Journal of Management Practices, Humanities and Social Sciences

Vol 5 Issue 6 pp. 69-78

https://doi.org/10.33152/jmphss-5.6.8

ORIGINAL CONTRIBUTION

Multileveled Central Trust Management Approach using Fog Computing

Ayesha Irshad[1], Syed Zohaib Hassan [2], Ayesha Aslam[3], Kalsoom Ayaz[4], Jamaluddin Mir[5,*], Muhammad Awais Bawazir[6]

[1, 3, 4] Department of Computer Science, Abbottabad University of Science & Technology, Abbottabad, Pakistan

[2] School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China

[5] Faculty of Computer Science & Information Technology, Universiti Tun Hossein Onn Malaysia, Batu Pahat, Malaysia

[6] Department of Computer Science, Bahria University, Islamabad, Pakistan

Abstract— In the IoT environment, one of the biggest issues is the devices' anonymity and mobility, i.e., continuously joining and leaving networks. This research aims to explore certain strategies that will enable users to overcome these issues. Fog computing is reclined of central cloud services on multiple points near edge devices. Fog computing creates a decentralized computing architecture that acts as an intermediary between the cloud and the devices producing the data. This decentralized approach enables the users to locate resources in such locations that are closer to the devices. Cloud services are more effective when they are provided with low latency, storage issues are reduced, bandwidth is saved, and QoS is enhanced. Distributed fog nodes can cope with the mobility of edge nodes. Although both edge and fog computing can bring computing processes to such locations where data is created by eliminating the need for central storage, this approach gives rise to unprecedented issues that do not exist in centralized architecture like cloud computing. Anonymity can be addressed by identifying vulnerable devices and evaluating their trust level. This research work proposes a trust management scheme to develop a reliable IoT infrastructure in terms of trust. In the proposed model, trust is evaluated and managed on multiple levels to at the tain quality of services and give customers the confidence to share their confidential data online. This goal will help the users connect to the internet without losing control of their data integrity and confidentiality.

Index Terms— Cloud computing, Fog computing, trust, Trust management, Quality of service

Received: 11 August 2021; **Accepted:** 26 October 2021; **Published:** 22 December 2021

Introduction

Today, almost everybody is becoming part of a worldwide network via social media; no one wants any compromise on their privacy or data breach, which raises the question of trusting the host when giving the information to them. While on the other hand, the question of the authenticity of data being poured onto the network also comes to light. This comes with many network data nodes (Yuan & Li, 2018).

Security and trust issues, handling of non-structured data, refurbishment of IoT devices, their connectivity, compatibility, and interoperability together with intelligent analytics are a few of the hindrances in the deployment of IoTs, which should be answered or resolved

[*] Email: mirjamal70@gmail.com

to achieve the needed amelioration (Wang et al., 2013; Wang et al., 2013). Trust is crucial to making the IoT deployment process safe and secure for everyone to benefit from. To develop a safe IoT architecture, the research focuses on the trust factor of new nodes coming into the network and of the existing ones also. The proposed model is a quantitative model to algorithmize the calculation of the trust value of IoT devices. This model bases its calculations on two main parameters, availability and reliability, making it a multiple-layer evaluation technique. The proposed methodology is beneficial to tackling the problem of constant sync-ups of trust values of incoming devices with fog nodes. In addition to centralized data distribution, the benefits of Fog computing are aided by trust.

We assessed our work by comparing it with the RGR (resilient graphical routing) and the GPSR (Greedy perimeter stateless routing)

The paper is organized as segment 2 gives the basic information needed to understand the proposed knowledge, 3 is a literature review, 4 describes the proposed work, and 5 is an experimental setup. The author concludes the study in section 6.

Background

This section includes the basic knowledge required to understand the proposed model.

IOT

The Internet of Things (IoT) is a term for the growing trend of using technology to connect everyday objects and devices to the internet (Atzori et al., 2010). In this concept, our lives are changed by interrelated objects that work together to advance forward-looking ideas. Smart cities, smart transportation systems, and Smart homes are some real-world examples of these ideas already coming into existence; smart access to real-time activities is achieved by capturing physical changes in our surroundings (Yi et al., 2015). The IoT is a revolutionary new way to connect and interact with the real world. It allows entities such as machines, sensors, and actuators to be interconnected seamlessly, whether they're located in a single room or on the other side of the world (Desai et al., 2015).

