


A Reliable Trust Computing Mechanism in Fog Computing

Vijay Lingaraddi Hallappanavar, K. L. E. College of Engineering and Technology, India

Mahantesh N. Birje, Visvesvaraya Technological University, India

 <https://orcid.org/0000-0003-0669-1829>

ABSTRACT

Due to the lack of trust on IoT devices, the integration of fog computing and IoT devices is hindered. Trust is considered to have two notions: subjective trust where the user puts his individual interests to the interactions and objective trust which depends only on individual interaction experiences. This paper proposes a reliable trust computing mechanism based on subjective and objective trust. The subjective trust is calculated from feedback of multiple sources. The incentive and punishment mechanism is applied to the subjective trust to avoid malicious devices. The objective trust is calculated based on quality of services. The overall trust helps the IoT devices to determine the trustworthiness of other IoT devices and in turn helps to establish a trusted environment. The experimental results show that the performance is better than existing methods in terms of time required to calculate the overall trust, reliability, and trustworthiness of IoT devices.

KEYWORDS

Fog Computing, Incentive Mechanism, IoT Devices, Objective Trust, Punishment Mechanism, Subjective Trust, Trust Computing Mechanism, Trustworthiness

1. INTRODUCTION

Fog computing is a distributed computing model that acts as an intermediate layer between Cloud layer and IoT layer. Due to large extent use of IoT devices in recent days, the computational demand has grown a lot and this demand is fulfilled by integrating Fog computing with IoT devices. This is possible by having Fog computing placed close to IoT devices (Yousefpour et. al., 2019; Mahmud, Srirama, Kotagiri & Buyya, 2019; Atlam, Walters & Wills, 2018). Fog computing not only provides services to Internet of things, but also extends its application to other networking systems such as Mobile network/Radio access network, Power line communication, Content distribution network, healthcare applications and Vehicular network (Mahmud, Kotagiri & Buyya, 2018; Paul & Pinjari, 2018). This integration has facilitated real time and latency sensitive applications to be deployed. But due to lack of trust on IoT devices, the integration of fog computing and IoT devices is hindering.

Numerous security issues and attacks exist such as message forging, message tampering and replay attacks (Al-khafajiy et. al., 2019; Khalid et. al., 2019; Birje, Challagidad, Goudar & Tapale, 2015; Birje & Hallappanavar, 2019; Mouna Jouini & Latifa Ben Arfa Rabai, 2016), which disturbs the secured communication and trust among entities (Usha Divakaria & K. Chandrasekaran, 2016). Trust is the basis for the IoT devices to collaborate with each other (Yuan & Li, 2018; Firdhous, Hassan & Ghazali, 2013). It requires establishment of a trust that eliminates the fear among entities and

DOI: 10.4018/IJCAC.2021010101

provides required quality of services (Hou et. al., 2015; Gupta & Saini, 2017). The trust mechanism eliminates the malicious service providers and allows the true service providers to provide services. It also keeps a track on the quality of services and keeps a check each service provider to provide good services. Hence there is a need of a mechanism to compute the trustworthiness of IoT devices.

Most of the previous works have considered either subjective trust (Jian & Qin, 2015) or objective trust for their trust calculation. The trust computing mechanism based on subjective trust in many works lack the information fusion from multiple sources and proper weight assignment to the feedbacks given (Azzedin & Ghaleb, 2019; Challagidad, Birje & Goudar, 2020). Trust mechanism based on objective trust in many works lack the proper weight assignment to the quality of services parameters (Zennaro, Ivanovska & Jøsang, 2019). Also there are no incentive and punishment mechanisms to promote or warn the IoT devices to provide correct feedback (Wang, Huang & Zou, 2016; Tian, Yang, Zhong & Liu, 2014; Xiong et. al., 2018; Lu & Mengshu, 2005). So it requires an attention to focus on subjective and objective trust which provides a reliable and trustworthy trust computation mechanism.

Therefore this work proposes a reliable trust computing mechanism that works in following three steps:

1. The subjective trust is computed through multiple source feedback fusion.
2. Further the incentive and punishment scheme is applied to the computed subjective trust
3. The objective trust is computed based on quality of services.

The contribution of this work is to design a reliable trust computing mechanism which combines the subjective and objective trust. Also, incentive and punishment mechanism is applied to the trust value to boost the IoT devices or punish the malicious devices.

The organization of the paper is as follows. Section II explains about the related work carried out so far. Section III covers architecture considered in the proposed work and trust computing mechanism. Section IV consists of results. The conclusion of the paper is covered in Section V.

2. RELATED WORK

Zhang, Zhou & Fortino (2018) classified secure communication into 2 types: First type is communication between IoT devices and Fog nodes and second is communication between fog nodes themselves. The paper presents the architecture of Fog computing and also shows the associated possible security and trust issues. Because Fog is extremely distributed, employment of security mechanisms for reliable data can affect its QoS to a great degree. The paper focuses the necessity to find new mechanisms to increase the security and trust of the Fog.

Yasir Hussain & Zhiqiu Huang (2018) presented trust and reputation based model for the malicious nodes in fog IoT computing. To calculate trust, multiple sources and reputation values are assigned different weights. This improves reliability of the system and helps the model to be unbiased and effective. For the reputation calculation in TRFIoT, an improved version of Page Rank system is implemented.

Wang et. al., (2017) proposed a fog based trust calculation method for trustworthy communication in sensor cloud system. It first establishes a general trust model that depends on previous feature values of the sensors' communication. Further when sensors upload communication features to fog nodes during each upload interval, the fog nodes calculate the trust value of the communications and classify the sensors into: credible nodes, suspect nodes and unbelievable nodes. If a sensor is found as unbelievable node, the fog node sends that information to the other sensors. Then, the unbelievable node cannot have access to resources, such as channels, data, and so on. The trust evaluation approach uses multiple linear regression problems. Also it adopts the least squares algorithm to find the best fitness function between sensors' behaviour and their trust values.

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/a-reliable-trust-computing-mechanism-in-fog-computing/266268

Related Content

Trust and Reputation in Digital Environments: A Judicial Inkling on E-Governance and M-Governance

Opeyemi Idowu Aluko (2019). *Security Frameworks in Contemporary Electronic Government* (pp. 191-206).

www.irma-international.org/chapter/trust-and-reputation-in-digital-environments/210944

Online Review Site Data in Service Innovation

Tuomo Eloranta (2016). *International Journal of E-Services and Mobile Applications* (pp. 20-34).

www.irma-international.org/article/online-review-site-data-in-service-innovation/163187

Prevention and Resolution of Labor Disputes

Irina Bocharova and Alexander Rymanov (2022). *International Journal of Service Science, Management, Engineering, and Technology* (pp. 1-13).

www.irma-international.org/article/prevention-and-resolution-of-labor-disputes/295559

Cloudlet and Virtual Machine Performance Enhancement With CLARA and Evolutionary Paradigm

Tanvi Gupta and Supriya P. Panda (2022). *International Journal of Cloud Applications and Computing* (pp. 1-16).

www.irma-international.org/article/cloudlet-and-virtual-machine-performance-enhancement-with-clara-and-evolutionary-paradigm/298322

Customers as Innovators in Senior Service Markets: An Examination of Innovation Potential and Characteristics

Lea Hennala, Helinä Melkas and Satu Pekkarinen (2013). *Best Practices and New Perspectives in Service Science and Management* (pp. 31-53).

www.irma-international.org/chapter/customers-innovators-senior-service-markets/74985