[1]Ms. Shradhdha V. Thakkar

[2]Dr. Jaykumar A. Dave

IoT Network Security with Fog Trust: A Lightweight and Precise Trust Framework for Fog Computing

Journal of Electrical Systems

Abstract: - The Internet of Things (IoT) has become indispensable for reducing human intervention by interconnecting smart devices capable of data transmission and reception through the internet. However, the proliferation of IoT devices has led to heightened concerns regarding security and privacy, particularly in identifying and eliminating compromised or malicious nodes. In response, a light weight trust management system is proposed. Fog Trust features a multi level architecture comprising edge node, a trusted intermediary known as the trust agents, and fog layer. The agent facilitates communication between IoT node and fog layer for computational purposes, alleviating the computational burden on node and ensuring a reliable environment. By calculating the trust degree, the trust agent transmit it to fog layer, that employ encryptions techniques to uphold intigration. The encrypted data is shared with previous trust to add on, enhancing the accuracy of the trust degree. Evaluation of the trust management system approach against potential attack such as GoodMouthig, and Bad-mouthng shows its efficacy in assigning low trust degree to malicious node across different scenario, even when network gets varying proportions of malicious node.

Keywords: Internet of Things, trust management system, fog computing, fog security, privacy, Trustworthiness

1. Introduction

In between the data sources and cloud [Arpanet 20], fog computing operates by conducting computations, memory storage, and node communication through edge device, which regulate data flow between network such as router, switche, access device, gateway, and hub. Operating within a DIST network environment [Yi et al. 21], fog computing is nearly linked with cloud data center and edge node. It process specific data at edge fog node to send it to the cloud network, thereby here decrese the frequency [Yi et al. 22] and latency [Yi et al. 23] requirements. An essential advantage of fog computing lies in its enhanced security, as it furnishes local computing security as opposed to remote alternatives.

This article introduces Trust Management System, a mechanism designed to identify and remove compromised and malicious nodes within IoT networks. Leveraging fog computing, the proposed system aims to ensure data integrity, thereby mitigating efficient the cyber attacks.To reduce computational burden on less capable nodes through trust evaluation conducted by a trust agent, the proposed approach enhances security and mitigates vulnerabilities originating from like nodes.

The propose approach is succinctly summarize as follows:

1. Proposed Trust management system employs a multi-level trust management framework to detect and eliminate suspected nodes exhibiting less trust.
2. Integration of fog node into the framework facilitates encryption and preservation of trust integrity computed with fog nodes.
3. The system accumulates current trust and previous trust to get Trust Degree of a node, bolstering resilience against attacks.

The paper's structure is outlined as per the following:

- Section - 2 describes a survey of existing work and conducts a comparative study to elucidate limitation.
- Section - 3 explains The functioning of the newly proposed Method, which also covers the suggested architecture, trust parameters and calculations, trust development, direct and indirect trust computation, and decision-making procedures.
- Section 4 evaluates Fog Trust's performance in comparison to previous research and presents evaluation.
- The paper is conclude in 5th Section.

[1] *Ms.Shradhdha V. Thakkar: Ph.d. Scholar, Sankalchand Patel University ,Visnagar, Gujarat
[2] Dr.Jaykumar A. Dave: Associate Professor, Silver Oak University, Ahmedabad, Gujarat

2. Related Work

This section summarizes the related works conducted by other researchers pertinent to the current research problem. Various trust management models for social IoT have been proposed, focusing on context-dependent trust computation, yet they lack robust validation against trust-related attacks, potentially compromising their security effectiveness