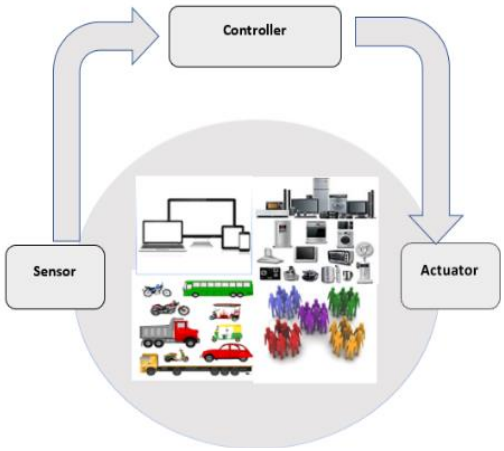

Fig. 1. IoT network

Cloud computing

It is a generic term for providing central services to customers connected to the internet and having limited hardware resources (Yoo, 2011). A cloud is a large pool of readily available, well-organized, and interoperable resources (for instance, development platform, services, and hardware). This can be achieved by dynamically reconfiguring these resources to adjust to variable loads (scale) and optimize for optimal resource use. A pay-per model is normally used to exploit these pool resources, with the guarantees offered via Infrastructure Provider through customized Service Level Agreements" (Etro, 2015).

A cloud server can provide ubiquitous and easy access and services to networked devices according to their needs. The services can be enjoyed with minimal management exposure and communication with serving authorities (Mell & Grance, 2011; Yoo, 2011). A few vital key features of cloud computing contribute a lot to fulfilling customer requirements like Resource pooling, Broad network access, On-demand self-service, Measured services, and Rapid elasticity.

Anyone can enjoy cloud computing, irrespective of their physical existence, background, or actual computing hardware. They can also use cloud-based software running over the server infrastructure (SaaS).

Fog computing

It acts as an alternative to cloud computing to provide computing processing, storage, maintenance, and control over a network of nearby IoT devices (Yi et al., 2015). It is a layer between the cloud and edge that processes data before transferring it to the cloud. Fog computing enables cloud services to be more effective by reducing latency, saving bandwidth and storage, and enhancing Quality of Service (QOS) (Tan & Koo, 2014; Varshney & Simmhan, 2017). Fog computing comprises a group of laddered nodes, and each group has specific obligations. Some nodes collect data through commands and sensor control, others are responsible for data management activities, and some are involved in computational tasks [CW17].

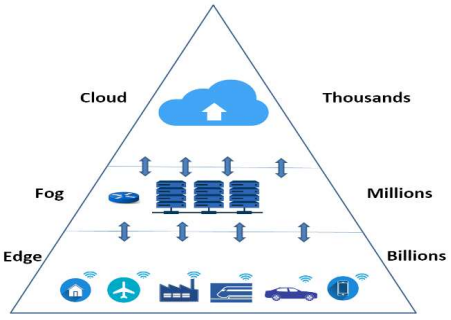

Fig. 2. Fog Computing Infrastructure (und Ort 2018-2019)

Trust

Trust" is a single word that describes the act of placing confidence in someone or something. Trust can be used in diverse contexts, so everyone defines this term differently. It's a degree of strict confidence in somebody's honesty, truthfulness, and reliability (Buttyan & Hubaux, 2007). Trust may be calculated through a multi-level inquiry of relationships in diverse contexts. However, this will result only in an increase in complexity and difficulty to measure, whereas the same increase in interaction domain can result in an increase in trust (Fulmer & Gelfand, 2012).

"Trust is a surety level that helps Trustor make logical decisions to expose its vulnerabilities to the Trustee [LS07]."

