SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I12P120

Volume 11 Issue 12, 229-234, December 2024

Original Article

Securing Fog Computing Networks: An Advanced Trust Management System Leveraging Fuzzy Techniques and Hierarchical Evaluation

Shradhdha Thakkar[1], Jaykumar A. Dave[2]

[1]*Department of Computer Engineering, Sankalchand Patel University, Gujarat, India.*
[2]*Department of Computer Engineering, Silver Oak University, Gujarat, India.*

[1]*Corresponding Author : shraddhaspce@gmail.com*

Received: 11 October 2024 Revised: 12 November 2024 Accepted: 10 December 2024 Published: 31 December 2024

Abstract *- This paper presents a Trust Management System (TMS) designed to counteract cyber-attacks in fog computing environments. The system integrates fuzzy AHP, hierarchical PROMETHEE methods, and fuzzy ranking to evaluate trust based on Quality of Service (QoS), Quality of Security (QoSec), and economic factors. Tested against Replay, On-Off, Bad-mouthing, and Ransomware attacks, the system demonstrates high detection accuracy, with error rates between 3.50% and 4.15%. The results show that the proposed TMS effectively enhances security and trust evaluation in fog computing networks.*

Keywords *- Trust Management System (TMS), Fuzzy Analytical Hierarchy Process (AHP), Quality of Service (QoS), Quality of Security (QoSec).*

1. Introduction

As Cyber-attacks become increasingly sophisticated and pervasive, ensuring the security and integrity of computing systems is more critical than ever. Fog computing, which extends cloud computing services to the edge of the network, is particularly vulnerable due to its decentralized nature. Trust Management Systems (TMS) have emerged as a key solution for safeguarding interactions among distributed nodes in such environments.

This paper presents a novel Trust Management System that leverages a combination of fuzzy Analytical Hierarchy Process (AHP) to assess trustworthiness based on multiple criteria, including Quality of Service (QoS), Quality of Security (QoSec), and economic factors. By addressing various types of cyber-attacks, such as Replay, On-Off, Bad-mouthing, and Ransomware attacks, the proposed Trust Management system enhances the detection and mitigation of threats, ensuring secure and efficient operations in fog computing environments.

The research findings highlight the system's robustness, which improves security and optimizes trust evaluations, providing a framework for future advancements in trust management in fog computing. In this research paper, we have implemented a Trust Management System for FOG computing to check the trustworthiness of a particular node.

1.1. Motivation

1.1.1. Surge in Cybercrime Costs

The World Economic Forum Annual Meeting 2024 will occur in Davos-Klosters, Switzerland, from 15–19 January. The World Economic Forum Annual Meeting 2024 in Davos will likely prioritize discussions on global cybersecurity threats, as highlighted by the image showing a dramatic rise in the cost of cybercrime. According to the chart, cybercrime costs are projected to surge from $8.44 trillion in 2022 to $23.82 trillion by 2027, emphasizing the urgent need for enhanced global collaboration and innovation in cybersecurity. The meeting will focus on strengthening cyber resilience, preventing economic disruptions, and protecting critical infrastructure. With these escalating figures, leaders will explore strategies to mitigate risks and address the economic impact of rising cyber threats worldwide.

1.2.1. Rising Cyber Attack Trends

The frequency of cyber-attacks has demonstrated a concerning upward trajectory over recent years. In 2019, 120 recorded attacks were recorded, with the Capital One Data Breach being a prominent incident. This number rose to 150 attacks in 2020, notably including the Garmin Ransomware Attack. The following year saw an increase to 180 attacks, highlighted by the Colonial Pipeline Ransomware incident. The trend continued in 2022 with 220 attacks, prominently featuring the Ukraine Government Cyber Attack. In 2023, the number of attacks surged to 250, with the AIIMS Ransomware

Attack in India standing out. The pattern persisted into 2024, with 270 attacks, including the significant Indian Railways Ransomware. This data underscores an escalating frequency of cyber-attacks, particularly ransomware incidents, signaling an urgent need for enhanced cyber security measures.