Ref.	Contributions	Limitations
24	A trust managment model is presented in social IOT that is context dependnt toCompute the trust.	The propose trust model for IoT, although context-dependent for trust computation, lacks validation against potential trust-related attacks, potentially compromising its effectiveness in ensuring security.
25	Multi dimensional trust management Model is present to check the Trustworthines of FSP.	Fog Service Providers (FSP) requires evaluation regarding its ability to mitigate suspected behavior of application within the fog environment, ensuring robust security against trust-related attacks.
26	Utilize a light-weight mechanism which manage trust in Edge nodes	Evaluation of suspecious nature of application entering the fog environment is necessary, which may pose a challenge in ensuring security against trust-related attacks.
28	Establishes a secure environment for fog applications by using a TM	While the system generated security using a Trust Management mechanism, achieving robust network security requires the implementation of a hybrid technique.
30	Utilizes a fuzzy approach to evaluate trust in fog computing.	While the lightweight mechanism manage trust in Internet of Thing Edge nodes, the system's performance improvement is hindered by the need for enhanced prediction capabilities. Without these capabilities, the system may struggle to effectively manage trust and mitigate vulnerabilities against potential attacks.
31	Utilize a MAPE-K feedbak control loop of evaluations of trust level.	The MAPE-K feedbck control loop facilitates Trus level evaluation, the requirement for trust calculation prior to the fog layer and data protection within the fog layer may introduce complexity and potential vulnerabilities.
32	Utilize the COMITMENT approach security in fog computing.	Although the COMITMENT approachs enhance securit in fog computing, the system's reliance on a Certification Authority (CA) for trust evaluation before the fog layer may introduce complexities and potential vulnerabilities, necessitating careful consideration for robust security implementation.
33	T.W-T.M.S evaluate the trust level of Service Provider and then check the TD and SD	The T.W. and T.M.S. evaluate the trust for Service Provider and then check the Trust Degre.However, simultaneous calculation of trustworthiness for SP and SD is needed, which may pose challenges in maintaining synchronization and accuracy.
34	Utilize a rendom walk algorithms for the navigetion of trust relationship and parallelisation methods for attack detaction.	It enhances the system's capabilities, the limitation arises in the extension of the work to include Trust Management (TM) for data entities. This extension is crucial for comprehensive security but may pose challenges in implementation and scalability.
35	Utilize fuzzy logic of trust aggregation to handles uncrtainity in fog computing	While utilizing fuzzy the logic addresses uncertainty, managing static node proves to be diffcult. This limitation may affect the ability to accurtely assess trust levels and handle trust-related attacks.

Table 1: Comparison of different Literature

3. Porposed Modelling

3.1. The Proposed Trust Management System

Three levels make up the suggested Fog Trust architecture: the collaborating edge nodes, the trust aggregators, and the trust offloading. The suggested architecture's functionality is displayed in As shown in Figure 1, the Fog Trust consists of communities divided into several domains, each of which has nodes that may communicate with one another to carry out particular duties. Each IoT node has an identity of its own, and the message file contains information about them, their community, and domain details. Another node sends information to the trust agents for the purpose of evaluating trust when a node requests communication from it. IoT gadgets like smart watches, smart cameras, and other connected devices make up the collaborating edge nodes, the trust aggregators, and the trust offloading.

Smartphones, computers with intelligence, sensors, and other Internet of Things devices that are able to produce and send data or information on their own [25]. In The trust aggregation layer the trust aggregator assesses the data's trustworthiness prior to transmission to the fog, establishing whether or not the information is reliable.