Trust management

Trust management is a service mechanism that assigns trust status to items based on the information they provide, then makes decisions based on it (Wang et al., 2013). Trust management is the construction of a framework where two devices come closer and makes a trust-based relation to interchange sensitive data with certainty. This can be done by assessing and computing the level of trust in relationships to make good decisions (Wang et al., 2013).

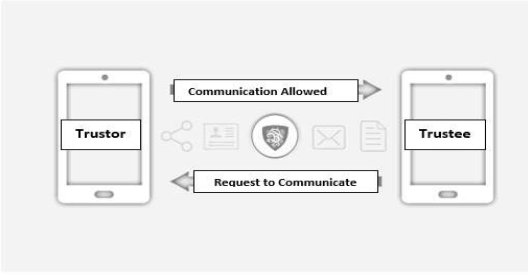

Fig. 3. Trust-based communication (Taheri, 2007)

Trust dimensions

Trust is a virtue that can never be created, only earned by showing goodness and loyalty. That can be evaluated by keenly examining the possessions of the trustee by the trustor (Cho et al., 2010; Guo et al., 2017). There are five trust dimensions:

Trust formation

One or more trust properties can be chosen in Trust formation to compute the trust composition. It can be a single trust or multi-trust.

Trust composition

Components involved in trust computation can be determined to increase the quality of services (QOS) and the excellence of relationships between networked entities (Social Trust).

Trust update

To make current trust values available to all IoT devices, there should be a mechanism to update these values for all nodes. These updates can be maintained by recording a continuous change in trust values. To achieve this, two practical approaches are purely based on energy resources.

- Time-based: Trust value gets updated after a fixed time interval.
- Event-based: Trust value gets updated on the occurrence of any event.

Trust aggregation

An amalgamation of direct and indirect trust values is called trust aggregation.

- Direct Trust: Refers to the use of personally assessed trust values.
- Indirect Trust: Refers to using the values calculated by community nodes.

There are several trust aggregation techniques that can be adopted. A few of them are weighted sum, Belief theory, Subjective logic, certain logic, Bayesian Inference, Fuzzy Logic, and Regression analysis (Jøsang et al., 2007). The trust computed by an entity itself is called direct trust, but when these values leverage other entities, it is said to be indirect trust. If direct and indirect both should be examined mutually, the weighted sum is the commonly used technique (Guo et al., 2017).

Trust propagation

Trust computed by a trustor should be disseminated to all other nodes for the smooth execution of network activities. There are two ways through which trust values propagate/disseminate.

- Centralized: Refers to the trust propagation through a single serving entity. Which can be a Cloud server (Nitti et al., 2013).
- Distributed: Trust is propagated through autonomous entities instead of a central server (Wang et al., 2019).

Literature Survey

The basic purpose of networking is sharing resources, which may lead to the exposure of resources for vulnerabilities or theft. Many access control methods are in use for a long time to avoid this unwanted situation. It is high time to study the part temporal dynamics play in trust, and a very intriguing guide on this has been presented by Perera et al. (2013). Realizing the temporal dynamics is very important as exchanged relationships can be changed, affecting trust. Contextual is given peer importance, and they have recommended the researchers specify context so the relationship between these trusts can be learned. Finally, fluidity between environment and persons has been called upon to be investigated (T. Wang et al., 2019) brings up with an idea that the relationship between place and persons is elastic and could be worked upon after, According to Ali et al. (2021), integration, execution, planning, and commitment are the important steps to be taken before multi-level trust is developed through leaders to the administration.

The relationship between trust and control is discussed by (Roman et al., 2018), who concluded these dependencies over institutions and situations. The job of aggregate trust is subsequently inspected, and people's response to changes is set the standard. People's illustrative and theoretical influence in forming their organizations has been studied. Shi et al. (2016) recommended the requirement for separation between trust as well as distrust.

According to Jøsang et al., (2007), IC3 identified a 22.3 % increase in online fraud, which is an ample reason to distrust online services. Running an online business demands various requirements for the consumers and the vendors according to their roles. Trust is the fundamental need of each business, whether it runs in a traditional way or online (M. Ali et al., 2021).

The collection of feedback is used to measure reputation-based trust. Similarly, Xiang and Liu (Yuan & Li, 2018) used the weighted sum of five peers' feedback to evaluate the trust.

