Access Control Method Based on a Mutual Trust Mechanism in the Edge Computing Environment

Weijin Jiang and Sijian Lv(✉)

College of Computer and Information Engineering,
Hunan University of Technology and Business, Changsha 410205, China
lvsijian8@qq.com

Abstract. The problem of mutual trust between users and edge nodes in an edge computing environment is a sufficient guarantee for the double security of edge computing service users and service providers. How to achieve the user's security and credibility and ensure the trust of the edge service nodes is a serious challenge facing the security of edge computing. In this paper, based on the user behavior trust model and the edge service node trust evaluation model, the concept of mutual trust in edge computing is defined, the mutual trust mechanism and the mutual trust model are designed, and on this basis, the access control model EUSMTM based on mutual trust is proposed. (Edge Users and Edge Servers Mutual Trust Model), the EUSMTM is described in detail in terms of model definition, framework structure, algorithm flow and authorization decision mechanism. The EUSMTM model closely integrates trust management with the RBAC (Role-Based Access Control) model. Aiming at the multi-domain characteristics of the edge computing environment, The EUSMTM model implements intra-domain access control and cross-domain access control strategies based on mutual trust, and it implements the improvement and expansion of the RBAC model in the edge computing environment. By comparing and analyzing the performance of EUSMTM through a simulated environment, the validity of the trust model between the user and the edge server is verified; Through the comparative experiment of two-way trust and one-way trust between the edge user and the edge server, the relative advantages of access control based on two-way trust in the EUSMTM model are analyzed.

Keywords: Edge user · Edge service node · Mutual trust mechanism · Access control · Edge computing

1 Introduction

The dynamic and distributed characteristics of the edge computing environment [1] cause users to face a series of security issues in the process of using the edge computing services and edge platforms [2] in providing services [3], The key to solving these security issues lies in ensuring the security and credibility of the edge computing environment and its users. The security credibility of the edge computing environment is proposed [4], which strengthens the dynamic processing of the edge computing

G. Wang et al. (Eds.): SpaCCS 2020, LNCS 12383, pp. 334–344, 2021.
https://doi.org/10.1007/978-3-030-68884-4_28

network status. It provides a strong policy guarantee for the implementation of more flexible and adaptive edge computing network security and edge service quality [5].

In the edge computing environment, on the one hand, users directly use the software, systems, information resources, programming environment, network infrastructure and other software and hardware devices provided by the edge server [6], which has resulted in the user's impact and destruction on edge computing resources being much more serious than the threat posed by users' use of the Internet, especially the active attacks and sabotage activities initiated by users under cover of their legal identities, which pose a serious threat to the edge computing platform. Therefore, whether the behavior of the edge user is credible and how to predict and evaluate the behavior trust of the edge user is one of the important contents of the edge computing security research. On the other hand, due to the lack of controllability of edge computing resources, devices, and systems, users will psychologically distrust the edge server, including the leakage of user's private information, the security risks of information storage location, data loss, service interruption, and the closure of edge computing operators [7] and other risks. The user's trust in the edge server is the premise to decide whether the user accepts the services provided by edge computing and is willing to store the information in the cloud [8]. Therefore, the user's trust in the edge server is very important. Establishing an effective mutual trust model between the edge server and user behavior is the key to ensuring the security of the edge computing environment. The importance of establishing mutual trust between the user and the edge server is mainly reflected in the following three aspects [9, 10].

(1) Through the problem abstraction to accurately describe the credibility requirements of the edge computing system, it is convenient to achieve a comprehensive understanding of the edge computing security requirements. And through the mathematical method to analyze the loopholes in the credibility of the system and establish a trust model.

(2) The formal description, verification and application of the trust model can improve the credibility of the edge computing system and help the two-way trust choice between users and edge servers.

(3) Establishing a trust assessment theory that includes the risk assessment of the edge computing environment and the description of user's attack behavior is the prerequisite and foundation for the realization of trust monitoring, prediction and assessment of a comprehensive edge computing system.

