keep trustworthy backups and stop data destruction or loss. the proportion of a service's total time to the amount of time a customer can access it through fog request is the availability of a fog. Access control is a method for granting or denying a requester access to a service. Information security must include the management of resource access.

Social relationship is the bonds that exist between a truster and a truste and involve frequent exchanges that both sides deem to be significant. Social relational measures such as honesty, kindness, and cooperation are of interest in a fog computing environment. The trust in a node's reliability as directly observed by another node over a period of time is known as honesty [39, 40]. It assists the trustor in keeping track of some potentially dishonest actions taken by the trustee over a specified period of time, such as the identification of misbehaving nodes, the detection of false recommendations, the lowering of the risk involved in dealing with strangers, attack resistance, and the assurance of reliable provisioning [40].

The degree of an effective relationship between two or more nodes is measured by friendliness. The degree of trustworthiness between two nodes increases with the number of beneficial interactions between them. It is the proportion of connections requests that are successful to all queries [6]. When a service connection request is accepted by a fog server, it means that the trustee's trust value is greater than a predetermined threshold. The level of a node's cooperativeness indicates how willing it is to communicate with another node over a specific time period. A node may be cooperative one moment and uncooperative the next section.

Past Reputation is the trustor past evaluation of the truste base on the gap inbetween the last time the trustors and truste interacted and the present. When there are no interactions with the trustor over time, a trustee direct trust score gradually declines. In a social setting, the less frequently we interact with someone, the more likely it is that we may mistrust them since we are unsure of whether or not they still possess the qualities

that make them trustworthy. Based on the elapsed time between the two events, trust decay aids in modelling the impact of past's trust levels on present's value. Since the trust deterioration is dependent on the trustor's estimation of the trustee trustworthiness, it only pertains to the trustee's direct trust score and not the over all trusts value

Recommendations: When the trustor has no prior contacts with the trustee, recommendation from trustworthie nodes can be used to assess the trustee's trustworthiness. Suppose node a wishes to communicate with node b, but an is also engaged in another sessions with node c, which offers advice for b. Node an evaluates the reliability of b using the recommendetion it receive from C. The degree to a trust can consider the recommender evaluation of a truste is crucial to consider even though recommendations are a valuable and essential component of the total trust score. This is cumpolsory to counteract certain trust base attack including vote-rigging, and defamation.

Table 1: Various QoS, QoSec and Scocial based Trust Evaluation Parameters

QoS	QoSec	Social relationships
Latency	Integrity	Friendliness
Packet Loss Ratio	Availability	Cooperativeness
Reliability	Access Control	Past reputation
Confidentiality	Honesty	Recommendations
Transmission Energy		

Table 2: Pair wise Comparison Matrix (PCM)

Parameters (P)	**Weight α**	**Weight β**	**Weight ϒ**
QoS (P1)	αP1		
QoSec (P2) (Direct Trust+ Indirect Trust)		βP2	
Economic (P3)			ϒP3

Proposed Algorithm

Weighted Multi - criteria trust model will be used to assign weights for each category

$$Trust\ Factor = \alpha \times QoS\ Parameters + \beta \times QoSec\ Parameters + \gamma \times Economic\ Parameters$$

where,

α, β, and γ are weights for each categorical parameters.

$$\text{Normalized Trust Factor} = \text{Normalize}(\text{Trust factor})$$

Each categorical parameter has further sub divisions which have further assigned weights

$$QoS = \sum_{\alpha=1}^{m} \alpha \times Parameters$$

where,

$$QoS = \alpha 1 \times Latency Time + \alpha 2 \times Packet\ Loss\ Ratio + \alpha 3 \times \text{Re}liability + \alpha 4 \times Total\ Blocking\ Time$$

$$QoSec = \sum_{\beta=1}^{n} \beta \times Parameters$$

where,

$$QoSec = \beta 1 \times Friendlyness + \beta 2 \times Cooperativeness + \beta 3 \times \text{Re}commandation$$

$$Economic = \sum_{\gamma=1}^{l} \gamma \times Parameters$$

Where,

$$Economic = \gamma 1 \times Execution\ Cost + \gamma 2 \times Migration\ Cost$$

The Trust Model's primary procedures and processes fall under the following categories