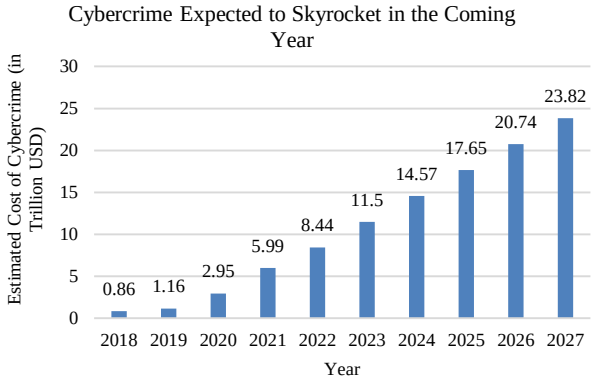


Fig. 1 Cybercrime expected as per the statistics [12]

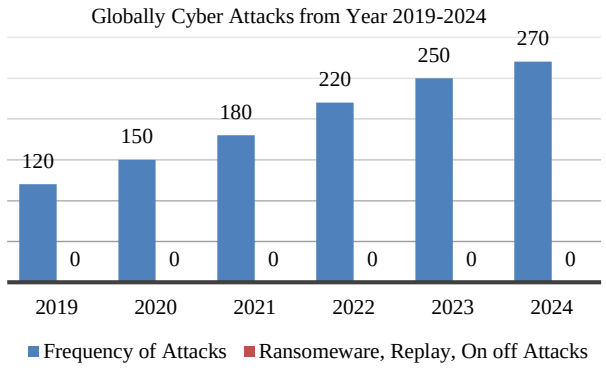


Fig. 2 Frequency of attack from the year 2019-2024 [14]

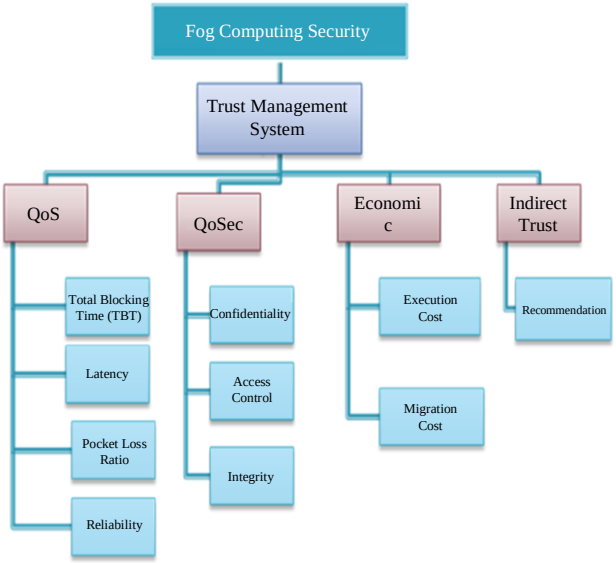


Fig. 3 Parameters to evaluate criteria

2. Proposed Trust Management System

Effective trust management ensures secure and reliable interactions among distributed nodes in fog computing. This research paper presents a novel approach to trust management by integrating the fuzzy Analytical Hierarchy Process (AHP) with hierarchical PROMETHEE methods and fuzzy ranking. The proposed system evaluates trustworthiness through a comprehensive framework that considers Quality of Service (QoS), Quality of Security (QoSec), and economic parameters. By leveraging fuzzy AHP, the model facilitates nuanced decision-making in uncertain environments, allowing for a more flexible and accurate assessment of trust based on multiple criteria.

The hierarchical PROMETHEE method further refines this evaluation by structuring trust management into a layered hierarchy, addressing various aspects of trust in fog computing environments. This approach enhances the robustness of trust assessments by systematically analyzing and prioritizing the criteria of QoS, QoSec, and economic factors. Incorporating fuzzy ranking allows for a more granular evaluation of trust, accommodating the inherent uncertainties and subjective judgments involved. This integrated trust management system improves the reliability and security of fog computing systems and optimizes economic efficiencies, paving the way for more resilient and cost-effective fog computing frameworks.

