A Scalable Framework for Responsive Trustworthiness Dissemination in Social IoA

Federica de Trizio
f.detrizio@phd.poliba.it
Politecnico di Bari
Bari, Italy

Giancarlo Sciddurlo
giancarlo.sciddurlo@poliba.it
Politecnico di Bari
Bari, Italy

Antonio Petrosino
antonio.petrosino@poliba.it
Politecnico di Bari
Bari, Italy

Giuseppe Piro
giuseppe.piro@poliba.it
Politecnico di Bari
Bari, Italy

Gennaro Boggia
gennaro.boggia@poliba.it
Politecnico di Bari
Bari, Italy

Abstract

The Social Internet of Anything (SIoA) has recently emerged as a novel approach that fosters information sharing by connecting people, processes, data, and IoT devices through social networks. In this context, existing methodologies for managing the increasing number of connected entities and ensuring the dynamic and efficient dissemination and maintenance of trustworthiness information are often computationally intensive and time-consuming. As a result, this work introduces a scalable double-clustered architecture that leverages edge-fog computing alongside a novel framework to enable the responsive dissemination of available and updated trustworthiness information for entities within a Social Internet of Anything environment.

Keywords

Social Internet of Anything; trustworthiness dissemination

ACM Reference Format:
Federica de Trizio, Giancarlo Sciddurlo, Antonio Petrosino, Giuseppe Piro, and Gennaro Boggia. 2024. A Scalable Framework for Responsive Trustworthiness Dissemination in Social IoA. In *Proceedings of the CoNEXT Student Workshop 2024 (CoNEXT-SW '24), December 9–12, 2024, Los Angeles, CA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3694812.3699925

1 Introduction

The Social Internet of Anything (SIoA) integrates people, processes, data, and Internet of Things (IoT) devices to enhance the utility of network interactions, enabling novel network experiences and creating unparalleled economic opportunities [2]. The arisen technology has progressively influenced a wide range of applications, including healthcare, smart homes, and smart manufacturing, facilitated by the widespread access to the global Internet provided by Beyond 5G (B5G) networks. By leveraging the concept of social networks, the SIoA has the potential to enhance interactions, particularly in terms of security and trust, thereby addressing prevalent challenges in IoT technology, such as user visibility and the effective discovery of resources and services. Research in this field explores trust management and evaluation techniques aimed at establishing reliable relationships and securing communications, thereby enabling trustworthy information sharing [3].

CoNEXT-SW '24, December 9–12, 2024, Los Angeles, CA, USA

ACM ISBN 979-8-4007-1255-5/24/12
https://doi.org/10.1145/3694812.3699925

2 Problem Statement

In a SIoA environment, interconnected people, processes, and devices—referred to as entities—are endowed with social awareness, enabling them to autonomously establish social relationships. In this context, ensuring the availability and continuous updating of entities' trustworthiness has become increasingly challenging in large-scale networks. The mobility and frequent state transitions of entities, such as sleeping, waking up, or leaving and rejoining networks, further exacerbate this challenge. Therefore, maintaining scalability and a high level of responsiveness is crucial to support billions of entities that interact, share resources, and provide services, while ensuring access to up-to-date information about the most trustworthy service providers [5]. Related works in the scientific literature have proposed blockchain technology as a viable solution for developing effective frameworks to disseminate essential information within the social network of entities [4]. However, this solution is not well-suited to handle large volumes of data and suffers from high latency and limited adaptability to dynamic network changes. Consequently, scalability and responsiveness in disseminating and maintaining trustworthiness information remain significant challenges [1].

To address this gap, new strategies are needed for the responsive aggregation, updating, and dissemination of trustworthiness information in SIoA systems.

3 Proposed Framework

To advance the scientific literature, this work proposes an architecture that leverages edge-fog computing. By combining local processing at the network edge with fog computing resources, this approach aims to optimize performance and scalability for distributed applications and services. Furthermore, the proposed design incorporates two levels of clustering, as illustrated in Fig. 1.

At the first level, a social entity can represent its digital counterpart of the physical entity. Depending on their application context, these digital counterparts can join communities, thereby enhancing network navigability. In a SIoA environment, a service-based

grouping solution effectively reduces latencies in the service discovery process. Each community is managed by an edge node, which is responsible for computing and storing the trust values of its members and, if necessary, excluding malicious entities through trust management procedures. The second level, instead, is based on geographical position and is managed by Primary Fog nodes, which handle a territorial cluster's data collection. Furthermore, this work defines a framework for sharing trustworthiness information between independent territorial clusters, enhancing the system's scalability while improving the responsiveness required by B5G networks. Specifically, the proposed framework eliminates the need for a centralized services orchestrator with comprehensive knowledge of the network topology or the trustworthiness of each entity. Instead, this responsibility is delegated to Primary Fog nodes distributed across different geographical areas. Thus, this work introduces a novel publisher/subscriber design pattern (i.e., MQTT-based) to facilitate fog-cloud communication for information sharing among independent clusters. This approach ensures service continuity by accommodating the mobility of entities between territorial clusters. The message flow of the designed model is described below:

1. The moving entity attempts to join a service community managed by an edge node in a new territorial cluster.
2. To initiate this process, the Primary Fog node sends a *"trust discovery request"* via the cloud to retrieve the entity's trustworthiness information.
3. The cloud creates a query for the entire network by contacting the broker and publishing the request.