1. Fog Performance: To keep track of fog performance, Trust Model routinely checks its resources (such as CPU usage), active processes (such as stakeholder service processes), and incoming service request traffic. Upon detecting a fog overload, the Trust Model will cause the service's request offloading feature to activate. Procedures to identify the requests for the overloaded service are covered in more detail in next Section.

2. Fog interactions: When an overload is detected, the Trust Model is in charge of determining which nodes are the best neighbours. that can cope with the overload. The trustworthiness of the suggested fogs for managing the overload is evaluated during this phase. This guarantees that the hosted fog's QoP and QoS match SSLA requirements and user expectations for the targeted service, such as seamless service operation and guaranteed data security. More about this is covered in next Section.

3. offloading to balance work load

Let's say fog nodes receives a request for data process from the things , it responds after processing the requests. When it is occupied with other requests, the fog node might only be able to

processes a portion of payload and transfer the other portions to other Fog node. Based on calculations, a fog nodes decides whether to assist the process of a data process request received or to offload the request to one another fog.

This method is useful for recognising various attack kinds. It is, nevertheless, vulnerable to process and communicate costs. The work of [46] trust evaluation techniques for cloud and edge computing, leading to a significant reduction in resource consumption for trust evaluation and an increase in the effectiveness of IoT-cloud services. They used the mean trust value method in this approach, which was determined using the observed values collected from the interacting devices. This could result in network communication overhead. Offloading across fog nodes allows for resource efficiency, avoiding congestion and bottlenecks [55]. Numerous approaches to the issues of offload request in a fog comput environments are discussed in the literature. However, they do not consider trust to be a crucial factor when queries are offloaded from one node to an other [56]. The policy takes implementation, energy prices, and other expens into consideration. Fricker et al. [58] developed an analytical framework to examine a basic offloading technique for data centres in fog computing under excessive demand.

The Model took When the intended data centre is overcrowded, the model considers passing request with a specific probablity to nearby data centree. Additionally, depending on whether the arriving requests can be offloaded to other data centres, requests may be denied or rejected. An analytical approach was put forth by Zhang et al. [59] to facilitate nice ofloading among numerous fog node when preserving minimal time wast. According to rules that reduce task delay and a fairness metric, it chooses fog nodes to offload work to.

They concentrated only on forwarding time, routing failure rates, and packet loss rate. A fog-based middleware that uses entropy definition to determine trusts inbetween a fog and the cloud is what Elmisery et al. [63] proposed. For safeguarding vehicle networks, the author of [64] presented a fuzzy trust approach which takes into consideration experience. A number of security checks are made to make sure the data gathered from authorised vehicles is accurate. Additionally, a facility based on fog is employed to assess the event's location's degree of accuracy.

In conclusion, there are a number of methods that take into account the problems of offload and building trust amongst fog node. But not regard trust as the most important factor metrics of offloading or outsoursing request in a fog computing para.

Table 3: Comparison of the Trust Model with Other Studies

Researches	Description and Goals of the Study							
	Q o S	**Latency**	**Security**	**Availability**	**Scalability**	**SSLA**	**Energy**	**Resource Management**
By Deng eet al. [26]	✔	✔	✘	✘	✔	✘	✔	✔
By Al-khafjiy et al. [17]	✔	✔	✘	✔	✘	✔	✘	✔
By Ha et al. [27]	✘	✘	✔	✘	✘	✘	✘	✘
By Yanuzzi et al. [28]	✔	✘	✘	✔	✔	✘	✘	✘