Proposed Work

The proposed model is a centralized approach to achieving a trustworthy interaction among two communicating nodes. The node that permits the others to communicate is named a trustor, whereas the other communicating member is a trustee (Atzori et al., 2010). Once a new trustee joins a network, the node's behavior is unpredictable as there is no historical trust value that could specify negative or positive interactions. Therefore, for a trustee to initiate a new communication within the network, fog allows it conditionally to partake in the network for a specific period in controlled access. After completion of the first communication session, the trustee's performance provides a reason based on which the trustor can evaluate its trustworthiness through personal experience.

This approach supports direct observations only because, in indirect observations, the biasedness of a single entity may lead to computing wrong trust values. Trust values are labeled to the trustee when that trustee becomes an old participant within the network and has a trust-level history.

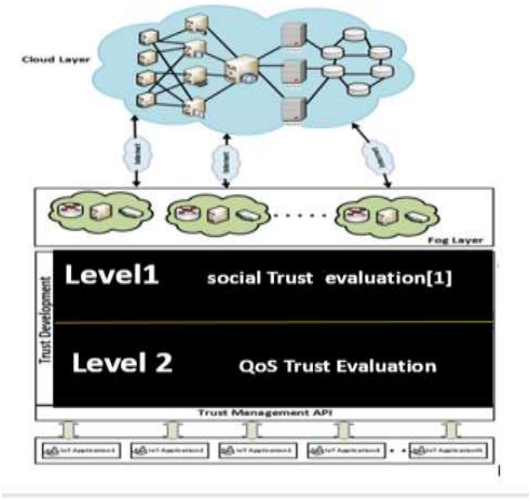

Fig. 4. Multi-level central trust management approach

Those labels are a token for a trustee to communicate over the network. To access the network, value ranges 0 to 100 is set as a scale for the trustee nodes.

- If the label on any trustee is less than 50, it can only access information (acts as a dumb terminal).
- If the trust value exceeds 50, it can exchange data in the network.
- If the trust value exceeds 90, the trustee can be selected as a service provider.

In circumstances where a trustee is to be taken as a service provider through any node, it must be a trustful entity. To find that out, the label is matched with centrally broadcasted trust value to avoid each tricky situation. If the node's trust value accomplishes the threshold requirement, then communication is started, or access is denied.

Trustor computes the trust values of the trustee computed based on experience after the first completion of the successful communication session among the trustee and trustor. Two distinct features of the trustee are considered to inspect the trustworthiness of that particular node on two distinct levels. At level one, termed social trust, Liu's strategy is utilized to decide if the node is honest or dishonest. If the device is predicted as honest in level one, it is derived to level two (QoS trust) for additional evaluation. At this level, evaluation is done utilizing considering the reliability and the availability as the two standard trust properties. They are checked comprehensively on this level. These two key factors are used;