2 Related Work

Edge computing uses many edge devices to provide users with near-earth real-time computing and storage functions It migrates some or all of the computing tasks in the cloud to edge devices, which can meet the needs of users for low latency and fast response. It has good application effects in scenarios such as smart car networking, virtual reality, medical care, smart home, and smart city [11]. Edge devices take care of consumers and producers of data, and most of the user's privacy information is stored at the edge layer. However, edge computing lacks the same stable infrastructure protection facilities as cloud computing, coupled with the open features of edge computing such as content perception, real-time computing, and parallel processing, resulting in a lack of necessary trust between devices that brings challenges to the security of edge devices.

The trust mechanism can effectively resist internal attacks on the network and is currently one of the key technologies to ensure that the device provides reliable services [12], It is widely used in computing modes such as cloud computing, P2P, and wireless sensor networks [13]. There are many existing trust model research results. In addition to evaluation models based on subjective logic, DS evidence theory, fuzzy evidence theory, Bayesian networks, and neural networks, there are also evaluation models based on other methods such as recommended node similarity, scoring deviation, and reward and punishment measures. However, in the face of a complex and changeable edge computing environment, the old trust model will have certain limitations. Firstly, the edge layer contains a large number of high-frequency interactive devices that form a complex and huge trust network. Storing and querying this trust information will consume a lot of time and space; Secondly, most edge devices are resource-constrained devices, which are difficult to undertake complex storage and query tasks. Therefore, building a lightweight trust evaluation model suitable for edge computing environments has important practical significance.

3 Access Control Method Based on Mutual Trust

3.1 Mutual Trust Model Between the User and Edge Server

Overview of Mutual Trust Mechanism

The mutual trust mechanism between the user and the edge server is divided into two layers: one layer is the trust prediction of the edge server to the user's behavior, and the other layer is the user's trust evaluation of the edge service node [14]. Whether it is the user's trust screening of edge service nodes or the judgment of the edge server's trust in user behavior, the basic trust mechanism follows the general construction process of the trust model.

In the edge computing environment, users interact with edge service nodes to obtain edge computing resources or services. In the interaction process, the user and the edge server are equal, that is, trust is mutual [15]. In order to achieve trusted interaction in the edge computing environment, the edge server must prevent malicious user behavior from damaging the cloud environment. Therefore, the behavior information of the edge user, whether it is the user's legal or malicious behavior, will affect the edge server's judgment on the credibility of the edge user, and then screens users for trust; At the same time, when the edge service node provides resources or services to users, factors such as the timeliness of response, the availability of resources and the effectiveness of the service will affect the user's judgment on the trustworthiness of the edge service node, that is, The trust relationship between the user and the edge service node must include two two-way trust selection processes [16, 17]. As shown in Fig. 1.

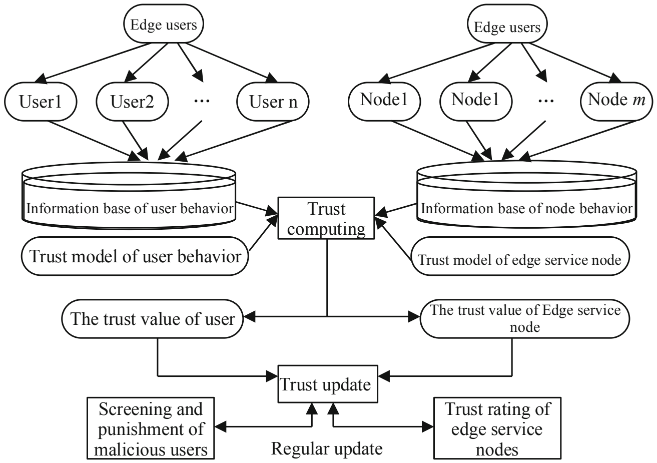
Edge users
User1
User2
···
User n
Edge users
Node1
Node1
···
Node *m*
Information base of user behavior
Trust computing
Information base of node behavior
Trust model of user behavior
Trust model of edge service node
The trust value of user
The trust value of Edge service node
Trust update
Screening and punishment of malicious users
Regular update
Trust rating of edge service nodes

Fig. 1. The process of the trust relationship between edge users and edge service nodes

Through the research of related trust models in distributed systems, grid computing, P2P systems, cloud computing, and edge computing systems, the behavioral trust model between edge users and edge servers in this paper is based on the following basic ideas.

