[1]Upul JAYASINGHE, [2]Gyu Myoung LEE
([1,2]Department of Computer Science, Liverpool John Moores University, Liverpool, UK)

AI AND BLOCKCHAIN ENABLED EDGE OF THINGS WITH PRIVACY PRESERVING COMPUTATION

Annotation. Recent research has brought cloud, edge, and Internet of Things (IoT) technologies together to develop integrated platforms for utilizing resource-rich clouds to support resource-constrained IoT applications. However, their success is limited, in particular, they are lack of efficient intelligence for data processing and service operations as well as dynamic and trustworthy service composition across multi-layers from IoT devices to clouds, which are important for IoT applications. This article will thus propose an innovative platform for composing smart and trustworthy edges (ROOF (Real-time Onsite Operations Facilitation) plus Fog) of things to support applications ranging from ultra-low delay and lightweight to complex services. To achieve this goal, the research employs the microservice concept to decompose applications into lightweight services located from the edge of things to cloud data centers. Further, inspired by the artificial intelligence and blockchain technologies, this work proposes a novel approach for composing microservices that will provide prosumer-driven, decentralized and autonomous service composition while preserving the privacy of the participating stakeholders.

Keywords. Blockchain, Edge Computing, Internet of Things, Microservice, Privacy, Trust.

1. Introduction

Internet of Things (IoT) data is becoming one of the most valuable assets in today's data-driven digital economy as it leads to developing many business models providing numerous ubiquitous and intelligent services [1]. However, these data contain sensitive personal information and can reveal the identity of the associated stakeholders if a proper privacy preserving mechanism is not in place [2]. On the other hand, distributed nature; massive scale; and scarcity of computational power, storage, bandwidth, etc. of IoT does not provide a safe platform for privacy preserving applications. Further, traditional applications of IoT are designed in such a way that data management functions, i.e. data collection, data storage, data processing, data sharing, and data destruction, are executed in a centralized fashion, neglecting the distributed nature of IoT devices. This approach has proved to lead to significant delays and traffic congestion when used for delay sensitive applications and thus cannot satisfy the requirements of ultra-low delay sensitive IoT applications such as a real-time computer vision for smart city security. It not only worsens the issues associated with scalability and latency, but it also makes IoT nodes more vulnerable for privacy and security threats including lack of control over personal data hence unauthorized user profiling and identity theft, fake knowledge propagation, network eavesdropping, illegal invasion, and denial of service (DoS) attacks.

On the other hand, a hierarchical edge computing architecture can resolve the issues associated with centralized architectures by pushing data pipeline functions towards the edge of the IoT networks depending on the resource availability and application requirements [3], [4]. Deployment of such an architecture is beneficial to build an ecosystem involving content providers, application developers, network equipment vendors, third-party partners, and middleware providers; and thereby to improve the end-user experience dramatically due to powerful and energy efficient computing power at hand, low latency, mobility, location, and context-aware support for IoT applications [5], [6]. However, edge computing alone cannot support the safeguarding of the privacy of the stakeholders, as it introduces a new set of vulnerabilities due to multiple attack surfaces, closeness to sensitive data generators, heterogeneity of the device resources, the scale of the network, and difficulty of assessing the trustworthiness of participating stakeholders [7], [8]. In contrast, the fundamental concept behind blockchain technology provides a promising approach to establish a healthy interaction among untrustworthy and unknown entities, while supporting the distributed nature of IoT eliminating the need of a central authority as in cloud computing architectures [9], [10].

Motivated by the facts stated above, this article discusses a possible privacy perceiving edge computing architecture based on the concepts of microservices, Artificial Intelligence (AI), and Blockchain. Basically, microservice concepts are applied here to overcome computationally inefficient resource and service management as in cloud-based architectures. Further to enhance the privacy and intelligent use of resources, the idea of microservice concept is combined with AI and blockchain technology. The structure of this publication is as follows: Section 2 presents the concept of AI and blockchain based service composition for the edge of things platform. Section 3 discusses the usability of blockchain technology on preserving the privacy and Section 4 deals with the conclusions.

2. AI and blockchain based service composition for the edge of things

The idea of distributed edge refers to fluid data management and decision-making towards physical things, working as a middle layer between the cloud and the users. Comply with edge computing requirements, this article further breakdown the so-called middle layer by introducing two layers, i.e., ROOF[1] [11] and Fog, in order to make the system architecture more feasible and deployable in a real-time environment with an ambitious vision for seamless fluid control and decision-making through harmonize resource management among different layers.