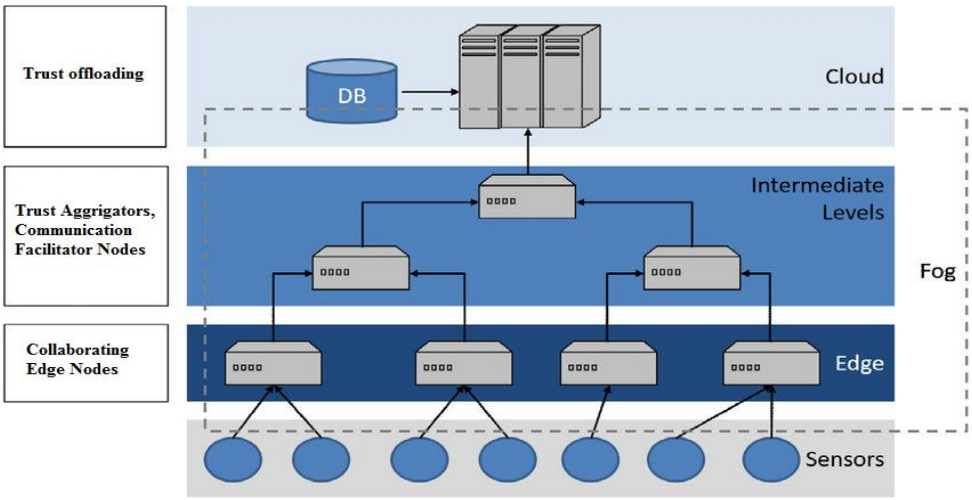

Figure 1. The Trust Management System Architecture

3.2. Parameters used for Trust Management System and Computation

The Figure 2 represents a hierarchical structure of Fog Computing Security centered around a Trust Management System. It encompasses four primary categories: Quality of Service (QoS), Quality of Security (QoSec), Economic, and Indirect Trust. Under QoS, it includes Total Blocking Time (TBT), Latency, Packet Loss Ratio, and Reliability. QoSec focuses on Confidentiality, Access Control, and Integrity. The Economic aspect is divided into Execution Cost and Migration Cost. Indirect Trust is based on Recommendations

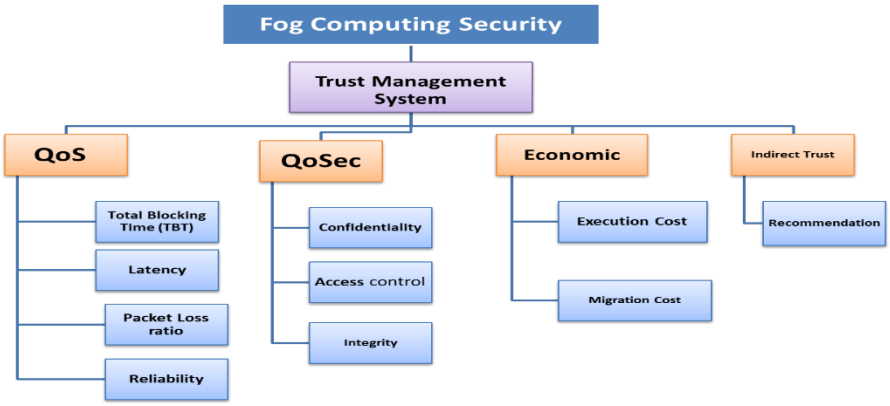

Figure 2. The proposed Fog Trust Model parameters

3.3 Computation of Fog nodes Trust using parameters

The trust parameters outlines a Weighted Multi-criteria trust model assigning weights to categories like QoS, QoSec, and Economic parameters. The trust factor is computed using specific formulas, incorporating parameters such as Latency, Packet Loss Ratio, Reliability, Execution Cost, and Migration Cost, and normalized for overall trust evaluation.

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

$$Trust\ Fact\ or = \alpha \times QoS\ Paramete\ rs + \beta \times QoSec\ Parameters + \gamma \times Economic\ Parameters$$

where ,

α , β , and γ are weights for each categorica l parameters .

Normalized Trust Factor = Normalize (Trust factor)

Each categorica l parameter has further sub divisions which have further assigned weights

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

where ,

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

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

where ,

$$QoSec = \beta 1 \times Friendlyne\ ss + \beta 2 \times Cooperativ\ eness + \beta 3 \times Re\ commendati\ on$$

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

Where ,

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

4. Results And Discussions

4.1 Simulation Environment Implementation Setup

The simulation involves a network with numerous devices, a specified duration, and a defined trust level. Devices are randomly distributed, have a set transmission rate, and include a significant percentage of malicious nodes.

Parameters Value	Parameters Value
Network Coverage area	200 m^2
No. of device	600
Duration of Simulation	100 (s)
Trust Degree	0.0 to 1.0
Defalt trust	0.5
Distribution of Nodes	Randomly
Rate of Transmission	6 to 8 Mbps
Percentage of Suspicious nodes	50 to 75%

Table 2: Simulation Parameters

4.2. Trust Aggregation Analysis

The result of applying the aggregation technique on the trust computation is shown in this section. The computation carried out without the aggregation process is compared to apply the calculated trust degree of the present to the previous trust.