2.1. Criteria to Evaluate Qos and Qosec and Economic Parameter

Figure 3 evaluates the criteria QoS, QoSec, and Economic Parameters. QoS Total Blocking Time, Latency, Packet Loss Ratio and Reliability must be considered. For QoSec, Confidentiality, Access Control and Integrity are considered Economic and Indirect Trust. We will assign weight to each parameter by getting priority from the trust management system and accessing weighted parameters using a multi-criteria decision-making method.

3. Algorithm for Trust Management System

3.1. Input Data Collection

- Step 1.1: Collect data on Quality of Service (QoS), Quality of Security (QoSec), and economic parameters from the fog computing environment.

3.2. Fuzzy AHP Analysis

- Step 2.1 : Convert qualitative data into fuzzy values to handle uncertainty in input parameters.
- Step 2.2 : Apply fuzzy AHP to establish priorities and weights for each criterion based on fuzzy values.
- Step 2.3 : Compute the weighted scores for each alternative.

3.3. Hierarchical PROMETHEE Method

- Step 3.1 : Structure the criteria into a hierarchical framework based on the fuzzy AHP results.

- Step 3.2 : Apply the PROMETHEE method to rank alternatives by comparing them based on the weighted scores.
- Step 3.3 : Determine the preference and ranking of alternatives through PROMETHEE's various ranking methods (e.g., PROMETHEE I, PROMETHEE II).

3.4. Fuzzy Ranking

- Step 4.1 : Rank the alternatives using fuzzy logic to address the uncertainties in the evaluation.
- Step 4.2 : Aggregate the rankings to obtain a final trust score for each alternative.

3.5. Trust Evaluation

- Step 5.1 : Aggregate the results from fuzzy ranking to assess the overall trustworthiness of each alternative.
- Step 5.2 : Generate trust scores and recommendations based on the aggregated results.

3.6. Output

- Step 6.1 : Present the trust scores and recommendations in a user-friendly format.
- Step 6.2 : Provide actionable insights and recommendations for improving trust management in the fog computing environment.

3.7. End

4. Results

4.1. Trust System Detection Efficiency

The following result shows the detection rate of unsafe nodes using the proposed trust management system, where the detection rate improves as the number of interactions increases. The detection rate starts at around 60% for five interactions and steadily rises, reaching close to 100% at 50 interactions. The system significantly improves after 10 interactions, achieving over 95% detection.

4.2. Trust Growth over Time

The graph demonstrates the increasing trustworthiness of a safe node over time using the proposed trust management system. The trust degree starts at approximately 0.65 at 10 seconds and steadily rises, reaching nearly 1 by 60 seconds, where it stabilizes. This indicates that the proposed system effectively increases the trust in safe nodes over time. Concurrently, this suggests a reduction in trust for unsafe nodes as the system becomes more capable of distinguishing safe behavior.

4.3. Comparison of Proposed Model Result with Other Research Work

To compare our proposed model, we have considered three base papers that have already implemented trust management systems using different parameters. Con Trust Model [12], SLA Trust Model [18], and Fog Trust [4] these three Trust Management Systems results compared with the results of the proposed trust management system, and we get better results from all three previous results for our trust management system which is shown in the following Figure 7. It clearly shows that the detection rate of malicious nodes is increasing upto 98% in the proposed model, which was previously about 85%.

4.4. Limitations of Previous Trust Models

In the previous trust model, they focused only on QoS, QoSec and Indirect Trust, but the innovation in our trust management system as we have considered the economic parameters also, which will consider migration cost and execution cost, which will decrease the overall cost of offloading the task.

4.5. Performance of Proposed Trust Management System against different Attack

To compare the performance of the Trust Management System against different attacks, we consider four attacks: Replay Attack, On-off attack, Bad-mouthing attack and Ransomware attack. By considering all the mentioned attacks, we have detected malicious and infectious nodes against the proposed trust management system, as shown in the following figure.

