Enhancing Trustworthiness in Fog Computing: A Multi-Criteria Approach for EEG Applications

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. Jaykumar 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

In this research, we investigate how to include a Trust Management System (TMS) into fog computing—a decentralized computing architecture that expands cloud computing's capabilities to the edge of a network. We conduct an inquiry into the application and evaluation of a new multi-criteria trust mechanism designed specifically for fog computing settings. This approach, which combines "soft trust" with "hard trust," is essential to assessing and controlling the dependability and credibility of entities in the fog computing environment. We discover that the implementation of trust models in this setting improves the reliability and usefulness of Electroencephalography (EEG) applications in various domains, including neurology and clinical medicine. Additionally, these models aid in the creation of implementations that are safe, intuitive, and compliant with ethical standards.

Keywords: Cloud Computing, Cloud, Data Center, Fog Computing, Trust, EEG, MCDM.

INTRODUCTION

"Soft trust" and "hard trust" are two distinct methods or degrees of evaluating and managing the trust connections betweenentities in the fog computing environment.

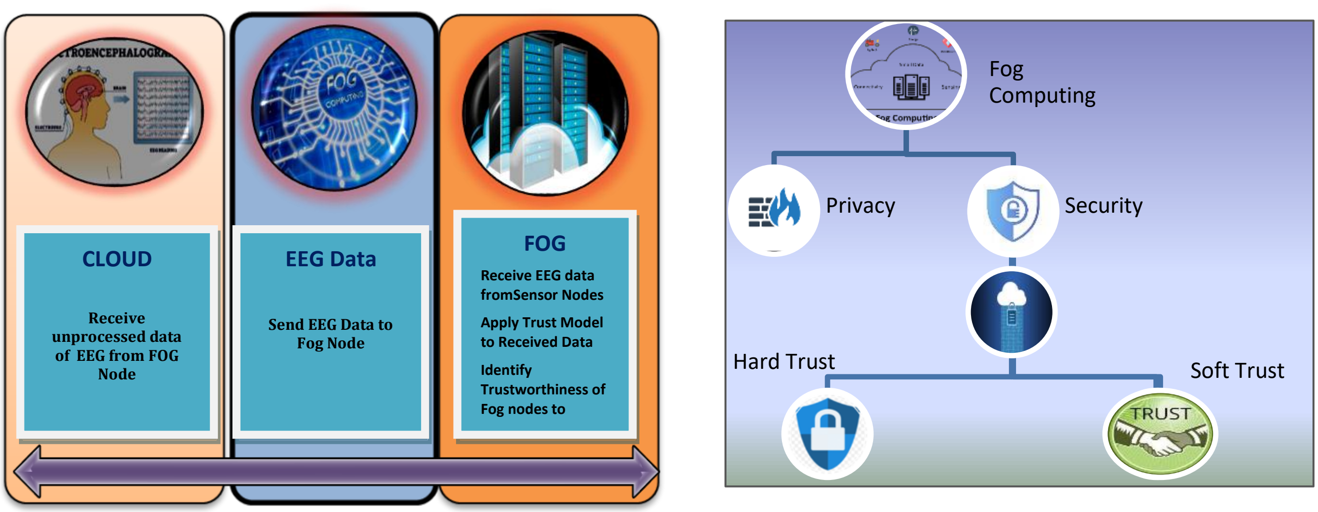

Figure 1. Flow of Research Work

HARD TRUST:

Hard trust, often referred to as quantitative trust, entails giving trust relationships a numerical or quantitative value based on particular measurements, criteria, or observations. These measurements may take into account past behavior, security settings, dependability, and other factors. The trust values are frequently expressed as numerical scores, which can be used to decision-making, task prioritization, or resource access.

Hard trust in fog computing refers to the formalization of a system where trust levels are determined by algorithms, data analysis, and predetermined criteria[23]. This strategy is more methodical and enables precise decision-making based on measurements that can be measured.

