Enhancing Cloud-Based IoT Security through Trustworthy Cloud Service: An Integration of Security and Reputation Approach – Paper Review

Maanya C Bharath

January 22, 2023

Paper Credits: Xiang Li , Qixu Wang , Xiao Lan , Xingshu Chen, Ning Zhang, (Member, IEEE), AND Dajaing Chen, (Member, IEEE)

1 Topic Overview

The Internet of things (IoT) is an emerging technology that is defined as the network of physical objects, devices. Through the integration of the IoT and the Cloud, we have the opportunity to expand the use of the available technology that is provided in cloud environments. It provides a new paradigm for the development of heterogeneous and distributed systems, and it has increasingly become a ubiquitous computing service platform. IoT devices generate vast amounts of data which will improve the overall efficiency of cloud- based IoT context. However, due to the lack of sufficient computing and storage resources dedicated to the processing and storage of huge volumes of the IoT data, it tends to adopt a cloud-based architecture to address the issues of resource constraints. Since there are increasingly more competing cloud service providers (CSPs) that have similar functional properties, determining the trustworthiness of cloud service customers (CSCs) is important. The trust assessment or selection of CSPs reflects the cognition of CSCs with respect to the multiple cloud service attributes, such as reliability, scalability, availability, safety, and security. Some existing studies attempt to assess the trustworthiness of CSPs based on the quality of service (QoS) of teach candidate. There are also some studies that attempt to assess the trustworthiness of CSPs by employing the feedback ratings of CSCs, namely, the rating-based reputation evaluation, which has been widely adopted in web service-based. Therefore, it is widely recognized that without a sufficient security assessment, the accurate and true trustworthiness of a cloud service cannot be determined. In this paper, a novel trust assessment framework for cloud services (named STRAF) that combines its security and reputation characters, is proposed.

2 Key Contributions

The following are the key contributions of the author, and an understanding of the points.

1. A SECURITY ASSESSMENT MODEL was presented.

This model evaluates the security of CSPs by employing the security metrics in the deliverable template, which is called the security controls deliverable (SCD).

Standardization: The SCD acts as the standardized artifact that can demonstrate the security controls that are implemented in the cloud service of a CSP.

Conformity: The CSP measures and verifies the security controls that are implemented in its cloud services according to the SCD.

Thus this model evaluates the security of CSPs by employing the security metrics in the deliverable template.

2. A REPUTATION ASSESSMENT MODEL was presented.

In the reputation assessment model, a CSC either gives a feedback rating regarding the trustworthiness of a holistic cloud service or the quality of service (QoS) of a specific cloud service.

Credibility: In the practical scenario, some malicious customers may cooperate to provide a large amount of unfaithful feedback ratings in order to increase or decrease the reputation of a specific cloud service.

Certainty: It is worth considering that some malicious CSCs subvert the reputation assessment model by creating a large number of pseudonymous identities and using them to give numerous unfaithful feedback ratings.

The credibility and certainty of feedback ratings play important roles in this model for evaluating the trustworthiness of cloud services.

3. DESIGN GOALS were presented. Security Goal, Reputation Goal, Trust Goal are aimed to achieve to develop a trust assessment framework based on security and reputation for assessing the trustworthiness of cloud services.

4. The following algorithms are designed to tackle the security level evaluation.

Algorithm 1: Security-Based Trust Assessment. Input: the number of candidate CSPs m and security metrics n. Steps: Data Collection and Pre-processing -¿ Security Controls Deliverables Quantification -¿ Security Level Evaluation.

Algorithm 2: Security Level Evaluation. Input: Set of SCD Q, size of the set m × n. Steps: Security Level Evaluation (Q, m, n). Within which, relative closeness is identified.

Algorithm 3: Reputation-Based Trust Assessment Steps: Data Collection and Pre-processing -¿ Weight Factor Assignment -¿ Local Objective Reputation -¿ Global Objective Reputation.

Algorithms 4 and 5 describe in detail the process of achieving local and global objective reputation.

5. The experimental results for validating the performance are presented. Comparision of some existing security assessment methods and reputation assessment methods with trust assessment methods (SeTA and ReTA).

SeTA: There is no weight assignment process in SeTA and the evaluation approach of SeTA is concise, it has little impact on the SeTA method. Thus the method proposed is effective and outperforms the other methods.

ReTA: The ReC method has the highest rate of change, that is, its reputation is most vulnerable to malicious feedback ratings, and it is followed by ReM, ReA and ReTA, respectively. This demonstrates that the method proposed outperforms the other methods, especially when the percentage of malicious feedback ratings increases.

3 My Views

This framework has the ability to enhance the security of the cloud-based IoT context through trustworthy cloud services. It also facilitates CSCs in assessing the trustworthiness of the cloud services provided by the functionally equivalent CSPs and selecting the most trustworthy one from them to on which to deploy the cloud service. It is worth noting that the advantage of the STRAF is that it takes into account both security and reputation as complementary features to evaluate trustworthiness of cloud services and accordingly obtain the quantitative trustworthiness of cloud services. Additionally, in order to incorporate the security metrics in the trust assessment, we present a security-based trust assessment method (namely, SeTA). In addition, for the improvement of the accuracy and reliability of the feedback rating-based reputation assessment model, we present a reputation-based trust assessment method (namely, ReTA). Furthermore, for the sake of the potent combination of SeTA and ReTA, an integrated trust assessment method (namely, InTA) is proposed to assess the overall trustworthiness of cloud services. Simulation-based experiments validated the performance and availability of our proposed methods.

Trust is an important, completely significant factor to consider while working on IoT, cloud systems and its future contributions in making “life easier”, as we know it. Several factors are responsible for deeming the trustworthiness of a machine. Technologically advancing means, trusting automation more and more, for its full use and advantages cannot be gained without doing so.

That being said, I believe a key point that is of utmost significance has not been given the importance it deserves. While speaking of trusting a system, any system, despite the performance evaluation, various techniques of ensuring maximum trust, the accessibility of the system needs to be questioned. A large population do not find it difficult to trust a cloud system for example, but their highly private data being put up and integrated with IoT only increases the percentage of access to said data. Data being one of the most coveted resources in this advancing world, needs to be protected at all costs. The paper beautifully describes methods to achieve the same.