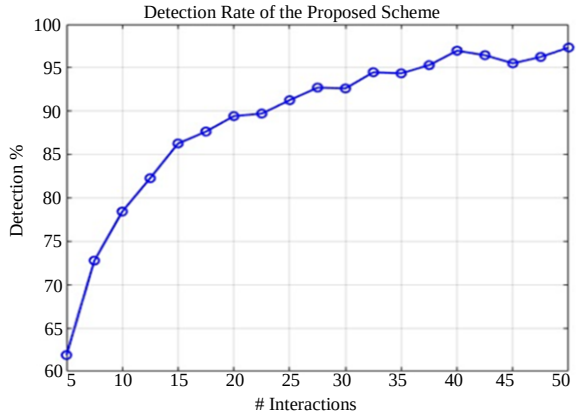


Fig. 4 Malicious node Detection rate

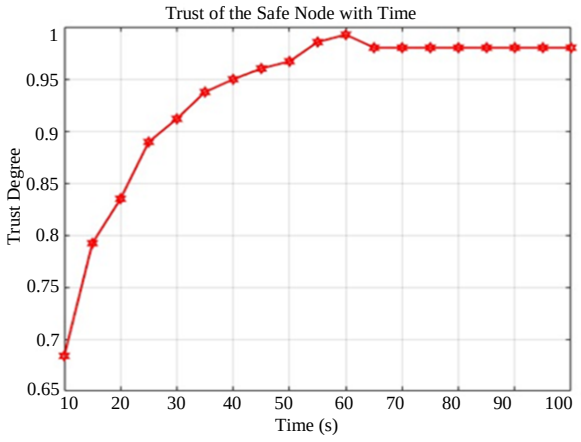


Fig. 5 Trust degree increases with safe node

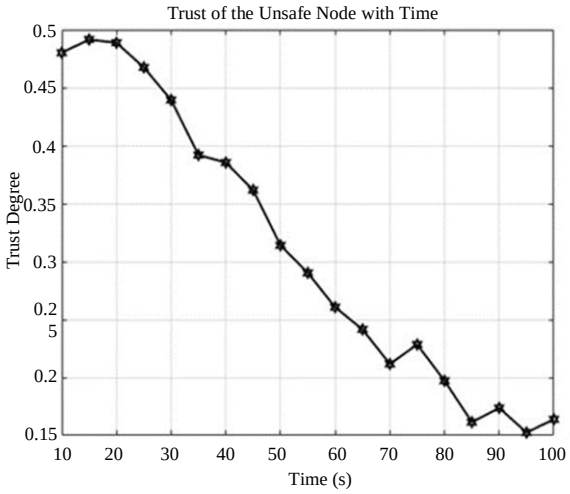
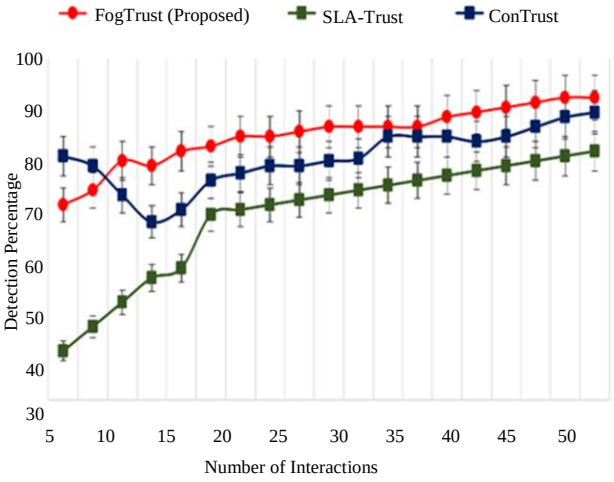