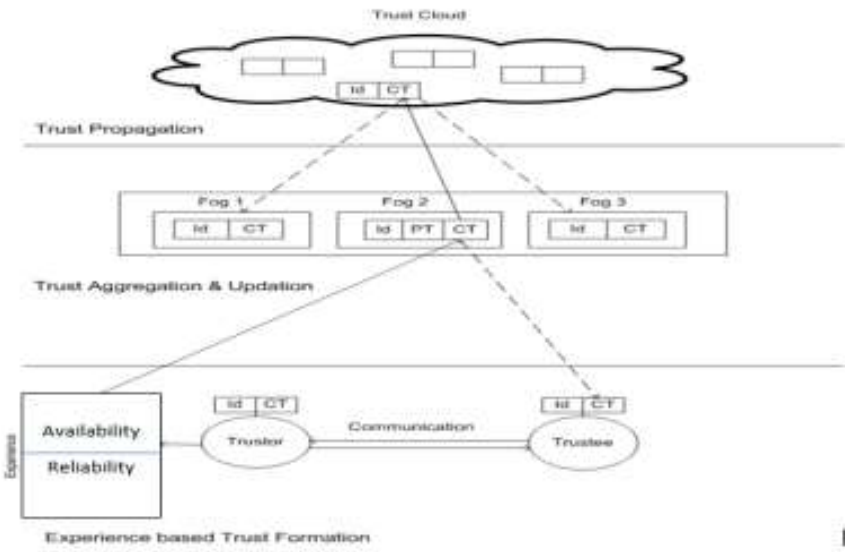

Fig. 5. Trust computing mechanism

Now Avionics assesses the risk of the failure and then decides on it. Choosing these factors shows their significance, where any incorrect selection has an immense real-life significance in the form of human lives. In this way, we selected these features as criteria for computing trust value to cope with susceptibilities that can be the reason for network failures. Our proposed approach has the prospective to develop a fear among users of being punished in real-time via technically controlling their network access based on their behaviors. This will force them to behave positively well along, if not the first time. • Reliability is the ability to show a satisfactory performance or a possibility of the failure of the system (Yuan & Li, 2018). It could be measured through the factors that reinforce the system's validity. We considered the response time to a request, the rate of energy consumed, and the packet delivery ratio as an evaluation matrix. • Availability is measured as the unpreparedness of the trustee in the network communication (Sakthivel & Vidhya, 2021). The availability can be estimated via estimating the possibility of downtimes in the life cycle.

The two properties are thought about separately to give readings in numeric quantities, which are utilized to create a healthy worth by playing out a few factual tasks. The resultant worth is considered the current trust worth of the trustee.

After calculating these trust values, the trustor sends this data to the Fog node to update the existing trust values. The fog node inspects if the node has any previous trust values. If so, trust calculation is done by taking the mean of the recent and the previous trust value. Otherwise, the trustor's direct observation is considered a trust value (this simply occurs once the new node is added to the network). The trust value is shared with the cloud server, which is then broadcasted to all the fog nodes to label it with the device. Devices profiles information is added up with this label to be available for the next time it confronts other nodes in the network. Thus, the trustee's influence on the previous behavior in the form of the trust value is visible; furthermore, its reputation proceeds it. Mobility issues of IoT nodes/ devices could be overcome by using this technique.

Experimental Setup

Proposed model algorithm is assessed by implementation in MATLAB. The model is designed to accomplish efficient and reliable behavior of the IoT nodes. For a node to be a trustee, we utilize two parameters, the first is 'availability' and the second is 'reliability.' Which is previously debated in the section of the proposed work. We assessed our work by relating it to GPSR (Greedy perimeter stateless routing)(Narayan et al., 2020). We build an IoT environment with 10 fog nodes (Fn), a cloud server (Cs), and 100 edge nodes (Te and Tr). The assessment metrics used to measure the trustworthiness of the nodes are:

Time

Proper time management helps us to accomplish a maximum job in minimum time. Our model performs multiple computational and Communicational tasks significantly quicker than GPRS. Ttot is the total time consumed by our model. T is the time taken by trustee (Te), trustor (Tr), fog node (FN), and cloud server (Cs).

$$T_{tot} = \sum_{req}^{comp} T(T_e, T_r, F_N C_s)$$

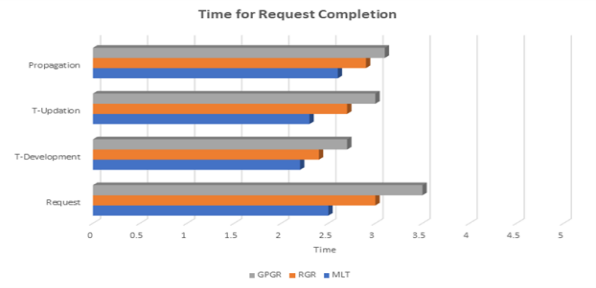

Fig. 6. Time for request completion

Packet delivery ratio

Measurement of the data dropped or concealed by the trustee can be used to predict the trustee's intentions. When a device shows a negative intention, it can never be considered reliable. Previously all the work packet delivery is measured in a specific period. However, we measured it differently.