(1) The two-way trust structure of the trust model. During the interaction between users and edge servers, the trust relationship is two-way and equal to each other. Users will screen the trust of each node in the edge server according to the level of trust. At the same time, in order to prevent malicious users from attacking the edge server, the edge server will also screen the user trust and provide selectively users with edge services or resources.

(2) Collection and processing of behavioral trust information. Behavior trust information is divided into two categories, user behavior information and node behavior information, which are stored in the user behavior information database and the node behavior information database respectively.

(3) Calculation and update of trust value. User behavior trust value is obtained through trust evidence and trust attribute matrix, and the update process shows a certain degree of reward and punishment; The calculation of the trust value of the edge server is combined with the ant colony algorithm to introduce trust pheromone, and the trust pheromone is used to determine the degree of user trust in the edge service node. In the process of updating the trust value, the influence of time must be fully considered.

Mutual Trust Model Design

In the edge computing environment, users send resource or service access requests to the edge server according to their needs [18]. In the process of cloud interaction, the user and the edge server are equal, so the trust between the two is mutual [19]. Due to the existence of uncertainty in the edge computing environment, the greater the uncertainty of cloud interaction, the more necessary mutual trust. In addition, due to the vulnerability of edge computing, its potential risks are very large, which also requires mutual trust.

Definition 1. Mutual trust. Due to the different focus, the definition of mutual trust varies. Mutual trust in edge computing is defined as the mutual trust between users and edge servers in uncertain future interaction behavior. At time t, the mutual trust between user u and edge service node c can be formally expressed as MT, $MT = <T_u, T_c(t)>$.

Definition 2. Mutual trust threshold. The mutual trust threshold MTT consists of a two-tuple, $MTT = <TT_{user}, TT_{cloud}>$, that is, the user trust threshold TT_{user}, and the edge server threshold TT_{cloud}, TT_{user} determines whether the edge user is trustworthy. The edge computing environment decides whether to allow the edge service nodes in it to accept and accept user access requests: TT_{cloud} determines whether the edge service node is qualified to provide services to users.

By defining the mutual trust threshold MTT, users with a trust level of less than TT_{user} will not be able to obtain edge computing resources and services, and edge service nodes with a trust level of less than TT_{cloud} will not be able to provide users with cloud resources and services.。

Definition 3 Trust decision. Trust decision is represented by the symbol Td,$Td \in \{0, 1\}$. The trust decision-making process is represented by Eq. (7–1).

$$Td = \{ \begin{matrix} 1, (T_{\text{user}} \geq TT_{\text{user}}) \cap (T_c(t) \geq TT_{\text{cloud}}) \\ 0, other \end{matrix} \tag{1}$$

If Td = 1, the mutual trust relationship between the user and the edge service node is established, and the edge computing platform allows the two to interact; If Td = 0, cloud interaction between the two is not allowed.

4 Simulation Experiment and Performance Analysis

In order to gain a deeper understanding of the mutual trust relationship between the user and the edge server, and analyze the impact of various factors on the mutual trust in the edge computing environment, including the relationship between user behavior trust and edge service node trust, behavior and time, we designed two Group simulation experiment. The first group is the simulation experiment of the trust model between the user and the edge server. Through this group of experiments, on the one hand, the influence of the entity's behavior information and time factors on the degree of trust is studied; on the other hand, the effectiveness of the proposed trust model between users and edge servers in this article is verified by comparison with other trust models. The second group is the EUSMTM model simulation experiment analysis. Through this group of comparative experiments, it is found that trust-based access control is more dynamic than the RBAC model and other untrusted access control systems. Besides, a comparative analysis of cloud interaction success rates based on mutual trust access control and one-way trust access control highlights the superiority of the EUSMTM model proposed in this paper.