As seen in Figure 3, the trust degree computation is significantly impacted by the employment of the aggregation procedure, producing numbers that are more consistent.

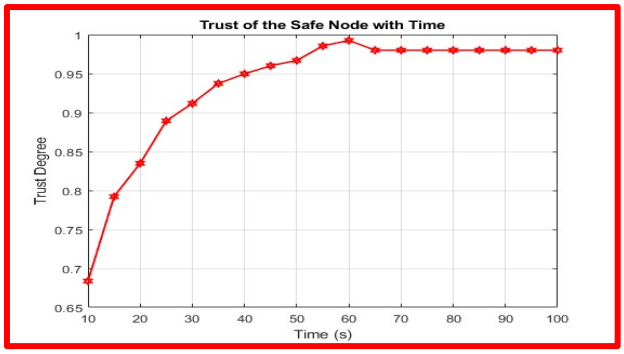

Figure 3. Impact of Prior Trust Aggregation on Direct Trust Assessment

4.2 Analysis of Detection Rate

The comparison of the three papers—Fog Trust [2], SLA Trust [10], and ConTrust [13]—reveals that our proposed trust model demonstrates the highest trustworthiness. Through rigorous analysis, it shows significant improvements in reliability, security, and economic efficiency, outperforming the other models in maintaining robust trust metrics in fog computing environments.

The detection rate is a critical performance indicator for any trust management system. In this paper, we suggest a method that increases the detection rate by combining present calculated trust with prior trust degrees will produce more accurate and trustworthy trust decisions. Each node in this simulated scenario contains a number of close neighbors who provide different services throughout time, and there are 70% malevolent and compromised nodes.