Trust ∝ 1/ (Hidden-Data)

We tested our technique by deploying 100 nodes. The fog nodes (FN) are 10 and a central server (CS). We sent 60 packets of data in different intervals and predicted the data loss's trust rate (0 percent to 100 percent).

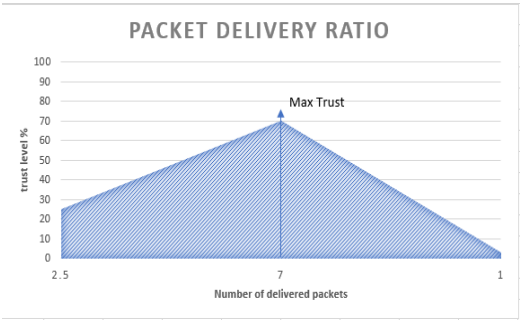

Fig. 7. Packet delivery ratio

Energy consumption

Energy consumption is assumed to be a significant part of the model's success or failure. It must be estimated cautiously. Econ is the total energy consumed by the model. E is a metric for the energy utilized/ consumed by the request submission (rq), trust update (tu), trust propagation (tp), and trust development (td). Again, we compared our results with RGR and GPSR (Tan and Koo 2014).

$$E_{con} = \sum_{req}^{comp} E(r_q, t_d, tup, t_p)$$

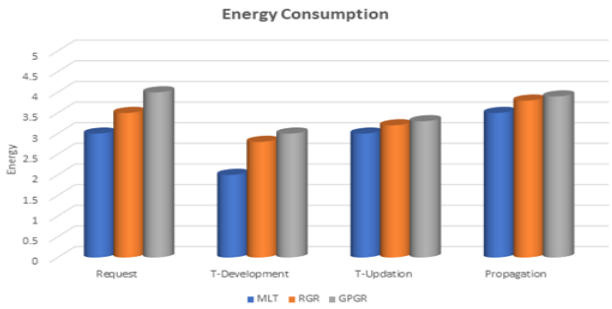

Fig. 8. Energy consumed

Conclusion

We introduced a model for centralized multilayered trust management aimed at fog computation. We also prove with the help of simulations that the model is named a two-layer trust evaluation model. The simulation results of our model showed improved results than that of RGR and GPSR (already accepted methods), showing our selection of "Availability" and "Reliability" as the right standard for the trust evaluation of a trustee. Our chosen parameters, together with our model of centrally synchronized fog nodes, come out to be the best option when it can accomplish low latency from a fog computation by synchronizing all the fog nodes by the trust values of a trustee, activated at an event of the interactions of the trustee within the network.

Limitations and Future Work

The current research is based on the assumption that fog computing architecture nodes are stationary. In the real world, most scenarios involve constant movement nodes. This assumption is one of the major limitations of the current work. For future work, researchers can focus on movable nodes, which might give rise to new issues that must be addressed. Also, for future work, researchers can consider several social and qualitative parameters for calculating trust.

REFERENCES

Ali, A., Iqbal, M. M., Jamil, H., Akbar, H., Muthanna, A., Ammi, M., & Althobaiti, M. M. (2021). Multilevel central trust management approach for task scheduling on IoT-based mobile cloud computing. *Sensors, 22*(1), 1-22. https://doi.org/10.3390/s22010108

Ali, M., Raza, S. A., Khamis, B., Puah, C. H., & Amin, H. (2021). How perceived risk, benefit and trust determine user Fintech adoption: A new dimension for Islamic finance. Foresight, 23(4), 403-420. https://doi.org/10.1108/FS-09-2020-0095

Arvind Narayan, S., Rajashekar Reddy, R., & Femilda Josephin, J. S. (2020). Secured congestion control in VANET using greedy perimeter stateless routing (GPSR). In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*. Berlin, Germany: Springer. https://doi.org/10.1007/978-981-15-0199-9_59

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

Buttyan, L., & Hubaux, J. P. (2007). *Security and cooperation in wireless networks: Thwarting malicious and selfish behavior in the age of ubiquitous computing*. Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/CBO9780511815102

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. https://doi.org/10.1109/SURV.2011.092110.00088