By Chan and eao [29]	✔	✘	✘	✘	✘	✘	✘	✘
By Gieng et al. [30]	✔	✘	✔	✘	✔	✘	✔	✔
By Pahal et al. [31]	✘	✘	✔	✘	✘	✘	✘	✘
By Srkar et al. [32]	✔	✔	✘	✘	✘	✘	✔	✘
By Skarlt et al. [33]	✔	✘	✘	✔	✔	✘	✘	✔
By Guptaa et al. [34]	✔	✔	✘	✘	✔	✘	✔	✘
By Shan et al. [35]	✘	✘	✔	✘	✔	✘	✘	✘
By Wan et al. [36]	✔	✘	✘	✘	✘	✘	✘	✔
By Lie et al. [37]	✔	✘	✘	✔	✔	✘	✘	✔
Bhaardwaj et al. [38]	✘	✘	✔	✘	✘	✘	✘	✘
By Weng et al. [39]	✔	✔	✘	✔	✔	✘	✘	✔
By Heu et al. [40]	✘	✘	✔	✘	✘	✘	✘	✘
Valati et al. [41]	✔	✘	✘	✘	✘	✘	✔	✘
By Azmi et al. [42]	✔	✘	✘	✔	✔	✘	✘	✔
Markakis et al. [43]	✔	✘	✔	✘	✘	✘	✘	✔
By Chen and Xeu [44]	✔	✘	✘	✘	✔	✘	✔	✘
Ne et al. [45]	✘	✘	✔	✘	✘	✘	✘	✘
Propose Trust Model	✔	✔	✔	✔	✘	✔	✔	✔

Conclusion

This paper presents a Trust Model, a fog computing solution to managing trust, was discussed in this study. First, we discussed the architecture of fog-based systems and the corresponding dangers, assaults, and security needs. Then, we spoke about performances and interaction of the Fog node in relation to the Trust Model procedures and processes. In addition, utilising both direct and indirect experiences, we identified the issue and developed the suggested model of trust recommendation. Finally, we ran a number of tests to confirm the accuracy and efficacy of the suggested strategy, finding that the Trust Model surpassed the competing benchmark algorithms. In our upcoming study, we want to expand the simulation by measuring how much energy fog nodes use when collaborating and offloading.

References

[1] Shi, C., Ren, Z., Yang, K., Chen, C., Zhang, H., Xiao, Y., &Hou, X. (2018, April). Ultra-low latency cloud-fog computing for industrial internet of things. In 2018 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

[2] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: A review. big data and cognitive computing, 2(2), 10.

[3] Msanjila, S. S., &Afsarmanesh, H. (2009, October). On hard and soft models to analyze trust life cycle for mediating collaboration. In Working Conference on Virtual Enterprises (pp. 381-392). Springer, Berlin, Heidelberg.

[4] Trcek, D. (2011). Trust management in the pervasive computing era. IEEE security & Privacy, 9(4), 52-55.

[5] Cho, J. H., Swami, A., & Chen, R. (2010). A survey on trust management for mobile ad hoc networks.

IEEE communications surveys & tutorials, 13(4), 562-583.

[6] Selcuk, A. A., Uzun, E., &Pariente, M. R. (2004, April). A reputation-based trust management system for P2P networks. In IEEE International Symposium on Cluster Computing and the Grid, 2004. CCGrid 2004. (pp. 251-258). IEEE.

[7] Ogundoyin, S. O., &Kamil, I. A. (2020). A Fuzzy-AHP based prioritization of trust criteria in fog computing services. Applied Soft Computing, 97, 106789.

[8] Jabeen, F., Khan, Z. U. R., Hamid, Z., Rehman, Z., & Khan, A. (2021). Adaptive and survivable trust management for Internet of Things systems. IET Information Security, 15(5), 375-394.

[9] Al-Khafajiy, M., Baker, T., Asim, M., Guo, Z., Ranjan, R., Longo, A., ... & Taylor, M. (2020). COMITMENT: A fog computing trust management approach. Journal of Parallel and Distributed Computing, 137, 1-16.