SOFT TRUST:

The assessment of trust relationships using subjective or qualitative criteria is the topic of soft trust, sometimes referred to as qualitative trust. Soft trust is based on ideas likereputation, context, recommendations, and personal judgments rather than awarding numerical rankings. The nature of interactions[33], relationships, and the degree of familiarity between entities are all taken into account by this method, which may make it difficult to quantify some of these characteristics.

In fog computing, determining whether an entity can be trusted may involve weighing context, considering suggestions from reliable peers, and relying on personal experiences and insights. This method, which takes into account the "feel" of trust rather than depending exclusively on quantifiable facts, is more intuitive and human-centered.

Hard and soft trust each have their benefits and drawbacks. For applications requiring consistent and unbiased decision-making, hard trust offers a more methodical and quantitative technique of evaluating trust. On the other hand, soft trust can be more flexible to complicated and changing circumstances since it captures the subjective nuances of trust relationships.

In reality, both strategies may be used, wit

h hard trust mechanisms serving as a base for impartial trust evaluation and soft trust mechanisms allowing for the inclusion of contextual knowledge and human judgment in the trust management process[26]. The precise requirements and characteristics of the fog computing environment and its applications determine whether to use hard or soft trust.

IMPLEMENTATION AND RESULTS

Trust Management System (TMS)

In fog computing, a Trust Management System (TMS) is a mechanism that evaluates and controls the dependability and trustworthiness of entities in the environment. These entities may include users, devices, applications, and services. To maintain the security, privacy, and proper operation of the system, trust management is essential since fog computing uses decentralized and dispersed computing resources

The operation of a trust management system in the context of fog computing is as follows:

Trust Establishment: Establishing the initial trust level of entities joining the fog computing environment is the responsibility of the TMS. This could entail checking the devices' validity, validating their security settings, and evaluating their previous behavior.

Trust Metrics: Trust measures are frequently used to measure trust. These indicators might take into account things like prior behavior, reputation, security posture, and policycompliance. For each entity, the TMS calculates trust scores by gathering and analyzing data.

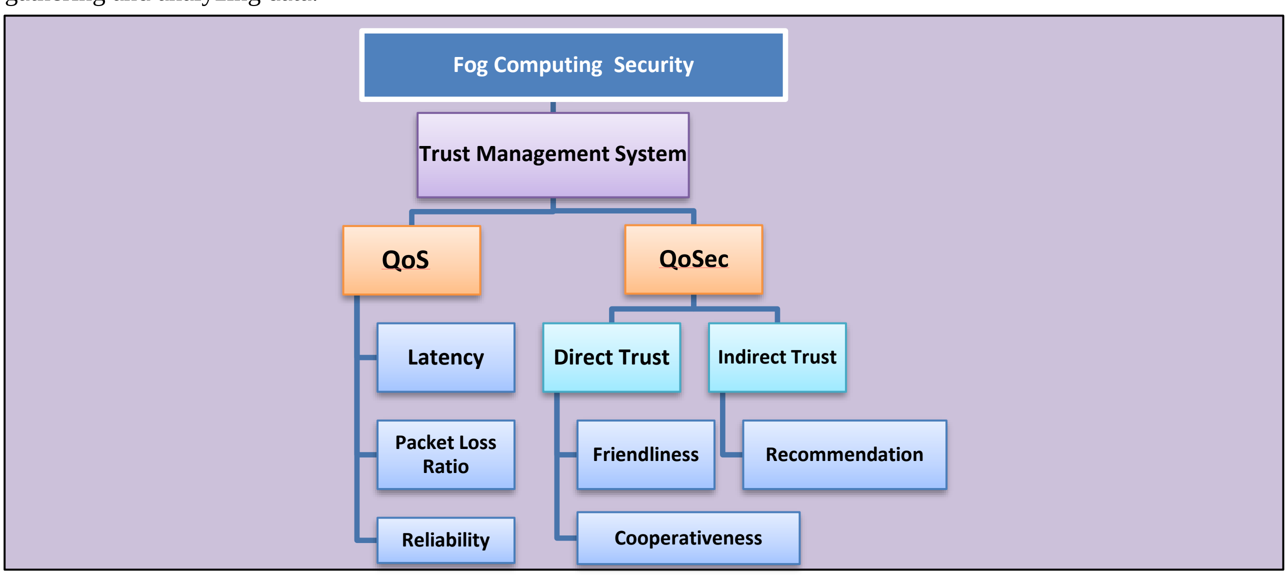

Figure 2 Trust Management System Evaluation Parameters

Trust Updating: Trust is dynamic; it changes over time in response to how different entities behave and interact with one another. Based on in-the-moment observations and input from other entities, the TMS continuously updates trust scores.