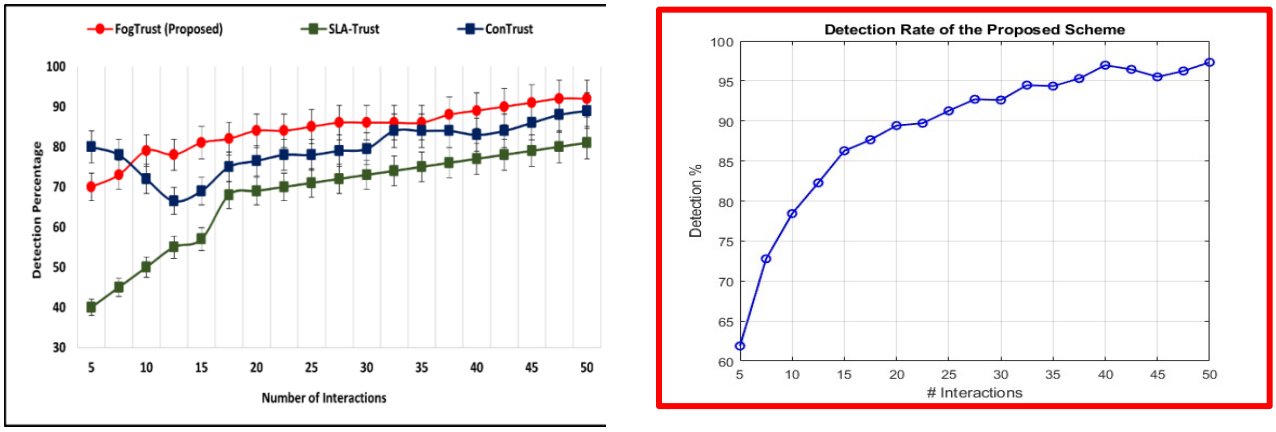

Figure 4: Comparison of three trust model with proposed Model

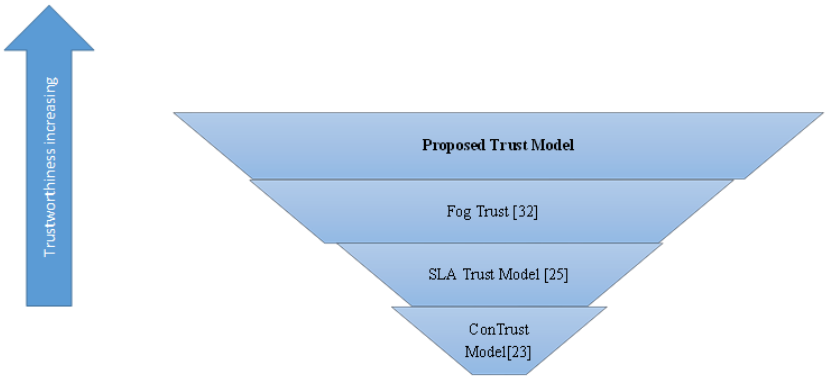

Figure 5**.** The Trustworthiness Comparison of Fog Trust with Exiting Approaches

4.4. Good Mouthing and Bad Mouthing Attack

Given section cover the comparative simulation outcome Vs good and bad mouthing attack. The trust has fixed threshold which fall between 0.0 & 1.0.Trust is set to 0.5 by default, and Time (s) is 100. To evaluate the effectiveness of the suggested strategy

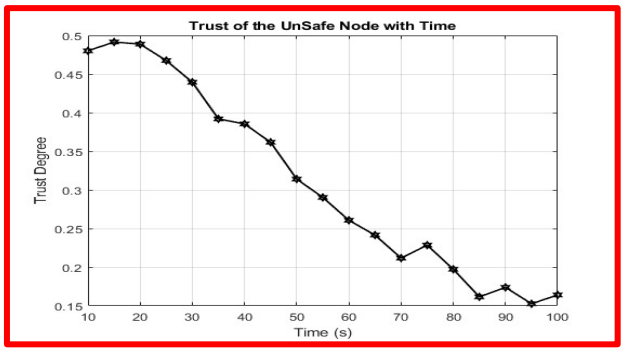

Figure 6: Result Analysis against Mouthing Attack

We implemented three trust management strategies to guard against good mouth assaults. Figure 6 illustrates how trust levels decrease over time as the quantity of unfavorable recommendations rises.

5. Conclusion

Many companies use the Internet of Things (IOT), however IoT nodes sometimes find it difficult to maintain security on their own, leaving them vulnerable to many types of assaults. Many privacy and trust management procedures are in place to help reduce these concerns. Nevertheless, several aspects of central authority trust management, including trust agents, and central trust authority communications are overlooked by existing methods. When it comes to controlling trust in fog computing's communication with Internet of Things devices, the suggested Trust Management System works well. Although other trust management strategies have been put forth, they don't take into account the establishment of a centralised trust authority prior to the fog layer. By lessening the computing burden on IoT nodes, this centrally trust authority increase accuracy which reduces risk and offer standard security. The total no. of malicious node detected ranges from 50% to 75% in the suggested Trust Management System technique when compared to current methods.

References

[1] Koohang, A.; Sargent, C.S.; Nord, J.H.; Paliszkiewicz, J. Internet of Things (IoT): From awareness to continued use. *Int. J. Inf. Manag.* **2022**, *62*, 102442. Ashton, K. That ‘internet of things’ thing. *RFID J.* **2009**, *22*, 97–114.

[2] Abid, M.A.; Afaqui, N.; Khan, M.A.; Akhtar, M.W.; Malik, A.W.; Munir, A.; Ahmad, J.; Shabir, B. Evolution towards smart and software-defined internet of things. *AI* **2022**, *3*, 100–123.

[3] Babangida, L.; Perumal, T.; Mustapha, N.; Yaakob, R. Internet of Things (IoT) Based Activity Recognition Strategies in Smart Homes: A Review. *IEEE Sens. J.* **2022**, *22*, 8327–8336.

[4] Trovato, V.; Sfameni, S.; Rando, G.; Rosace, G.; Libertino, S.; Ferri, A.; Plutino, M.R. A Review of Stimuli-Responsive Smart Materials for Wearable Technology in Healthcare: Retrospective, Perspective, and Prospective. *Molecules* **2022**, *27*, 5709.