All Primary Fog nodes that have information related to the service community of the searched entity's trustworthiness relay the requested data. 4. The cloud waits for and collects all data received from edge nodes, as signaled by the appropriate Primary Fog nodes, and aggregates this into synthetic data.

5. The Primary Fog node that initiated the *"trust discovery request"* receives the updated trust value and assigns a degree of trust to the moving entity, based on the aggregated network knowledge.

4 Preliminary Evaluation

Computer simulations are conducted using a C++ simulator to evaluate the system's performance in terms of information-sharing responsiveness. To assess the effectiveness of the proposed methodology, its performance is compared with two benchmark approaches: the baseline and blockchain-based approaches, as shown in Fig. 2. In the baseline approach, each cluster operates independently, without synchronization. In the blockchain approach, data sharing is achieved through a transaction process that incurs a mandated delay due to the Proof of Work (PoW) protocol. Fig. 2 demonstrates that the proposed methodology outperforms the others in both efficiency and responsiveness. Specifically, compared to the baseline approach, the proposed framework prevents malicious entities from resetting their reputation during handover. Additionally, it achieves lower latencies in synchronization between clusters compared to the blockchain approach.

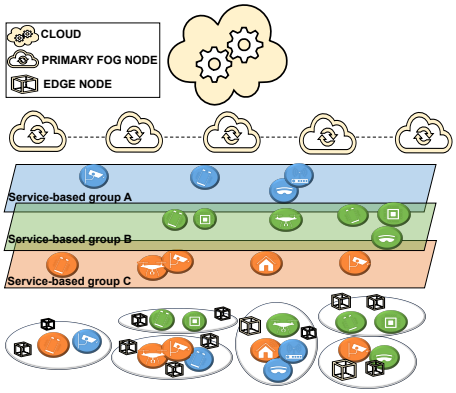

Figure 1: The proposed double-clustered architecture.

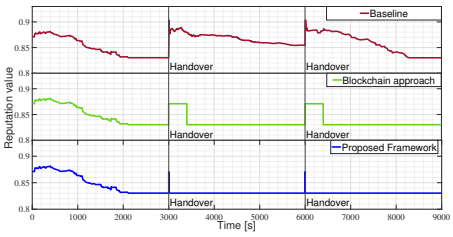

Figure 2: Entities' reputation values propagation.

Acknowledgments

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, Mission 4, Component 2, in the context of partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART", CUP: D93C22000910001), national center on "Sustainable Mobility" (CN00000023 - program "MOST", CUP: D93C22000410001), and partnership on "Cybersecurity" (PE00000007 - program "SERICS", CUP: D33C22001300002, project ISP5G+). It was also supported by the PRIN 2022 projects INSPIRE (grant no. 2022BEXMXN 01) and HORUS (grant no. 2022P44KA8) funded by the Italian MUR, by the HORIZON MSCA project BRIDGITISE (grant no. 101119554) and the HORIZON JU SNS project 6G-GOALS (grant no. 101139232).

References

[1] Min Deng, Yuanlin Lyu, Chunmeng Yang, Fang Xu, Manzoor Ahmed, Na Yang, Ze Xu, and Can Ke. 2024. Lightweight trust management scheme based on blockchain in resource-constrained intelligent iot systems. *IEEE Internet of Things Journal*, 11, 15, 25706–25719.

[2] Ching-Hsien Hsu, Carlos Enrique Montenegro Marin, Ruben Gonzalez Crespo, and Hassan Fouad Mohamed El-sayed. 2022. Guest editorial introduction to the special section on social computing and social internet of things. *IEEE Transactions on Network Science and Engineering*, 9, 3, 947–949.

[3] Wazir Zada Khan, Qurat-ul-Ain Arshad, Saqib Hakak, Muhammad Khurram Khan, and Saeed-Ur-Rehman. 2021. Trust management in social internet of things: architectures, recent advancements, and future challenges. *IEEE Internet of Things Journal*, 8, 10, 7768–7788.

[4] Oscar Novo. 2018. Blockchain meets iot: an architecture for scalable access management in iot. *IEEE Internet of Things Journal*, 5, 2, 1184–1195.

[5] Giancarlo Sciddurlo, Antonio Petrosino, Domenico Striccoli, Giuseppe Piro, Luigi Alfredo Grieco, and Gennaro Boggia. 2022. Boosting service provisioning in siot by exploiting trust and capability levels of social objects. In *2022 IEEE International Conference on Smart Computing (SMARTCOMP)*, 1–6.