International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 149-151
Published Online July 2022 in IJEAST (http://www.ijeast.com)

BLOCKCHAIN-ENABLED FOG RESOURCE ACCESS AND GRANTING

Sowmya M Y
PG Student, Department of CSE,
Akshaya Institute of Technology, Tumakuru, Karnataka
Visvesvaraya Technological University,
Belagavi, Karnataka, India

Mrs Roopa T
Assistant Professor, Dept of CSE,
Akshaya Institute of Technology, Tumakuru, Karnataka
Visvesvaraya Technological University,
Belagavi, Karnataka, India

Abstract— **Fog computing is a new computing paradigm for meeting ubiquitous massive access and latency-critical applications by moving the processing capability closer to end users. The geographical distribution/floating features with potential autonomy requirements introduce new challenges to the traditional methodology of network access control.**

In this project, a blockchain-enabled fog resource access and the granting solution is proposed to tackle the unique requirements brought by fog computing. The smart contractual concept is introduced to enable dynamic, and automatic credential generation and delivery for an independent offer of fog resources. Negotiated transaction mechanism supports the fog resource provider to dynamically publish an offer and facilitates the choice of the preferred resource by the end-user. There is no central authority needed to verify your identity, and relieve the processing pressure brought by massive access and single-point failure. Our solution can be extended and used in multi-access and especially multi-carrier scenarios in which centralized authorities are absent.

Keywords: **Blockchain, digital ledger, distributed ledger technology, supply chain management.**

I. INTRODUCTION

Fog computing, as shown in Fig. 1, is an extension of traditional cloud-based computing model, which selectively moves computing, data storage, transmission, jurisdiction and decision-making closer to the network edge where data are being generated. Similar with edge computing concept, fog computing can relieve the limitations in current network infrastructure and better support mission-critical, data-dense use cases.

Fog computing is often erroneously called edge computing, but there are key differences. As its name suggests, fog is geographically distributed with uncertainty and instability, similar to the real fog that floats everywhere without a fixed shape. As for the edge concept, it always means relatively static or stable resources, which are typically deployed at certain places, e.g., a central office.

In a word, federating and floating are the key differences between the fog and edge nodes rather than physical location. In fog cases, the geo-distributed fog resources are formed as a widespread resource pool.

In addition, different fog nodes may work together to support collaborative tasks, e.g., Augmented Reality(AR) mobility, robot teamwork, and distributed storage. Services or applications can be unaware of any specific fog node that provides resources and where it is. To some extent, edge computing can also be considered as a type of fog computing.

In contrast with traditional cloud computing, several unique features bring quite different problems in fog computing scenarios. First, each fog node must authenticate the requestor and verify its right to access the fog resources. In traditional cloud computing, normally an access entrance is responsible for all authentication and authorization actions.

This centralized access entrance performs a unified authentication and authorization procedure, which means that each subscriber usually uses a static password/key to access corresponding resources until they intend or are required to change the password/key.

In addition, the price of a resource usually is static and unified no matter when the subscriber requests that resource unit. A similar phenomenon occurs in a telecom network: all resources for upper-layer applications are deployed behind an access gateway that is responsible for performing authentication/authorization/accounting functions. All the resources belong to the operator and a uniform access offer is provided.

In fog scenarios, fog resources are physically located on the network edge, which is beyond the traditional access gateway, e.g., broadband network gateway and mobile management entity entities. Basically, traffic must undergo a round trip through an access gateway, because the edge/fog node cannot perform access control. In addition, different fog nodes may belong to different vendors, and even an individual can share spare resources on a residential gateway or WLAN AP and make these entities work as fog nodes. These different fog providers may have to perform autonomous access control and independent charging actions. To some extent, fog providers must build their own access control infrastructure. On the other hand, fog node providers may decide their own price for a resource according to the cost, time, node status, and even personal preference. The subscribers have more choices on fog nodes/providers and therefore may choose more cost-effective nodes to fulfill their requirements. During the access of the entire fog resource and granting procedure, several issues emerge.