4.1 Edge Server Dynamic Trust Evaluation Method

Edge Server Trust Relationship

There are multiple edge service nodes in the edge computing environment to provide users with resources or services, and the network environment and scale of edge computing have been in a dynamic state of change. The interaction and trust relationship between users and edge service nodes are intricate. The historical interaction behavior and time influencing factors, we give the following definition of their trust level.

Definition 4. Direct Trust. Direct trust is the degree of trust established by the user and the edge server through direct interaction experience. The direct trust of the user to the edge server is related to the interaction events and time factors between the two. The more interactions, the higher direct trust of the entity, indicated by the symbol *Dt,* for two entities that have never interacted, the value of *Dt* is usually set to zero. At time *t*, the direct trust of user *u* in edge service node *c* is expressed as $Dt_c(t)$.

Definition 5. Trust Pheromone. Trust pheromone is the basic knowledge of the user's direct trust degree of the edge service node behavior. This word is marked as *Tp*. At time *t*, the trust pheromone of the user *u* to the edge service node *c* can be expressed as $Tp_c(t)$. At the initial moment, $Tp_c(0) = C$ (*C* is a constant). If the initial trust level is zero, then the trust pheromone must also be zero, $Dt_c(t) = 0 \Rightarrow Tp_c(0) = 0$.

Definition 6. Heuristic Pheromone. Cognitive pheromone is the user's cognitive information about the edge service node, that is, the user's perception of the Euler distance from the node. This word is marked as *Hp*. At time *t,* the cognitive pheromone of the user *u* to the edge service node *c* can be expressed as $Tp_c(t)$. Cognitive pheromone can be calculated by the following formula:

$$Hp_c(t) = \frac{1}{d_{u,c}} \tag{2}$$

The trust pheromone and cognitive trust element given in Definition 5 and Definition 6 together constitute the direct trust relationship of the user to the entity. In the ACO algorithm, the transfer probability of an ant is used to represent the ant's choice of different paths. In the edge computing environment, the important basis for the user to select an entity that provides resources/services is the entity's direct trust. Therefore, at time *t*, the direct trust user *u* in edge service node *C* can be formalized as:

$$Dt_c(t) = \frac{Tp_c(t)^a Hp_c^{\beta}}{\sum\limits_{i \in E} Tp_i(t)^a Hp_i^{\beta}} \tag{3}$$

Among them, *a* is the weight of the trust pheromone between *u* and *c*, which is the weight of the cognitive trust element (the initial value is given according to the actual situation), *E* represents the set of entities that can be selected by the user *u*, *E* = {1, 2, …, *m*}.

4.2 Model Experiment and Performance Analysis of Mutual Trust Between the User and Edge Server

This section verifies the effect of the proposed user and edge server trust evaluation model on the interaction success rate through simulation experiments and verifies the rationality and effectiveness of the improved ant colony optimization algorithm applied in edge server trust management.

Simulation Experiment Environment and Parameter Setting
Hadoop is open-source software that can realize large-scale distributed computing, and is widely used in the field of edge computing. Therefore, the experiment in this paper runs on the MapReduce platform in Hadoop. In order to verify the effectiveness of the mutual trust model between the user and the edge server, and to obtain the relationship of mutual trust with entity behavior and time, the following experimental network environment and entity interaction behavior scenarios were set up with the goal of being close to real random and complex networks.

Experiment 1 is to verify that the amount of data that needs to be processed in the experiments on the influence of entity behavior and time factors on mutual trust is not large, so only a small number of nodes are simulated in this experiment. Experiment 2 is to verify the effectiveness of the trust evaluation algorithm between users and edge servers and requires high network complexity and dynamics. Therefore, a network environment composed of 100–700 nodes is simulated in the laboratory to compare users and the success rate of the interaction between the edge server trust evaluation model and the Apriori model and the ability to resist attacks. The user and edge server trust evaluation model are proposed under the co-inspiration of the analytic hierarchy process AHP and the ant colony optimization algorithm ACO.