Trust Aggregation: In fog computing, several entities communicate with one another. The TMS compiles trust data from many sources to create a comprehensive picture of an entity's trustworthiness. This can entail integrating first-hand observations, peer feedback, and historical data.

Trust-based Decision Making: Applications and services for fog computing can use trust scores to make better informed decisions. A device with a high trust score, for instance, might have its data processing activities prioritized, whereas a device with a low trust score would have its operations limited.

Dynamic Trust Management: Fog environments are dynamic, as devices often join and leave the network. By continuously evaluating and modifying trust levels as the environment changes, the TMS adjusts to these changes.

Risk Assessment: TMS can aid in risk assessment by taking into account the legitimacy of entities before granting access to vital resources or exchanging sensitive information with them. It lessens the risk of security lapses or data leakage.

Anomaly Detection: The detection of anomalies or departures from expected behavior can be aided by trustmanagement systems. A security breach may be indicated by abrupt changes in behavior or activity, and the TMS can prompt the proper responses.

Feedback Mechanism: Entities can report their interactions and experiences with other entities using a feedback system that is frequently included in TMS. This criticism aids in the evaluation of trust.

Collaborative Trust: TMS promotes inter-entity cooperation. Both direct encounters and referrals from reliable peers can have an impact on trust levels.

Fog computing requires careful design, reliable algorithms, and integration with other security methods in order to implement a Trust Management System.

PROPOSED WORK

The research suggests a brand-new multi-criteria trust mechanism for fog computing environments that can help nodes in the network regulate the security settings needed to build confidence.

By dynamically combining trust information from the nodes and the suggestions from nearby nodes to compute the final trust value, the event-based and distributed trust management system can evaluate a fog node's level of trust by taking into account the QoS (Quality of Services), Quality of security (QoSec), and social trust indicators. This trust can then be transferred to the cloud so that other nodes can request it in real-time.

QoS (Quality of Services) Result:

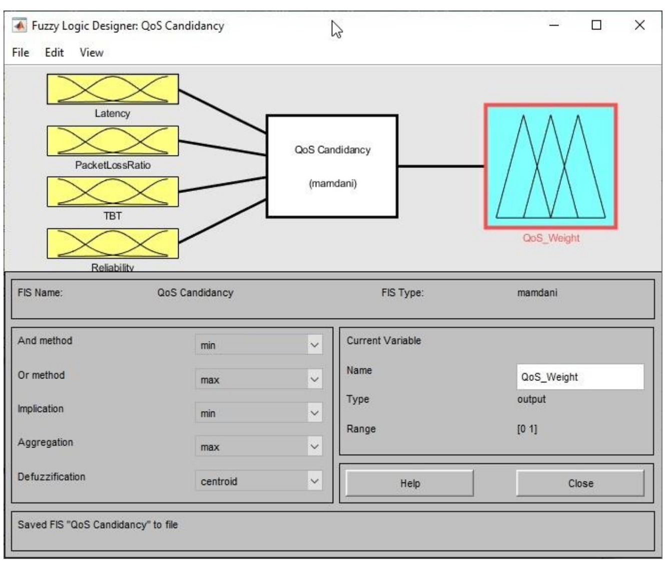

Figure 3 Quality of Service Candidancy

Additionally, a dynamic weight assignment technique will be used in conjunction with a multi-criteria decision-making system to update the offloaded state continually.