[10] [11]Trcek, D. (2011). Trust management in the pervasive computing era. IEEE security & Privacy, 9(4), 52-55

[11] [12] Cho, J. H., Swami, A., & Chen, R. (2010). A survey on trust management for mobile ad hoc networks. IEEE communications surveys & tutorials, 13(4), 562-583.

[12] [13]Selcuk, A. A., Uzun, E., &Pariente, M. R. (2004, April). A reputation-based trust management system for P2P networks. In IEEE International Symposium on Cluster Computing and the Grid, 2004. CCGrid 2004. (pp. 251-258). IEEE.

[13] Grandison, T., &Sloman, M. (2000). A survey of trust in internet applications. IEEE Communications Surveys & Tutorials, 3(4), 2-16.

[14] Irvine, C., & Levin, T. (2001, February). Quality of security service. In Proceedings of the 2000 workshop on New security paradigms (pp. 91-99).

[15] Gupta, H., VahidDastjerdi, A., Ghosh, S. K., &Buyya, R. (2017). iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. Software: Practice and Experience, 47(9), 1275-1296.

[16] Al-Khafajiy, M., Baker, T., Asim, M., Guo, Z., Ranjan, R., Longo, A., ... & Taylor, M. (2020). COMITMENT: A fog computing trust management approach. Journal of Parallel and Distributed Computing, 137, 1-16

[17] Grandison, T., &Sloman, M. (2000). A survey of trust in internet applications. IEEE Communications Surveys & Tutorials, 3(4), 2-16.

[18] Irvine, C., & Levin, T. (2001, February). Quality of security service. In Proceedings of the 2000 workshop on New security paradigms (pp. 91-99).

[19] Gupta, H., VahidDastjerdi, A., Ghosh, S. K., &Buyya, R. (2017). iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. Software: Practice and Experience, 47(9), 1275-1296.

[20] B. Zhang, N. Mor, J. Kolb, D.S. Chan, K. Lutz, E. Allman, J. Wawrzynek, E.A. Lee, J. Kubiatowicz, The cloud is not enough: saving iot from the cloud, in: Hotstorage, 2015.

[21] D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of things security: a top-down survey, Comput. Netw. 141 (2018) 199–221.

[22] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, All one needs to know about fog computing and related edge computing paradigms: a complete survey, J. Syst. Archit. 98 (2019) 289–330. [4] Fog computing and the Internet of Things

[23] A. Adewuyi, H. Cheng, Q. Shi, J. Cao, Á. MAcDermott, X. Wang, CTRUST: A dynamic trust model for collaborative applications in the internet of things, IEEE Internet Things J. 6 (3) (2019) 5432–5445.

[24] E. Alemneh, S. Sanouci, P. Brunet, T. Tegegne, A two-way trust management system for fog computing, Future Gener. Comput. Syst. (2020).

[25] M. Al-Khafajiy, T. Baker, H. Al-Libawy, Z. Maamar, M. Aloqaily, Y. Jararweh, Improving fog computing performance via fog-2-fog collaboration, Future Gener. Comput. Syst. 100 (2019) 266–280.

[26] A.K. Junejo, N. Komninos, M. Sathiyanarayanan, B.S. Chowdhry, Trustee: a trust management system for fog-enabled cyber physical systems, IEEE Internet Comput. (2019) http://dx.doi.org/10.1109/TETC.2019.2957394, in press

[27] [27] T. He, E. N. Ciftcioglu, S. Wang, and K. S. Chan, “Location privacy in mobile edge clouds: A chaff-based approach,” IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2625–2636, 2015

[28] M. Yannuzzi, R. Milito, R. Serral-Graci`a, D. Montero, and M. Nemirovsky, “Key ingredients in

an iot recipe: Fog computing, cloud computing, and more fog computing," in 2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 325–329, IEEE, 2014.