Due to the distributed nature of IoT, sharing data over different services creates an immense threat on user privacy, hence proper regulatory and protection mechanisms must be in place to safeguard the privacy of the consumers [12]. In this regard, the blockchain concept provides a resilient and distributed way to protect the integrity of the data due to its inherent resistance to data modification, which can be extended for privacy protection as well. Any given block in a blockchain cannot be altered retroactively, as this would invalidate all the previous blocks and hence break the consensus agreed among nodes in the peer-to-peer network used. However, this involves a computationally inefficient process, e.g. a so-called Proof-of-Work (PoW), which essentially uses a set of powerful nodes called "miners" to solve a computationally intensive puzzle to verify transactions and add them as an encrypted block to the chain. Due to this, it is unfeasible to perform the process with resource-limited nodes such as IoT devices, which introduces a major challenge in blockchain applications for IoT and other mobile services.

In order to avoid such drawbacks, it is beneficial to breakdown the blockchain into several sub-chains and combines them with edge computing concepts in order to improve the mining time while keeping the inherited properties of blockchains. Concepts like edge computing allow Service Providers (SPs) to deploy cloud computing services at the "edge" of the mobile Internet. For example, Base Stations (BS) equipped with a small data center, or at least a home server placed at the gateway of the smart home network might be able to accept offloaded jobs from adjacent mobile and IoT devices in order to deploy blockchains.

As shown in Figure 1 for a smart city use case, different layers of blockchains will be established by their responsible computing authorities. To explain the applicability of blockchain in a real-world scenario, a smart city use case has been used here. In which, bottom layer represents the IoT nodes like sensors, smartphones, tablets, etc. and ROOF agents such as hubs, routers, home servers, etc. To facilitate localized services which demand real-time decision-making capabilities like in emergency services, energy management services, etc. blockchains in ROOF will work together through smart contracts among them. Due to the light weight of the consensus protocol which will be investigated here, even a ROOF node has the ability to validate new blocks and add them to the genesis blockchain improving the overall performance of the IoT local network. At the area level, a collection of distributed servers at the Fog layer can establish a permissioned blockchain based on the data coming from ROOF nodes as well as data stored in the distributed blockchain at the fog to facilitate near real-time services. Further, depending on the computational power available to Fog nodes, it is possible to deploy AI and data mining techniques to obtain extra knowledge about a situation to respond it correctly. Blockchain at Fog layer will act as a control layer in such cases to compose the services required by area-level applications in a smart city. In order to improve the interoperability among several blockchains, distributed exchange (DEX) will act as a broker as shown in Figure 1.

[1] ROOF: Real-time Onsite Operations Facilitations

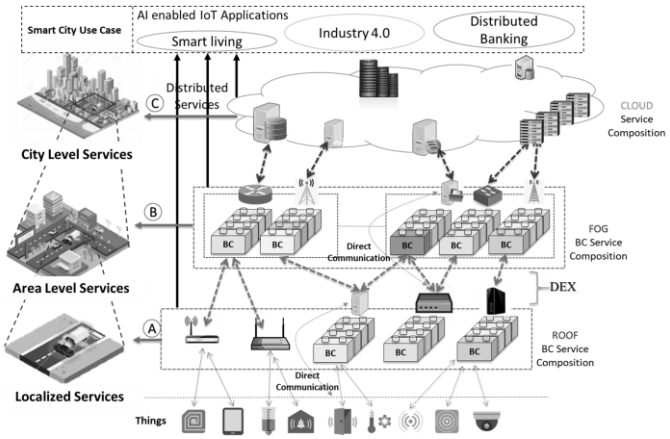

Figure 1. **Blockchain enabled Edge Computing in a Smart City.**

Note that not all entities are equipped with enough resources to form a permissioned blockchain especially at the ROOF level. Furthermore, it is not required to send all the data through the blockchain. Depending on the user consent and privacy requirements, some data is directly transmitted towards the upper layer for immediate processing (e.g. public domain data) as denoted with "Direct communication" in Figure 1. In certain cases, links based on cryptographic hashes can be utilized to preserve the privacy of data. On the other hand, blockchain-based service composition enables prosumers to interact with each other without a centralized authority but by a community of peers in the form of a peer-to-peer network, in which trust is not placed on an individual but rather distributed across the entire population. Hence, no one can unilaterally take actions on behalf of the community and approve or change the composition. Moreover, the distributed nature of blockchains enables both horizontal and vertical service composition depending on the application requirement. For example, it can be used to track microservices that are urgently needed in the composition to provide emergency services during an accident as shown at the bottom layer of Figure 1 (Point A). In such a situation, a smart contract can be used to trigger certain services stored in the blockchain or to find the services stored in a separate database and generate combined results. The scenario discussed also applies to fog and cloud levels in a similar manner, and the concept of smart contracts can be used to facilitate communications between different layers when taking higher level decisions, e.g. at the cloud layer.