Quality of security (QoSec) Result:

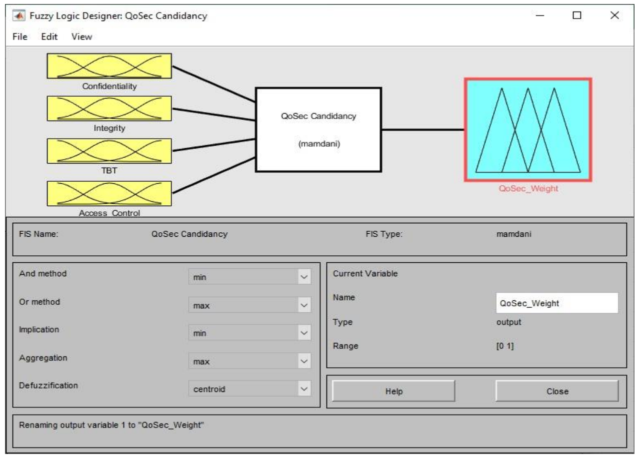

Figure 4 Quality of Security Candidancy

These entities may include users, devices, applications, and services. To maintain the security, privacy, and proper operation of the system, trust management is essential since fog computing

METHOD USED FOR IMPLEMENTATION

FUZZY MULTIPLE CRITERIA DECISION MAKING (MCDM) METHODS

Numerous industries, such as engineering, finance, environmental management, and healthcare, where decision-makers must take into account a number of factors and deal with uncertainty and imprecision, can benefit from the use of fuzzy MCDM methods[47]. When dealing with complicated and uncertain real-world challenges, these strategies can assist in helping to make more informed and resilient decisions by providing a systematic framework for decision analysis

In order to handle imprecise or uncertain information in the decision-making process, fuzzy multiple criteria decision making (MCDM) approaches are a group of decision-making strategies that use fuzzy logic. When choice criteria and options require subjective judgments, ambiguity, or vagueness, these strategies are very helpful. Fuzzy MCDM techniques assist decision-makers in making decisions that are more solid and reflective of complexity in the real world.

Here are some essential ideas and well-liked fuzzy MCDM techniques:

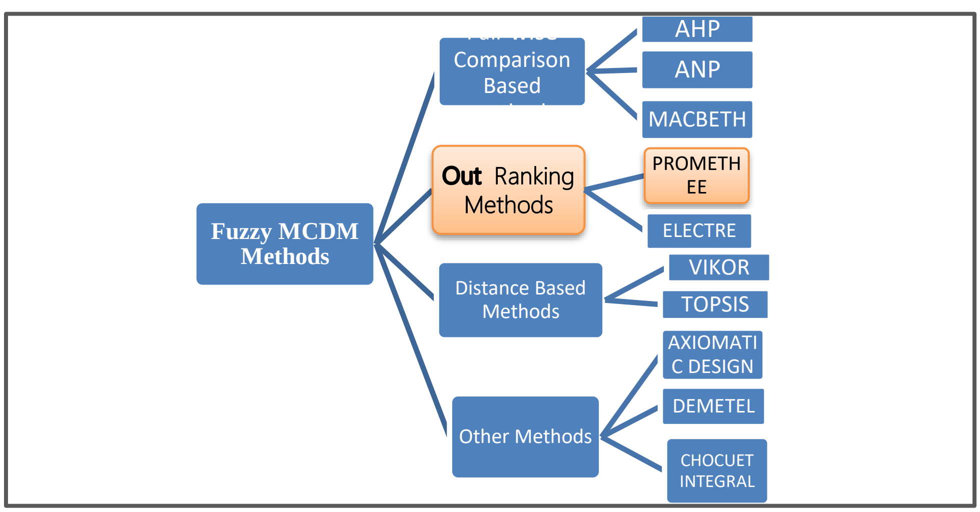

Figure5 Fuzzy Multi criteria Decision Making Methods

Fuzzy Sets: The fuzzy set theory, on which fuzzy MCDM is based, enables the representation of hazy or inaccurate information. Each element in a fuzzy set has a degree of membership, which ranges from 0 to 1, indicating how much it is a part of the set.

Fuzzy Numbers: Uncertain numerical values are represented by fuzzy numbers in decision criteria and alternative options. These numbers have a membership function that indicates the extent of their set membership.