[29] M. Chen and Y. Hao, "Task offloading for mobile edge computing in software defined ultra-dense network," IEEE Journal on Selected Areas in Communications, vol. 36, no. 3, pp. 587–597, 2018.

[30] N. K. Giang, M. Blackstock, R. Lea, and V. C. Leung, "Developing iot applications in the fog: A distributed dataflow approach," in 2015 5th International Conference on the Internet of Things (IOT), pp. 155–162, IEEE, 2015.

[31] C. Pahl, N. El Ioini, S. Helmer, and B. Lee, "An architecture pattern for trusted orchestration in iot edge clouds," in 2018 Third International

[32] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of internet of things," IEEE Transactions on Cloud Computing, vol. 6, no. 1, pp. 46–59, 2015.

[33] O. Skarlat, M. Nardelli, S. Schulte, M. Borkowski, and P. Leitner, "Op-timized iot service placement in the fog," Service Oriented Computingand Applications, vol. 11, pp. 427–443, Dec 2017.

[34] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "ifogsim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments," Software: Practice and Experience, vol. 47, no. 9, pp. 1275–1296, 2017.

[35] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight andprivacy-preserving secure cloud auditing scheme for group users via thethird party medium," Journal of Network and Computer Applications,vol. 82, pp. 56 – 64, 2017.

[36] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fogorchestration for internet of things services," IEEE Internet Computing,vol. 21, pp. 16–24, Mar 2017.

[37] P. Liu, L. Hartung, and S. Banerjee, "Lightweight multitenancy at thenetwork's extreme edge," Computer, vol. 50, no. 10, pp. 50–57, 2017.

[38] K. Bhardwaj, J. C. Miranda, and A. Gavrilovska, "Towards iotddos prevention using edge computing," in USENIX Workshop on Hot Topics in Edge Computing (HotEdge 18), (Boston, MA), USENIX Association, 2018.

[39] N. Wang, B. Varghese, M. Matthaiou, and D. S. Nikolopoulos, "Enorm:A framework for edge node resource management," IEEE Transactionson Services Computing, pp. 1–1, 2018.

[40] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," IEEE Internet of Things Journal, vol. 4, pp. 1143–1155, Oct 2017.

[41] C. Vallati, A. Virdis, E. Mingozzi, and G. Stea, "Exploiting lte d2d com-munications in m2m fog platforms: Deployment and practical issues," in2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 585–590, Dec 2015.

[42] Azimi, A. Anzanpour, A. M. Rahmani, T. Pahikkala, M. Levorato, P. Liljeberg, and N. Dutt, "Hich: Hierarchical fog-assisted computing architecture for healthcare iot," ACM Trans. Embed. Comput. Syst., vol. 16, pp. 174:1–174:20, Sept. 2017.

[43] E. K. Markakis, K. Karras, A. Sideris, G. Alexiou, and E. Pallis, "Com-puting, caching, and communication at the edge: The cornerstone forbuilding a versatile 5g ecosystem," IEEE Communications Magazine, vol. 55, pp. 152–157, Nov 2017.

[44] L. Chen and J. Xu, "Socially trusted collaborative edge computing in ultra dense networks," in Proceedings of the Second ACM/IEEE Symposium on Edge Computing, SEC '17, (New York, NY, USA), pp. 9:1–9:11, ACM, 2017.

[45] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," IEEE Communications Surveys Tutorials, vol. 20, pp. 601–628, Firstquarter 2018.

[46] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, A secure IoTservice architecture with an efficient balance dynamics based on cloud and edge computing. IEEE Internet of Things Journal, 2018.

[47] M. Henze, R. Hummen, R. Matzutt, and K. Wehrle, "A trust point based security architecture for sensor data in the cloud," In Trusted Cloud Computing, pp. 77–106, 2014.

[48] Talukdar, V., Dhabliya, D., Kumar, B., Talukdar, S. B., Ahamad, S., & Gupta, A. (2022). Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach. 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), 531–535. IEEE.