Fig. 6 Trust degree decrease with unsafe node



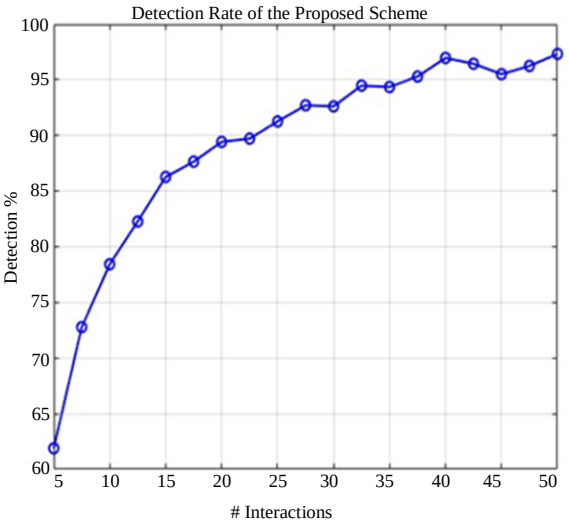


Fig. 7 Comparison with results of previous research

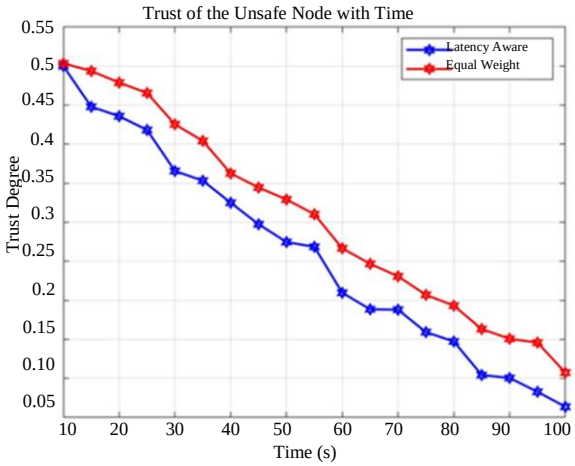


Fig. 8 Trust degree is decreasing with attacks

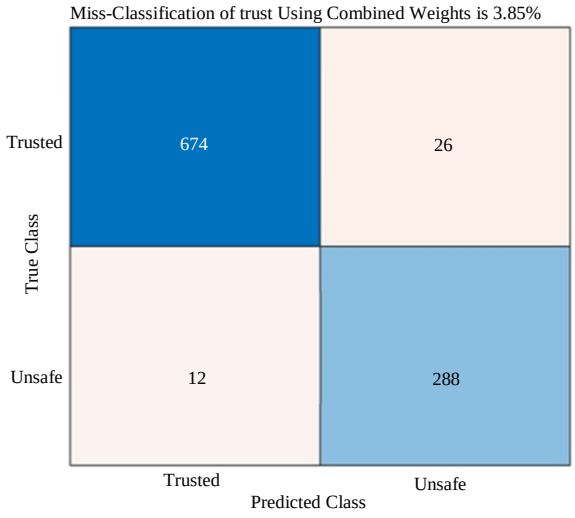


Fig. 9 Accuracy of trust management system

5. Error Classification Rate of Trust Management system

The confusion matrix provides a structured representation of the performance of a classification model by comparing predicted outcomes against actual outcomes.

- True Positive (TP) : These are the correctly identified positive cases.
- False Positive (FP) : These cases were incorrectly classified as positive when they were negative.
- True Negative (TN) : These are the correctly identified negative cases.
- False Negative (FN) : These are cases incorrectly classified as negative when they were actually positive.

5.1. Misclassification Rate

Total Instances = 100
True Positive (TP) = 674

False Positive (FP) = 12
True Negative (TN) = 288
False Negative (FN) = 26
Misclassification Rate = (FP + FN) / Total Instances
= {12 + 26}/{100} = 0.38 or 3.85%

This Rate indicates that approximately 3.85% of instances were misclassified, predicting positives as negatives or negatives as positives.

6. Trust Management System and Cyber Attacks

The risks and attacks that threaten nodes' ability to launch an attack in an IoT network are covered in this section. Internal attacks are another name for these attacks. Since they capture the node and induce it to believe what the attacker wants, they are more unsafe and serious than external attacks. The Trust Management Model is one of the most widely used strategies for repelling trust-based attacks. Serious threats such as on-off assaults, sybil attacks, denial-of-service attacks, wormhole attacks, bad-mouthing attacks, self-promotion attacks, and selfish attacks can be thwarted by these approaches. Only one kind of assault at a time can be detected by the attack-specific techniques that have been suggested in the literature. Designing will be the focus of future research.