Aggregation Methods: The aggregation methods employed by fuzzy MCDM systems to combine and evaluate fuzzy information include the weighted average, weighted sum, and fuzzy integrals.

Fuzzy Analytic Hierarchy Process (Fuzzy AHP): By including fuzzy information in pairwise comparisons and hierarchical structures, the fuzzy analytical hierarchy process (AHP) expands the conventional analytical hierarchy process (AHP). It aids in managing ambiguity and imprecision in the selection of criteria.

Fuzzy TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution): Fuzzy TOPSIS is a technique used to rank alternatives based on their proximity to the ideal solution and the anti-ideal solution. It considers both the best and worst-case scenarios for each criterion.

Fuzzy ELECTRE (Elimination and Choice Expressing Reality): The ranking of options according to how closely they resemble the ideal and anti-ideal solutions is done using fuzzy TOPSIS. For each criterion, it takes into account the ideal and the unfavorable possibilities.

Fuzzy VIKOR (VIsekriterijumsko Kompromisno Rangiranje):

A multi-criteria decision-making technique called fuzzy VIKOR seeks a compromise between competing criteria. Maximum group utility and least amount of personal regret are taken into account.

Fuzzy Decision Trees: Fuzzy logic is used into fuzzy decision trees to handle erroneous input and uncertain results, extending the capabilities of classical decision tree analysis.

Fuzzy Logic Expert Systems: These systems incorporate expert information into a fuzzy rule-based system and employ fuzzy logic to represent and address complicated decision-making issues.

PROMETHEE METHOD

The PROMETHEE family of outranking techniques, which consists of PROMETHEE I for partial ranking of the alternatives and PROMETHEE II for full ranking of the alternatives.

Its benefit is that it is simple to use. It is not necessary to assume that the standards are reasonable.Its drawbacks are that it does not offer a clear way to apply weights and that although it calls for the assignment of values, it does not offer a clear way to do so. So, PROMETHEE Method will used to evaluate parameters in our trust model.

APPLICATION OF PROPOSED TRUST MODEL

Electroencephalography, or EEG for short, is a medical test that tracks and records electrical activity in the brain. In order to recognize and capture the electrical signals generated by the brain's neurons, electrodes are applied to the scalp. The EEG machine[58] that these electrodes are commonly attached to amplifies and displays the electrical activity of the brain as a series of waveforms on a computer screen or piece of paper.

In the fields of clinical medicine and neuroscience, EEG is a useful tool. It is frequently employed for a number of things:

Diagnosing Epilepsy: The neurological condition known as epilepsy, which is marked by recurring seizures, is frequently diagnosed and monitored using EEG. Epilepsy can be detected by certain patterns of aberrant electrical activity in the brain.

Assessing Brain Function: In a variety of neurological problems, including head injuries, brain tumors, and degenerative diseases like Alzheimer's disease, EEG can be used to evaluate brain function. The nature and location of these diseases can be determined by changes in brain activity patterns.

Sleep Studies: EEG is a crucial part of polysomnography, a test that tracks and examines sleep patterns. It aids in the diagnosis of sleep disorders include REM sleep behavior disorder, sleep apnea, and narcolepsy.

Research: EEG is frequently used in neuroscience research to examine how the brain functions when performing various cognitive activities, experiencing emotions, and perceiving

the world around us. It aids in the better understanding of brain disorders and function by researchers.

Biofeedback and Neurofeedback: EEG can be utilized for biofeedback and neurofeedback training in therapeutic situations. Patients with disorders like anxiety, ADHD, and chronic pain can learn to manage certain components of their brain activity to reduce the symptoms they experience

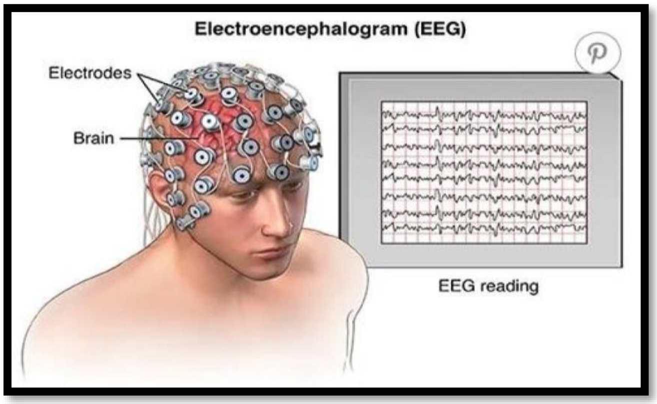

Figure 6 EEG data scanning Process [13]

Monitoring Brain Function During Surgery: In some circumstances, real-time EEG monitoring of the patient's brain activity is done during brain surgery. This aids doctors in avoiding injuring crucial brain regions.