[5] Awan, K.A.; Ud Din, I.; Almogren, A.; Almajed, H. AgriTrust—A trust management approach for smart agriculture in cloud-based internet of agriculture things. *Sensors* **2020**, *20*, 6174.

[6] Mishra, V.K.; Tripathi, R.; Tiwari, R.G.; Misra, A.; Yadav, S.K. Issues, Challenges, and Possibilities in IoT and Cloud Computing. In *Proceedings of the International Conference on Computational Intelligence in Pattern Recognition*; Springer: Singapore, 2022; pp. 326–334.

[7] George, A.; Ravindran, A.; Mendieta, M.; Tabkhi, H. Mez: An adaptive messaging system for latency-sensitive multi-camera machine vision at the IoT edge. *IEEE Access* **2021**, *9*, 21457–21473.

[8] Bhat, S.A.; Huang, N.F.; Sofi, I.B.; Sultan, M. Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability. *Agriculture* **2021**, *12*, 40.

[9] Farhan, L.; Kharel, R.; Kaiwartya, O.; Quiroz-Castellanos, M.; Alissa, A.; Abdulsalam, M. A concise review on Internet of Things (IoT)-problems, challenges and opportunities. In *Proceedings of the 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*, Budapest, Hungary, 18–20 July 2018; pp. 1–6.

[10] Abiodun, O.I.; Abiodun, E.O.; Alawida, M.; Alkhawaldeh, R.S.; Arshad, H. A review on the security of the internet of things: Challenges and solutions. *Wirel. Pers. Commun.* **2021**, *119*, 2603–2637.

[11] Din, I.U.; Guizani, M.; Hassan, S.; Kim, B.S.; Khan, M.K.; Atiquzzaman, M.; Ahmed, S.H. The Internet of Things: A review of enabled technologies and future challenges. *IEEE Access* **2018**, *7*, 7606–7640.

[12] Zhang, J.; Shen, C.; Su, H.; Arafin, M.T.; Qu, G. Voltage over-scaling-based lightweight authentication for IoT security. *IEEE Trans. Comput.* **2021**, *71*, 323–336.

[13] Ouaddah, A.; Mousannif, H.; Abou Elkalam, A.; Ouahman, A.A. Access control in the Internet of Things: Big challenges and new opportunities. *Comput. Netw.* **2017**, *112*, 237–262.

[14] Sahay, R.; Meng, W.; Estay, D.S.; Jensen, C.D.; Barfod, M.B. CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships. *Future Gener. Comput. Syst.* **2019**, *100*, 736–750.

[15] Garg, S.; Kaur, K.; Kaddoum, G.; Garigipati, P.; Aujla, G.S. Security in IoT-driven mobile edge computing: New paradigms, challenges, and opportunities. *IEEE Netw.* **2021**, *35*, 298–305.

[16] Mishra, V.K.; Tripathi, R.; Tiwari, R.G.; Misra, A.; Yadav, S.K. Issues, Challenges, and Possibilities in IoT and Cloud Computing. In *Proceedings of the International Conference on Computational Intelligence in Pattern Recognition*; Springer: Singapore, 2022; pp. 326–334.

[17] Tanwar, S.; Gupta, N.; Iwendi, C.; Kumar, K.; Alenezi, M. Next Generation IoT and Blockchain Integration. *J. Sens.* **2022**, *2022*, 9077348.

[18] Mendieta, M.; Neff, C.; Lingerfelt, D.; Beam, C.; George, A.; Rogers, S.; Ravindran, A.; Tabkhi, H. A Novel Application/Infrastructure Co-design Approach for Real-time Edge Video Analytics. In *Proceedings of the 2019 SoutheastCon*, Huntsville, AL, USA, 11–14 April 2019; pp. 1–7.