3. Blockchain based privacy preserving for edge of things

By design, the proposed platform is developed as a permissioned type of blockchain to control the privacy matters associated with a public blockchain and support business requirements demands by the service providers. Therefore, all entities who need edge of thing services are required to register with the membership services in the platform in order to obtain an identity to access the distributed services such as to carrying out transactions, obtaining services offered by service providers, interacting with smart contracts, etc. However, there is no centralized authority to manage such credentials and hence the responsibility relies on the distributed microservices who act as agents on such cases. Basically, when assigning an identity by an agent to a prospective entity, it will first evaluate the trustworthiness of the entity with respect to the services he is demanding. The trust evaluation process follows a similar approach as discussed in our previous work [8]. It's up to the entities to behave and collaborate in a good manner to improve his reputation gradually if he needs to access more advanced services in the proposed edge of things environment. On the other hand, policy services are considered in the platform on preserving the privacy of the prosumers, monitoring consents, meeting consensus rules and ensuring accountability in case of policy violations. In this regard, the trust service can support to track such rules to detect violations beforehand and take necessary countermeasures in case of an incident already occurred. More detail version of building such a system is discussed in our previous work [12] in compliance with EU General Data Protection Regulation (GDPR) legislation when it comes to privacy matters.

4. Conclusions

This work proposes a novel edge computing solution by integrating Cloud, ROOF, Fog, IoT, microservices, AI, and blockchain technologies to support efficient, ultra-low delay sensitive, smart and trustworthy future IoT applications. The microservices represents a collection of miniature, self-contained, and autonomous services which can be coupled together to serve a more advanced task. Further, blockchain as a decentralized data structure provides a promising approach to handle the security, privacy, and accountability issues associated in a distributed environment. The proposed work also envisions providing intelligence at the edge of things, which represents Fog, ROOF, and IoT nodes collectively, such that the data on IoT resources and operations would not have to be transmitted to the cloud data centers, as intelligent decisions can be taken closer to where they are needed. The approach is based on a distributed and integrated ROOF-Fog-Cloud architecture where AI functionality can be factored into smaller functions that can be independently implemented and deployed on the platform as distributed microservices. With this approach, intelligence does not have to be provided by AI algorithms running on some powerful cloud data centers. Instead, the intelligence can be provided in a hierarchical and fluid manner from the ROOF layer to the Cloud layer, depending on the available and required resources by the functions being executed by the AI microservices. Further, AI and blockchain combined approach create new ways for negotiating, selecting, composing, validating, and monitoring service composition and coordination in a smart, secure, dynamic, autonomous and efficient manner while preserving the privacy of the participating stakeholders.

Acknowledgments

This work was supported by the Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT). [2018-0-00261, GDPR Compliant Personally Identifiable Information Management Technology for IoT Environment].

Bibliographic List

[1] A. Opher, A. Onda, A. Chou, and K. Sounderrajan, "The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization," *IBM Corporation: Somers, NY, USA*, 2016.

[2] M. Seliem, K. Elgazzar, and K. Khalil, "Towards Privacy Preserving IoT Environments: A Survey," *Wireless Communications and Mobile Computing,* vol. 2018, pp. 15, 2018.

[3] H. Tianfield, "Towards Edge-Cloud Computing," in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 4883-4885.

[4] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A Survey on the Edge Computing for the Internet of Things," *IEEE Access,* vol. 6, pp. 6900-6919, 2018.

[5] V. Moysiadis, P. Sarigiannidis, and I. Moscholios, "Towards Distributed Data Management in Fog Computing," *Wireless Communications and Mobile Computing,* vol. 2018, pp. 14, 2018.

[6] S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications and issues," in *Proceedings of the 2015 workshop on mobile big data*, 2015, pp. 37-42.

[7] W. Shi, and S. Dustdar, "The Promise of Edge Computing," *Computer,* vol. 49, no. 5, pp. 78-81, 2016.

[8] U. Jayasinghe, G. M. Lee, T. Um, and Q. Shi, "Machine Learning Based Trust Computational Model for IoT Services," *IEEE Transactions on Sustainable Computing,* vol. 4, no. 1, pp. 39-52, 2019.

[9] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Transactions on Knowledge and Data Engineering,* vol. 30, no. 7, pp. 1366-1385, 2018.

[10] N. Rifi, N. Agoulmine, N. Chendeb Taher, and E. Rachkidi, "Blockchain Technology: Is It a Good Candidate for Securing IoT Sensitive Medical Data?," *Wireless Communications and Mobile Computing,* vol. 2018, pp. 11, 2018.

[11] A. Meloni, S. Madanapalli, S. K. Divakaran, S. F. Browdy, A. Paranthaman, A. Jasti, N. Krishna, and D. Kumar, "Exploiting the IoT Potential of Blockchain in the IEEE P1931.1 ROOF Standard," *IEEE Communications Standards Magazine,* vol. 2, no. 3, pp. 38-44, 2018.

[12] U. Jayasinghe, G. M. Lee, and A. MacDermott, "Trust-Based Data Controller for Personal Information Management," in *2018 International Conference on Innovations in Information Technology (IIT)*, Al Ain, UAE, 2018, pp. 123-128.