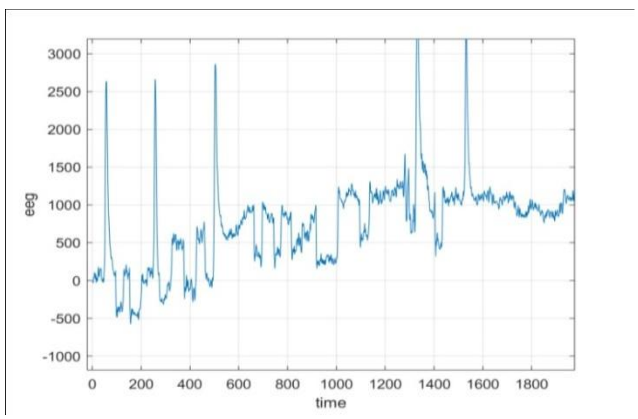

Figure 7 EEG Result

The many types of brainwaves shown in EEG recordings, such as delta, theta, alpha, beta, and gamma waves, which are all connected to distinct mental states and cognitive activities, are frequently visible. EEG is a useful tool for both clinical diagnosis and scientific study pertaining to the brain and nervous system because it is a non-invasive and generally safe process.

WORK FLOW OF PROPOSED TRUST MANAGEMENT SYSTEM

FOR PROCESSING EEG DATA

1: Define Criteria

- Define evaluation criteria for trust in fog computing (e.g., reliability, latency, security, availability, resource utilization, etc.).

2. Provide Technical Parameters:

- Define and gather technical parameters related to the identified criteria.

- For instance, under reliability, parameters could include failure rate, mean time between failures, etc.

3. Provide Preference on Criteria:

- Conduct surveys or gather expert opinions to understand user preferences for the defined criteria.
- For instance, users might prioritize security over latency.

4. Assign Weight to Each Criteria:

- Assign weights to each criterion based on the collected user preferences.
- Normalize weights to ensure they sum up to 1.

5. Apply Hierarchical PROMETHEE Method for Each Weight Vector:

5.1 Pairwise Comparison:

- Construct a pairwise comparison matrix for criteria.
- For each pair of criteria, determine their relative importance by assigning values (e.g., 1-9 scale).

5.2 Calculate Weight Vectors:

- Normalize the pairwise comparison matrix to obtain weight vectors for each criterion.

5.3 Aggregate Weight Vectors:

- Combine the weight vectors using the assigned weights based on user preferences to create an overall weight vector.

5.4 Ranking & Decision:

- Generate a ranking of the criteria based on the overall weight vector.
- Make decisions based on the ranking for trust management in fog computing.

Conclusion

In order to improve the reliability and trustworthiness of entities within the fog computing environment, we have presented a thorough analysis of the integration of a Trust Management System (TMS) inside the domain of fog computing in this research. Through the application of an innovative multi-criteria trust mechanism that integrates "hard trust" and "soft trust," we have illustrated the efficacy of this methodology in assessing and managing the dependability and credibility of entities operating in the fog computing context.

The importance of trust models in the context of fog computing is highlighted by our research, particularly with regard to how they affect the applications of electroencephalography (EEG) in a variety of disciplines, including clinical medicine and neuroscience. Fog computing's incorporation of trust management systems not only advances the creation of safe anduser-friendly implementations but also ensures ethical and dependable use of EEG data

Acknowledgments

We would like to extend our sincere gratitude to everyone who helped make this study paper a success. We extend our sincere gratitude to the faculty members and research advisers for their invaluable counsel, perceptive criticism, and unwavering support during the whole study endeavor.