In addition, the setting of parameters in the ant colony algorithm has a great influence on the performance of the algorithm. According to the experiment, the best parameter setting of the ant colony model is selected, namely $\alpha = 1$, $\beta = 5$, $\rho = 0.5$.

Experimental Results and Performance Analysis
Experiment 1. The performance comparison between EUSMTM model and APRIORI model.

The APRIORI model is a network trust management model that uses the Apriori algorithm to extract the behavior patterns adopted by users during their network interactions in the literature [20], and uses the naive Bayes classifier for the final decision of the probability of user trust. It can be seen from Fig. 2 that in the initial stage, the interaction success rate of the APRIORI model is lower than that of EUSMTM. The reason is that in the edge computing environment, the number of nodes and the number of users in the network is in a dynamic process, although APRIORI is in The interaction success rate in the static network can reach over 96%, but the interaction success rate in the dynamic network is relatively lower than the EUSMTM model. As the number of interactions increases, both the EUSMTM model and the APRIORI model can continuously learn to select nodes with higher trust to interact with each other through the ant colony algorithm, so as to increase the success rate of their interactions. Malicious implementation problems will inevitably occur in the general trust model. The APRIORI model does not consider malicious recommendation entities, while the EUSMTM model fully considers the trust of intermediate entities and selects entities with relatively high trust as the recommendation entity to reduce the number of attacks.

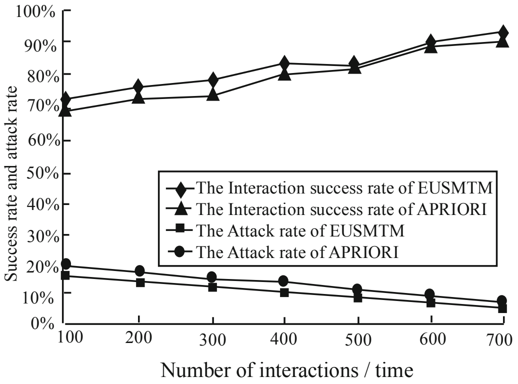

Fig. 2. Performance comparison between EUSMTM model and APRIORI

4.3 EUSMTM Model Simulation Experiment and Performance Analysis

In order to verify the feasibility and effectiveness of the access control model (EUSMTM) based on mutual trust between users and edge servers proposed in this paper, the simulation experiment of EUSMTM algorithm is carried out through the Hadoop edge computing application platform built on the server in the laboratory. Finally, the performance of the algorithm is analyzed and compared according to the experimental results. The experimental evaluation standard adopts Rate of Successful Transaction, which is the ratio of the number of successful interactions between users and edge services to the total number of interactions.

Trust-Based Access Control and Untrusted Access Control Model

Experiment 2. Comparison of trust-based access control and role-based access control.

This experiment compares the trust-based access control model proposed in this paper with the RBAC model. The user entity sends a resource access request to the trust-based access control system and the RBAC system at the same time, and the two systems authorize and access resources according to their respective access control rules. Over time, the number of accessible resources of the user in the two systems is changing. The data obtained from the experiment is shown in Fig. 3. It can be seen that in the RBAC system, the number of resources accessible by the user entity is constant, while in the trust-based access control system, the number of accessible resources of the user entity changes with the change of the trust value, which is sufficient to prove that the model is fine-grained.