Desai, P., Sheth, A., & Anantharam, P. (2015). Semantic gateway as a service architecture for iot interoperability. *IEEE International Conference on Mobile Services*, New York, NY. https://doi.org/10.1109/MobServ.2015.51

Etro, F. (2015). The economics of cloud computing. *Cloud Technology: Concepts, Methodologies, Tools, and Applications*. Hershey, Pennsylvania: IGI global.https://doi.org/10.4018/978-1-4666-6539-2.ch101

Fulmer, C. A., & Gelfand, M. J. (2012). At what level (and in whom) we trust: Trust across multiple organizational levels. *Journal of Management, 38*(4), 1167-1230. https://doi.org/10.1177/0149206312439327

Guo, J., Chen, R., & Tsai, J. J. P. (2017). A survey of trust computation models for service management in internet of things systems. *Computer Communications, 97*, 1-14. https://doi.org/10.1016/j.comcom.2016.10.012

Horzela.(2019). Elements of Social Responsibility in Clusters. *Journal of Management Practices, Humanities and Social Sciences, 3*(2), 65-72.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems, 43*(2), 618-644. https://doi.org/10.1016/j.dss.2005.05.019

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (Tech. Report). Gaithersburg, MD: National Institute of Standards and Technology Special. https://doi.org/10.6028/NIST.SP.800-145

Nitti, M., Girau, R., & Atzori, L. (2013). Trustworthiness management in the social internet of things. *IEEE Transactions on Knowledge and Data Engineering, 26*(5), 1253-1266. https://doi.org/10.1109/TKDE.2013.105

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials, 16*(1), 414-454. https://doi.org/10.1109/SURV.2013.042313.00197

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78*, 680-698. https://doi.org/10.1016/j.future.2016.11.009

Sakthivel, S., & Vidhya, G. (2021). A trust-based access control mechanism for intra-sensor network communication in Internet of things. *Arabian Journal for Science and Engineering, 46*(4), 3147-3153. https://doi.org/10.1007/s13369-020-05102-4

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637-646. https://doi.org/10.1109/JIOT.2016.2579198

Tan, J., & Koo, S. G. (2014, May). A survey of technologies in internet of things. In *IEEE International Conference on Distributed Computing in Sensor Systems*, Marina Del Rey, CA. https://doi.org/10.1109/DCOSS.2014.45

Varshney, P., & Simmhan, Y. (2017). Demystifying fog computing: Characterizing architectures, applications and abstractions. *IEEE 1st International Conference on Fog and Edge Computing (ICFEC)*, Madrid, Spain. https://doi.org/10.1109/ICFEC.2017.20

Wang, C., Daneshmand, M., Dohler, M., Mao, X., Hu, R. Q., & Wang, H. (2013). Guest Editorial-Special issue on internet of things (IoT): Architecture, protocols and services. *IEEE Sensors Journal, 13*(10), 3505-3510. https://doi.org/10.1109/JSEN.2013.2274906

Wang, J. P., Bin, S., Yu, Y., & Niu, X. X. (2013). Distributed trust management mechanism for the internet of things. *Applied Mechanics and Materials, 347*, 2463-2467. https://doi.org/10.4028/www.scientific.net/AMM.347-350.2463

Wang, T., Luo, H., Zheng, X., & Xie, M. (2019). Crowd sourcing mechanism for trust evaluation in CPCS based on intelligent mobile edge computing. *ACM Transactions on Intelligent Systems and Technology (TIST), 10*(6), 1-19. https://doi.org/10.1145/3293317

Yi, S., Qin, Z., & Li, Q. (2015). Security and privacy issues of fog computing: A survey. *International Conference on Wireless Algorithms, Systems, and Applications*, Qufu, China. https://doi.org/10.1007/978-3-319-21837-3_67

Yoo, C. S. (2011). Cloud computing: Architectural and policy implications. *Review of Industrial Organization, 38*(4), 405-421. https://doi.org/10.1007/s11151-011-9295-7

Yuan, J., & Li, X. (2018). A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion. *IEEE Access, 6*, 23626-23638. https://doi.org/10.1109/ACCESS.2018.2831898