[49] L. Galluccio, S. Milardo, G. Morabito, and P. S. S. wise: Design, "Pro-totyping and experimentation of a stateful sdn solution for wireless sen-sor networks," in 2015 IEEE Conference on Computer Communications(INFOCOM), pp. 513–521, IEEE, 2015.

[50] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management formobile ad hoc networks,"

IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pp. 562–583, 2010.

[51] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation- based announcement scheme for vanets," IEEE Transactions on Vehicular Technology, vol. 61, no. 9, pp. 4095–4108, 2012.

[52] R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing,"IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 5,pp. 1200–1210, 2013.

[53] J. Ren, Y. Zhang, K. Zhang, and S. X. S. Sacrm, "Social aware crowd-sourcing with reputation management in mobile sensing," ComputerCommunications, vol. 65, pp. 55–65, 2015.

[54] K. Hwang, S. Kulkareni, and Y. Hu., "Cloud security with virtualized defense and reputation-based trust mangement," in 2009 Eighth IEEE International Conference on Dependable, (IEEE), pp. 717–722, Autonomic and Secure Computing, 2009.

[55] 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, 2015.

[56] Q. Fan and N. Ansari, "Towards workload balancing in fog computingempowered iot," IEEE Transactions on Network Science and Engineer-ing, 2018.

[57] C.-H. Hong and B. Varghese, "Resource management in fog/edge com-puting: A survey," arXiv preprint arXiv:1810.00305, 2018.

[58] Q. Zhu, B. Si, F. Yang, and Y. Ma., "Task offloading decision in fog computing system," China Communications, vol. 14, no. 11, pp. 59–68, 2017.

[59] C. Fricker, F. Guillemin, P. Robert, and G. Thompson, "Analysis of an offloading scheme for data centers in the framework of fog computing," ACM Transactions on Modeling and Performance Evaluation of Computing Systems (TOMPECS), vol. 1, no. 4, p. 16, 2016.

[60] Pandey, J. K., Ahamad, S., Veeraiah, V., Adil, N., Dhabliya, D., Koujalagi, A., & Gupta, A. (2023). Impact of Call Drop Ratio Over 5G Network. In Innovative Smart Materials Used in Wireless Communication Technology (pp. 201–224). IGI Global.

[61] G. Zhang, F. Shen, Y. Yang, H. Qian, and W. Yao, "Fair task offloadingamong fog nodes in fog computing networks," in 2018 IEEE Interna-tional Conference on Communications (ICC), pp. 1–6, IEEE, 2018.

[62] W. Masri, I. Al Ridhawi, N. Mostafa, and P. Pourghomi, "Minimizing delay in iot systems through collaborative fog-to-fog (f2f) communication," in 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 1005–1010, IEEE, 2017.3A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," IEEE Internet ComputingMar, vol. 1, no. 21, p. 2, 2017.

[63] T. Wang, G. Zhang, M. D. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, A novel trust mechanism based on fog computing in sensor–cloud system.Future Generation Computer Systems, 2018.

[64] A. M. Elmisery, S. Rho, and D. Botvich, "A fog based middleware for automated compliance with oecd privacy principles in internet of health- care things," IEEE Access, vol. 4, pp. 8418–8441, 2016.

[65] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas- Rosales, M. K. Khan, and S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," IEEE Access, vol. 5, pp. 15619–15629, 2017.

[66] J. Yan, Y. Ma, L. Wang, K.-K. R. Choo, and W. Jie, "A cloud-based remote sensing data production system," Future Generation Computer Systems, vol. 86, pp. 1154–1166, 2018.

[67] L.Wang, Y. Ma, J. Yan, V. Chang, and A. Y. Zomaya, "pipscloud: Highperformance cloud computing for remote sensing big data management and processing," Future Generation Computer Systems, vol. 78, pp. 353–368, 2018.