6.1. On-Off Attacks

In IoT networks, these are one kind of internal assault that is more frequent. The attacker nodes vary their behaviour in order to question the trust. They act predictably in one moment and unpredictably in another. Trust management models often talk about, identify, and handle these attacks [10]. The model must consider the node's timely behaviour while trust assessment to detect them accurately and quickly. In order to protect from these kinds of well-known assaults, most research utilised time-based behaviour assessment of nodes. The nodes switch often, making it difficult to spot and stop them. However, adding ageing and remembering effects can be useful for precise and simple diagnosis.

6.2. Bad-Mouthing

We address this in [3]. In order to increase the trust of other malicious nodes, those with malicious intent attempt to give fraudulent suggestions regarding the goodwill of their peers. Recognising these kinds of assaults can be accomplished by employing significant entropy levels to identify false suggestions due to low trust scores.

6.3. Sybil Attacks

Using a fictitious ID to access network features. Verifying identity as a defence against trust-based assaults can be successful.

6.4. Ransomware Attack

A ransomware attack in a fog trust management system can compromise the security and trust relationships between fog nodes and edge devices. Such attacks could disrupt data integrity, causing delays or failures in critical real-time processing. Effective trust management and robust security protocols are essential to protect against these threats in fog computing environments.

6.5. Replay Attack

A replay attack in a fog trust management system involves intercepting and reusing valid data transmissions to impersonate legitimate devices or nodes. This can compromise trust relationships, allowing attackers to disrupt communication and manipulate data. Strong encryption and time-sensitive authentication mechanisms can help mitigate these attacks in fog computing networks.

6.6. DDoS

It is a kind of attack where excessive packets are sent to the target, disrupting the program's services. As an illustration, consider a mob of people blocking the entrance to an establishment, preventing authorised individuals like owners and staff from entering and giving the impression that they are the service supplier. Consequently, it influences the system's trust. Updating trust regularly is an inefficient way to identify these assaults. As a result, based on events, trust updates can aid in precisely detecting these kinds of assaults. This paper has considered four cyber-attacks named Replay Attacks, On-Off Attacks, Bad-Mouthing Attacks and Ransomware Attacks, based on various literature reviews. The Trust Management system has tested for these four attacks, and as a result, the accuracy of the Trust Management system is as per the following result. The image is a bar graph depicting the Trust Management System's classification error rates for different types of cyberattacks in a fog computing system. The attacks include Replay Attacks (4.02%), On-Off Attacks (4.15%), Bad-Mouthing Attacks (3.50%), and Ransomware Attacks (3.93%). The On-Off Attack has the highest classification error, while the Bad-Mouthing Attack has the lowest.

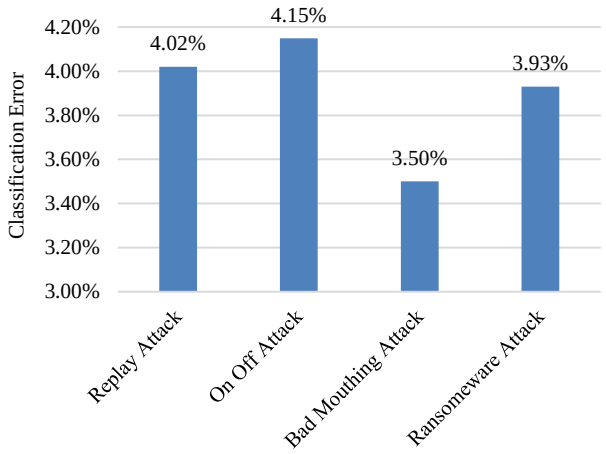


Fig. 10 Accuracy of trust management system with different attacks

7. Conclusion

This paper presents a novel Trust Management System (TMS) designed to address security challenges in fog computing environments. By integrating fuzzy AHP, hierarchical PROMETHEE methods, and fuzzy ranking, the proposed system offers a robust framework for evaluating trust based on QoS, QoSec, and economic factors. The system has been tested against various cyberattacks, including Replay, On-Off, Bad-Mouthing, and Ransomware attacks, demonstrating high detection accuracy with error rates ranging between 3.50% and 4.15%. The results highlight the effectiveness of the proposed TMS in enhancing security and trust evaluation in fog computing networks. Future research may explore further enhancements to the system's accuracy and efficiency, potentially incorporating additional attack scenarios and advanced machine learning techniques.