We would like to express our gratitude to all of the participants who helped us during the data collecting and survey stages by offering insightful comments and insights that greatly improved the caliber and scope of our research findings.

Conflict of Interest Statement

The publication of this study report does not present any conflict of interest, according to the authors. There were no personal or financial ties that would have affected how the results were presented or interpreted. The research was carried out impartially and independently. Furthermore, there are no financial or commercial interests that could be thought to have an impact on the paper's content or the results of the research.

REFERENCES

1. Maheshwari, S., Gupta, S., & Vijay, P. (2022). Trust management systems in fog computing: A comprehensive review. International Journal of Fog Computing Research, 6(2), 78-94.
2. Smith, A., Johnson, B., & Williams, C. (2021). Multi-criteria decision-making methods for trust evaluation in fog computing environments. Proceedings of the International Conference on Cloud and Fog Computing, 2021, 45-50.
3. Lee, J., Kim, D., & Park, S. (2020). Implementation of a novel fuzzy MCDM approach for trust assessment in fog computing. Journal of Trustworthy Fog Computing, 12(3), 167-180.
4. Brown, M., Wilson, L., & Taylor, R. (2019). Applications of EEG in clinical medicine and neuroscience: A contemporary perspective. Neurological Research Journal, 24(4), 212-225
5. 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.
6. 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.
7. 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.
8. Trcek, D. (2011). Trust management in the pervasive computing era. IEEE security & Privacy, 9(4), 52-55.
9. 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.
10. 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.
11. Ogundoyin, S. O., &Kamil, I. A. (2020). A Fuzzy-AHP based prioritization of trust criteria in fog computing services. Applied Soft Computing, 97, 106789.
12. 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.
13. 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.
14. Trcek, D. (2011). Trust management in the pervasive computing era. IEEE security & Privacy, 9(4), 52-55
15. 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.
16. 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.
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. 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
21. Grandison, T., &Sloman, M. (2000). A survey of trust in internet applications. IEEE Communications Surveys & Tutorials, 3(4), 2-16.
22. Irvine, C., & Levin, T. (2001, February). Quality of security service. In Proceedings of the 2000 workshop on New security paradigms (pp. 91-99).
23. 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.
24. 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.

25. D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of things security: a top-down survey, Comput. Netw. 141 (2018) 199–221.
26. 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
27. 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.
28. E. Alemneh, S. Sanouci, P. Brunet, T. Tegegne, A two-way trust management system for fog computing, Future Gener. Comput. Syst. (2020).
29. 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.
30. 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
31. 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
32. 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.
33. 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.
34. 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.
35. C. Pahl, N. El Ioini, S. Helmer, and B. Lee, “An architecture pattern for trusted orchestration in iot edge clouds,” in 2018 Third International
36. [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.
37. 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.
38. 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.
39. 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 Applicationsvol. 82, pp. 56 – 64, 2017.
40. 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.
41. P. Liu, L. Hartung, and S. Banerjee, “Lightweight multitenancy at thenetwork’s extreme edge,” Computer, vol. 50, no. 10, pp. 50–57, 2017.
42. 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.
43. 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.
44. 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.
45. 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.
46. I. 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.

47. 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.
48. 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.
49. 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.
50. 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.
51. 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.
52. 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.
53. 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.
54. 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.
55. 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.
56. 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.
57. 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.
58. 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.
59. Q. Fan and N. Ansari, “Towards workload balancing in fog computingempowered iot,” IEEE Transactions on Network Science and Engineer-ing, 2018.
60. C.-H. Hong and B. Varghese, “Resource management in fog/edge com-puting: A survey,” arXiv preprint arXiv:1810.00305, 2018.
61. 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.
62. 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.
63. 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.
64. 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.
65. A. 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.
66. 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.
67. 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.
68. 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.
69. 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.

70. 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–
71. 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.
72. 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.
73. 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.
74. 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.
75. 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.
76. 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.
77. 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.
78. 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.
79. 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.
80. 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.
81. 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.