[19] Haseeb, K.; Alzahrani, F.A.; Siraj, M.; Ullah, Z.; Lloret, J. Energy-Aware Next-Generation Mobile Routing Chains with Fog Computing for Emerging Applications. *Electronics* **2023**, *12*, 574.

[20] Saad, Z.M.; Mhmood, M.R. Fog computing system for internet of things: Survey. *Tex. J. Eng. Technol.* **2023**, *16*, 1–10.

[21] Ruan, H.; Gao, H.; Qiu, H.; Gooi, H.B.; Liu, J. Distributed operation optimization of active distribution network with P2P electricity trading in blockchain environment. *Appl. Energy* **2023**, *331*, 120405.

[23] Gupta, P.; Saini, D.K. Introduction to Optimization in Fog Computing. In *Bio-Inspired Optimization in Fog and Edge Computing Environments*; Auerbach Publications: New York, NY, USA, 2023; pp. 1–24.

[23] Latif, R. ConTrust: A novel context-dependent trust management model in social Internet of Things. *IEEE Access* **2022**, *10*, 46526–46537.

[24] Kar, B.; Yahya, W.; Lin, Y.D.; Ali, A. Offloading using Traditional Optimization and Machine Learning in Federated Cloud-Edge-Fog Systems: A Survey. *IEEE Commun. Surv. Tutor.* **2023**.

[24] Chang, V.; Sidhu, J.; Singh, S.; Sandhu, R. SLA-based Multi-dimensional Trust Model for Fog Computing Environments. *J. Grid Comput.* **2023**, *21*, 1–19.

[26] Din, I.U.; Bano, A.; Awan, K.A.; Almogren, A.; Altameem, A.; Guizani, M. LightTrust: Lightweight trust management for edge devices in industrial internet of things. *IEEE Internet Things J.* **2021**.

[27] George, A.; Ravindran, A. Scalable approximate computing techniques for latency and bandwidth constrained IoT edge. In *Proceedings of the International Summit Smart City 360°*; Springer: Cham, Switzerland, 2021; pp. 274–292.

[28] Al Muhtadi, J.; Alamri, R.A.; Khan, F.A.; Saleem, K. Subjective logic-based trust model for fog computing. *Comput. Commun.* **2021**, *178*, 221–233.

[29] Baghalzadeh Shishehgarkhaneh, M.; Keivani, A.; Moehler, R.C.; Jelodari, N.; Roshdi Laleh, S. Internet of Things (IoT), Building Information Modeling (BIM), and Digital Twin (DT) in Construction Industry: A Review, Bibliometric, and Network Analysis. *Buildings* **2022**, *12*, 1503.

[30] Rahman, F.H.; Au, T.W.; Newaz, S.S.; Suhaili, W.S. Trustworthiness in fog: A fuzzy approach. In *Proceedings of the 2017 VI International Conference on Network, Communication and Computing*, Kunming, China, 8–10 December 2017; pp. 207–211.

[31] Namal, S.; Gamaarachchi, H.; MyoungLee, G.; Um, T.W. Autonomic trust management in cloud-based and highly dynamic IoT applications. In *Proceedings of the 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015)*, Barcelona, Spain, 9–11 December 2015; pp. 1–8.

[32] Al-Khafajiy, M.; Baker, T.; Asim, M.; Guo, Z.; Ranjan, R.; Longo, A.; Puthal, D.; Taylor, M. COMITMENT: A fog computing trust management approach. *J. Parallel Distrib. Comput.* **2020**, *137*, 1–16.

[33] Alemneh, E.; Senouci, S.M.; Brunet, P.; Tegegne, T. A two-way trust management system for fog computing. *Future Gener. Comput. Syst.* **2020**, *106*, 206–220.

[34] Dhelim, S.; Kechadi, T.; Aung, N.; Ning, H.; Chen, L.; Lakas, A. Trust2Vec: Large-Scale IoT Trust Management System based on Signed Network Embeddings. *arXiv* **2022**, arXiv:2204.06988.

[35] Ogundoyin, S.O.; Kamil, I.A. A trust management system for fog computing services. *Internet Things* **2021**, *14*, 100382.