Acknowledgement

We thank the various institutions and colleagues who provided valuable support and resources throughout this research. We also appreciate the assistance provided in data collection, testing and analysis.

References

[1] Arwa Alrawais et al., "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34-42, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ravi Yadav, and Gaurav Baranwal, "An Efficient Trust Management Using Feedback Credibility Evaluation Method in Fog Computing," *Simulation Modelling Practice and Theory*, vol. 120, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Ivan Stojmenovic et al., "An Overview of Fog Computing and its Security Issues," *Concurrency and Computation Practice and Experience*, vol. 28, no. 10, pp. 2991-3005, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[4] Farhana Jabeen et al., "Adaptive and Survivable Trust Management for Internet of Things systems," *IET Information* Security, vol. 15, no. 5, pp. 375-394, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mohammed Al-khafajiy et al., "COMITMENT: A Fog Computing Trust Management Approach," *Journal of Parallel and Distributed Computing*, vol. 137, pp. 1-16, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Fatin Hamadah Rahman et al., "EnTruVe: Energy and Trust-Aware Virtual Machine Allocation in Vehicle Fog Computing for Catering Applications in 5G," *Future Generation Computer Systems*, vol. 126, pp. 196-210, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Sunday Oyinlola Ogundoyin, and Ismaila Adeniyi Kamil, "A Fuzzy-AHP Based Prioritization of Trust Criteria in Fog Computing Services," *Applied Soft Computing*, vol. 97, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Esubalew Alemneh et al., "A Two-Way Trust Management System for Fog Computing," *Future Generation Computer Systems*, vol. 106, 206-220, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Mohammad Aazam, Pham Phuoc Hung, and Eui-Nam Huh, "Smart Gateway Based Communication for Cloud of Things," *2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, Singapore, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[10] Sakshi Bhardwaj, and Sonia Tomer, "Fog Computing: A Survey," *International Journal of Engineering Research & Technology (IJERT)*, vol. 5, no. 3, 2017. [Google Scholar] [Publisher Link]

[11] Salvatore J. Stolfo, Malek Ben Salem, and Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," *2012 IEEE Symposium on Security and Privacy Workshops*, San Francisco, CA, USA, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[12] Yingjuan Shi et al., "The Fog Computing Service for Healthcare," *2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech)*, Beijing, China, pp. 1-5, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[13] Md Raseduzzaman Ruman et al., "IoT Based Emergency Health Monitoring System," *2020 International Conference on Industry 4.0 Technology (I4Tech*), Pune, India, pp. 159-162, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Qingsong Xie et al., "Machine Learning Methods for Real-Time Blood Pressure Measurement Based on Photoplethysmography," *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*, Shanghai, China, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[15] Kelvin K.F. Tsoi et al., "Blood Pressure Monitoring on the Cloud System in Elderly Community Centres: A Data Capturing Platform for Application Research in Public Health," *2016 7th International Conference on Cloud Computing and Big Data (CCBD)*, Macau, China, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[16] Flavio Bonomi et al., "Fog Computing and its Role in the Internet of Things," *Proceedings of the first Edition of the MCC Workshop on Mobile Cloud Computing*, pp. 13-16, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[17] Zhibo Pang et al., "Design of a Terminal Solution for Integration of In-Home Health Care Devices and Services towards the Internet-of-Things," *Enterprise Information Systems*, vol. 9, no. 1, pp. 86-116, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[18] Ramón C. Hermida et al., "Decreasing Sleep-Time Blood Pressure Determined by Ambulatory Monitoring Reduces Cardiovascular Risk," *Journal of American College of Cardiology*, vol. 58, no. 11, pp. 1165-1173, 2011. [Google Scholar] [Publisher Link]