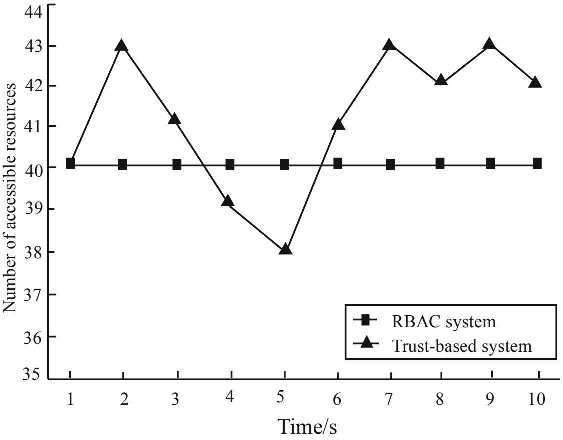

Fig. 3. Number of accessible resources in different access control systems

Experiment 3. Comparison of trust-based access control algorithms with traditional access control methods.

The trust-based evaluation algorithm in this article is compared with other computing methods, the edge service success rate under the edge computing environment is introduced, and the advantages and disadvantages of the two methods are compared. The edge service success rate is defined as the ratio of the number of successful services to the total number of services. It can be seen from Fig. 4 that the success rate of edge computing services based on traditional access control methods shows a decreasing trend over time, while the trust-based evaluation method proposed in this article has a higher success rate and dynamic changes. The accessible resources of trusted entities always have a higher success rate of edge services.

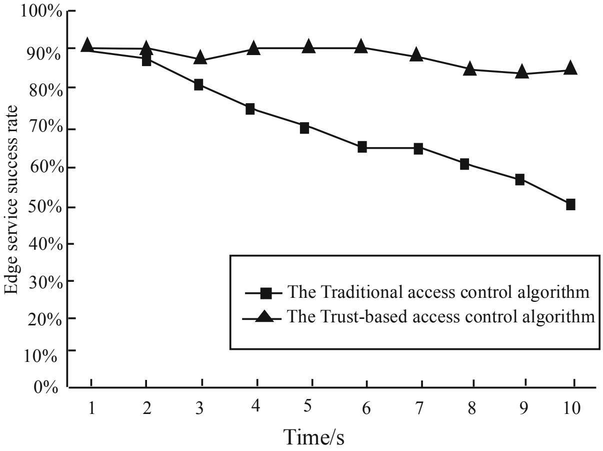

Fig. 4. Comparison of edge service success rate

5 Conclusion

Studying the mutual trust between users and edge servers in the edge computing environment is an effective guarantee for the dual security of edge computing service users and service providers. How to not only achieve user security and credibility but also ensure the trust and reliability of edge service nodes is also a severe challenge facing edge computing security. Based on the user behavior trust model and the edge server trust evaluation model, this paper defines the concept of mutual trust in edge computing designs the mutual trust mechanism and mutual trust model. And on this basis, a mutual trust-based access control model EUSMTM is proposed, and EUSMTM is defined and introduced in detail in terms of model definition, framework structure, algorithm flow and authorization decision mechanism. The EUSMTM model closely combines trust management with the RBAC model, implements intra-domain access control and cross-domain access control strategies based on mutual trust, and realizes the improvement and expansion of the RBAC model in the edge computing environment in view of the multi-domain characteristics of the edge computing environment. The EUSMTM model closely integrates trust management with the RBAC (Role-Based Access Control) model. Aiming at the multi-domain characteristics of the edge computing environment, The EUSMTM model implements intra-domain access control and cross-domain access control strategies based on mutual trust, and it implements the improvement and expansion of the RBAC model in the edge computing environment. By comparing and analyzing the performance of EUSMTM through a simulated environment, the validity of the trust model between the user and the edge server is verified; Through the comparative experiment of two-way trust and one-way trust between the edge user and the edge server, the relative advantages of access control based on two-way trust in the EUSMTM model are analyzed.

Acknowledgments. This work was supported by the National Natural Science Foundation of China (61772196; 61472136), and the Hunan Provincial Focus Natural Science Fund (2020JJ4249), and the Key Social Science Fund of Hunan Provincial (2016ZDB006), and the Key Project of Hunan Provincial Social Science Achievement Review Committee (XSP 19ZD1005), and the Hunan Province Academic Degree and Graduate Education Reform Research Project (2020JGYB234), and the Hunan University of Technology and Business Degree and Graduate Education Teaching Reform Project (YJG2019YB13), and the Hunan University of Technology and Business Teaching Reform Project (School Teaching Word [2020] No. 15).

