Event Evaluation and Trust Management in Fog Computing Architecture

Youssef Sellami, Youcef Imine, Antoine Gallais
LAMIH-UMR CNRS 8201, Université Polytechnique Hauts-de-France Valenciennes, France
Email: {Youssef.Sellami, Youcef.Imine, Antoine.Gallais}@uphf.fr

Abstract—Event trustworthiness is an important factor that influences every entity in fog computing systems. This raises many security concerns regarding the reliability of the events shared between fog nodes and data sources. Indeed, malicious entities may provide inaccurate or modified information to mislead honest ones and influence their behavior. To avoid these situations, robust information trust assessment and management mechanisms are required. Therefore, in this paper, we present a new Blockchain-based solution to evaluate event trustworthiness in fog computing architecture. Our solution creates a transparent and traceable environment, allowing for the preservation of trust scores and fostering accountability. Moreover, it presents a new trust model calculating event trustworthiness based on multiple factors such as the plausibility of the event, its temporal relevance, and its distance relevance. As a result, malicious entities can be identified and trustworthy behavior can be encouraged in the fog computing environment. Finally, we prove that our protocol is highly effective, as demonstrated by comprehensive simulations.

Index Terms—Fog computing, Security, Trust management, Blockchain.

I. INTRODUCTION

Fog computing has become an emerging paradigm in today’s digital ecosystem, enabling the seamless integration of cloud services and edge devices to analyze data as close to the edge as possible [1, 2]. This distributed design creates several opportunities for efficient data processing and improved user experience. However, to fully achieve the potential of fog computing, trustworthiness is an important consideration [4]. When it comes to building confidence and trustworthiness among entities involved in fog computing infrastructures, trust scores play a critical role. These scores are critical for establishing participant trustworthiness, making successful decisions, and maintaining a safe environment. Existing fog computing trust computation solutions [5] usually focus on judging the trustworthiness of the reporter, ignoring assessing the trustworthiness of the data itself.

To ensure the accuracy of information circulated on the network, trust must be established between these entities. The issue is to mitigate the dangers posed by malevolent actors and data manipulation. To overcome these challenges and develop a trustworthy ecosystem, blockchain technology has garnered significant attention [3, 6]. Blockchain is an immutable and decentralized ledger that enables transparency and traceability. As a result, the secure and transparent nature of blockchain allows trust scores to be securely kept.

To address these challenges, we present a novel event evaluation mechanism for fog computing architectures. Our approach introduces a new trust model for event evaluation that takes into account a variety of characteristics such as the evaluators’ reputation, location, and evaluation time when assessing the events. On the other hand, it updates the reputation of the evaluators depending on their overall activity in the network using Blockchain technology.

The remainder of this paper is organized as follows: In Section II, we present the proposed approach. In Section III, we evaluate the performance of our solution. Finally, in Section IV, we conclude the paper and we present some perspectives.

II. PROPOSED APPROACH

This section introduces our suggested scheme, in which several edge components play an important role in ensuring the trustworthiness of shared events. We address this issue by implementing a procedure at the fog layer that detects fake events and encourages edge devices to behave responsibly via reward or punishment mechanisms. Our approach awards trust scores to data based on direct feedback from other participants. The evaluation of events takes into account the temporal significance of the data, the distance between the event and the evaluator’s location, and the evaluator’s trust score. Furthermore, the Blockchain serves as a reference for trust scores of events and participants as they move across different zones.

A. Architecture design overview

Our distributed architecture is divided into zones as shown in figure 1. We have the following components within each zone:

- Fog servers: are critical components of our architecture for providing data and events storage services.
- Edge layer: composed of users that are event publishers or evaluators. Some of them can act maliciously. Note that, a publisher cannot act as an evaluator for the same event.
B. Our Trust Model

Our model evaluates the trustworthiness of an event $E_j$ over a duration (lifetime) $LT_j$ and geographical distance $D_{j_{\text{max}}}$. Thus, in our trust model, we utilize the following phrases to specify the parameters of our method:

- Event trustworthiness score $E_j^T$: it reflects the degree of trustworthiness toward the event $E_j$.
- Plausibility score $\text{Plaus}_j^i$: reported by evaluator $Eva_i$ to the fog servers.
- Time score $T_j^i$: reflecting temporal information about when the evaluator $Eva_i$ has evaluated the event.
- Distance score $D_j^i$: measures the proximity of the evaluator $Eva_i$ in terms of distance to the event location.

III. Performance evaluation

In this Section, we simulate several events that were distributed to all evaluators via an event publisher. Figure 2 depicts the evaluation of an event’s trustworthiness $E_j^T$ by several evaluators, with 30% of them being malicious ($\eta=0.7$). All evaluators maintain a certain rate $\Theta \leq 0.2$. For honest evaluators, the plausibility score $\text{Plaus}_j^i$ is at least 0.8. This Figure illustrates changes as a function of time and distance. It should be noted that malicious evaluators attempt to undermine the event from the start, resulting in initially poor plausibility rankings. However, due to the limits imposed by our theoretical study, these attempts ultimately fail. As a result, event reliability is constantly high, exceeding the predefined minimum threshold of $x=0.5$.

IV. Conclusion

In this paper, we present a new protocol for event evaluation in the fog computing architecture. We proposed a new trust model that provides an evaluation based on different aspects, including plausibility, temporal relevance and distance relevance. In addition, we use Blockchain to improve transparency and traceability, ensuring the storage of trust scores and fostering responsibility. In the future, we plan to examine the use of prediction techniques based on deep learning models to prevent malicious activity.

REFERENCES