[68] Z. Deng, M. Wang, L. Wang, X. Huang, W. Han, J. Chu, and A. Y. Zomaya, "An efficient indexing approach for continuous spatial approximate keyword queries over geo-textual streaming data," ISPRS Inter- national Journal of Geo-Information, vol. 8, no. 2, p. 57, 2019.

[69] J. Fan, J. Yan, Y. Ma, and L. Wang, "Big data integration in remote sensing across a distributed metadata-based spatial infrastructure," Re- mote Sensing, vol. 10, no. 1, p. 7, 2017.

[70] [69] M. Al-khafajiy, T. Baker, C. Chalmers, M. Asim, H. Kolivand, M. Fahim, and A. Waraich, "Remote health monitoring of elderly through wearable sensors," Multimedia Tools and Applications, Jan 2019.

[71] Anand, R., Ahamad, S., Veeraiah, V., Janardan, S. K., Dhabliya, D., Sindhwani, N., & Gupta, A. (2023). Optimizing 6G Wireless Network Security for Effective Communication. In Innovative Smart Materials Used in Wireless Communication Technology (pp. 1–20). IGI Global.

[72] Z. Maamar, T. Baker, N. Faci, M. Al-Khafajiy, E. Ugljanin, Y. Atif, and M. Sellami, "Weaving cognition into the internet-of-things: Application to water leaks," Cognitive Systems Research, vol. 56, pp. 233 – 245, 2019.

[73] X. Wang, Z. Ning, and L. Wang, “Offloading in internet of vehicles: A fog-enabled real-time traffic management system,” IEEE Transactions on Industrial Informatics, vol. 14, no. 10, pp. 4568–4578, 2018.

[74] M. A. Salahuddin, A. Al-Fuqaha, andM. Guizani, “Reinforcement learn-ing for resource provisioning in the vehicular cloud,” IEEE Wireless CommunicationsAug;, vol. 23, no. 4, pp. 128–35, 2016.

[75] R. Saini and M. Khari, “Defining malicious behavior of a node and its defensive methods in ad hoc network,” International Journal of Com- puter Applications Apr;, vol. 20, no. 4, pp. 18–21, 2011.

[76] A. Josang and R. Ismail, “The beta reputation system,” in In Proceed-ings of the 15th bled electronic commerce conference, pp. 2502–2511, 5,Jun 17 2002.

[77] X. Yang, Y. Guo, Y. Liu, and H. Steck, “A survey of collaborative filtering based social recommender systems,” Computer Communications, vol. 41, pp. 1–10, 2014.

[78] Y. Sahni, J. Cao, S. Zhang, and A. Yang L. Edge Mesh:, “new paradigmto enable distributed intelligence in internet of things,” IEEE access,vol. 5, pp. 16441–58, 2017.

[79] M. J. Canet, V. Almenar, J. Marin-Roig, and J. Valls, “Time synchronization for the ieee 802.11 a/g wlan standard,” in 2007 IEEE 18th International Symposium on Personal, (IEEE), pp. 1–5, Indoor and Mobile Radio Communications, 2007.

[80] A. Qureshi, Power-demand routing in massive geo-distributed systems.Massachusetts Institute of Technology. Doctoral dissertation.

[81] T. Q. Dinh, J. Tang, Q. D. La, and Q. TQ., “Offloading in mobile edge computing: Task allocation and computational frequency scaling,” IEEE Transactions on CommunicationsAug;, vol. 65, no. 8, pp. 3571–84, 2017.

[82] Y. Xiao and M. Krunz, “Qoe and power efficiency tradeoff for fog com-puting networks with fog node cooperation,” in Conference on ComputerCommunications (I. I. 2017-ieee, ed.), pp. 1–9, IEEE, 2017.

[83] [81] A. Bozorgchenani, D. Tarchi, and C. G. A. energy and, “An energy and delay-efficient partial offloading technique for fog computing ar-chitectures,” in GLOBECOM 2017-2017 IEEE Global Communications Conference, pp. 1–6, IEEE, Dec 4 2017.