References

1. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: vision and challenges. IEEE Internet Things J. **3**(5), 637–646 (2016)
2. Satyanarayanan, M.: The emergence of edge computing. Computer **50**(1), 30–39 (2017)
3. Mäkitalo, N., Ometov, A., Kannisto, J., Andreev, S., Koucheryavy, Y., Mikkonen, T.: Safe, secure executions at the network edge: coordinating cloud, edge, and fog computing. IEEE Softw. **35**(1), 30–37 (2017)

4. Roman, R., Lopez, J., Mambo, M.: Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future Gener. Comput. Syst. **78**, 680–698 (2018).
5. Wang, T., Zhang, G., Liu, A., Bhuiyan, M.Z.A., Jin, Q.: A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing. IEEE Internet Things J. **6**(3), 4831–4843 (2018)
6. Garcia Lopez, P., et al.: Edge-centric computing: vision and challenges. In: ACM, New York (2015)
7. Alrowaily, M., Lu, Z.: Secure edge computing in IoT systems: review and case studies. In: IEEE/ACM Symposium on Edge Computing (SEC), pp. 440–444. IEEE (2018)
8. Abbas, N., Zhang, Y., Taherkordi, A., Skeie, T.: Mobile edge computing: a survey. IEEE Internet Things J. **5**(1), 450–465 (2017)
9. Xu, X., Xue, Y., Qi, L., Yuan, Y., Zhang, X., Umer, T., Wan, S.: An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. Future Gener. Comput. Syst. **96**, 89–100 (2019)
10. Aggarwal, C., Srivastava, K.: Securing IoT devices using SDN and edge computing. In: 2nd International Conference on Next Generation Computing Technologies (NGCT) 2016, pp. 877–882. IEEE (2016)
11. Shi, W., Dustdar, S.: The promise of edge computing. Computer **49**(5), 78–81 (2016)
12. Guo, J., Ma, J., Li, X., Zhang, T., Liu, Z.: A situational awareness trust evolution model for mobile devices in D2D communication. IEEE Access **6**, 4375–4386 (2017)
13. Ahmed, A., Abu Bakar, K., Channa, M.I., Haseeb, K., Khan, A.W.: A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. Front. Comput. Sci. **9**(2), 280–296 (2014). https://doi.org/10.1007/s11704-014-4212-5
14. Zhang, P., Zhou, M., Fortino, G.: Security and trust issues in Fog computing: a survey. Future Gener. Comput. Syst. **88**, 16–27 (2018)
15. Zhang, J., Chen, B., Zhao, Y., Cheng, X., Hu, F.: Data security and privacy-preserving in edge computing paradigm: survey and open issues. IEEE Access **6**, 18209–18237 (2018)
16. Chen, L., Xu, J.: Socially trusted collaborative edge computing in ultra dense networks. In: Proceedings of the Second ACM/IEEE Symposium on Edge Computing, p. 11 (2017)
17. Wang, T., Luo, H., Jia, W., Liu, A., Xie, M.: MTES: an intelligent trust evaluation scheme in sensor-cloud enabled industrial Internet of Things. IEEE Trans. Ind. Inf. (2019)
18. He, Y., Yu, F.R., Zhao, N., Yin, H.: Secure social networks in 5G systems with mobile edge computing, caching, and device-to-device communications. IEEE Wirel. Commun. **25**(3), 103–109 (2018)
19. Rathi, S.R., Kolekar, V.K.: Trust Model for Computing Security of Cloud. In: Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1–5. IEEE (2018)
20. D'Angelo, G., Rampone, S., Palmieri, F.: Developing a trust model for pervasive computing based on Apriori association rules learning and Bayesian classification. Soft. Comput. **21** (21), 6297–6315 (2016). https://doi.org/10.1007/s00500-016-2183-1