II. LITERATURE SURVEY

[1] T. M. Fernandez-Carames and P. Fraga-Lamas, A review ´ on the use of blockchain for the internet of things, IEEE Access, vol. 6, pp. 32979–33001, 2018.

[2] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, ControlChain: Blockchain as a central enabler for access control authorizations in the IoT, in Proc. 2017 IEEE Global Communications Conf., Singapore, 2017, pp. 1–6.

[3] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, FairAccess: A new blockchain-based access control framework for the Internet of Things, Security and Communication Networks, vol. 9, pp. 5943–5964, 2016.

[4] P. Wang, Y. L. Yue, W. Sun, and J. J. Liu, An attribute based distributed access control for blockchain-enabled IoT, in Proc. 2019 Int. Conf. Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 2019, pp. 1–6.

[5] C. Dukkipati, Y. P. Zhang, and L. C. Cheng, Decentralized, Blockchain based access control framework for the heterogeneous Internet of Things, in Proc. 3rd ACM Workshop on Attribute-Based Access Control, Tempe, AZ, USA, 2018, pp. 61–69.

[6] Y. Y. Zhang, S. Kasahara, Y. L. Shen, X. H. Jiang, and J. X. Wan, Smart contract-based access control for the Internet of Things, IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594–1605, 2019.

[7] R. H. Xu, Y. Chen, E. Blasch, and G. S. Chen, BlendCAC: A Blockchain-enabled decentralized capability-based access control for IoTs, in Proc. 2018 IEEE Int. Conf. Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, Canada, 2018, pp. 1027–1034.

[8] D. Di, F. Maesa, P. Mori, and L. Ricci, Blockchain based access control, in Proc. Distributed Applications and Interoperable Systems, Neuchatel, Switzerland, 2017, pp. 206–220. [9] C. Lin, D. B. He, X. Y. Huang, K. K. R. Choo, and A. V. Vasilakos, BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, Journal of Network and Computer Applications, vol. 116, pp. 42–52, 2018. [10] T. Sanda and H. Inaba, Proposal of new authentication method in Wi-Fi access using Bitcoin 2.0, in Proc. IEEE 5th Global Conf. Consumer Electronics, Kyoto, Japan, 2016, pp. 1–5. [11] X. Jiang, M. Z. Liu, C. Yang, Y. H. Liu, and R. L. Wang, A blockchain-based authentication protocol for WLAN mesh security access, Computers, Materials and Continua, vol.58, no. 1, pp. 45–59, 2019. [12] Y. L. Chen, X. J. Wang, Y. L. Yang, and H. Li, Location aware Wi-Fi authentication scheme using smart contract, Sensors, vol. 20, no. 4, p. 1062, 2020. [13] X. Lin, J. H. Li, J. Wu, H. R. Liang, and W. Yang, Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach, IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6367–6378, 2019. [14] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf, 2008. [15] Geth client for building private blockchain networks, https://github.com/ethereum/go-ethereum, 2021. [16] V. Buterin, A next-generation smart contract and decentralized application platform, https://ethereum.org/ en/whitepaper/, 2021.

ISSUES IN THE EXISTING SYSTEM

In contrast with traditional cloud computing, several unique features bring quite different problems in fog computing scenarios. First, each fog node must authenticate the requestor and verify its right to access the fog resources. In traditional cloud computing, normally an access entrance is responsible for all authentication and authorization actions. This centralized access entrance performs a unified authentication and authorization procedure, which means that each subscriber usually uses a static password/key to access corresponding resources until they intend or are required to change the password/key. In addition, the price of a resource usually is static and unified no matter when the subscriber requests that resource unit. A similar phenomenon occurs in a telecom network: all resources for upper-layer applications are deployed behind an access gateway that is responsible for performing authentication/authorization/accounting functions. All the resources belong to the operator and a uniform access offer is provided.

III. PROPOSED SYSTEM

Fog resources are physically located on the network edge, which is beyond the traditional access gateway, e.g., broadband network gateway and mobile management entity entities. Basically, traffic must undergo a round trip through an access gateway, because the edge/fog node cannot perform access control.
chains,

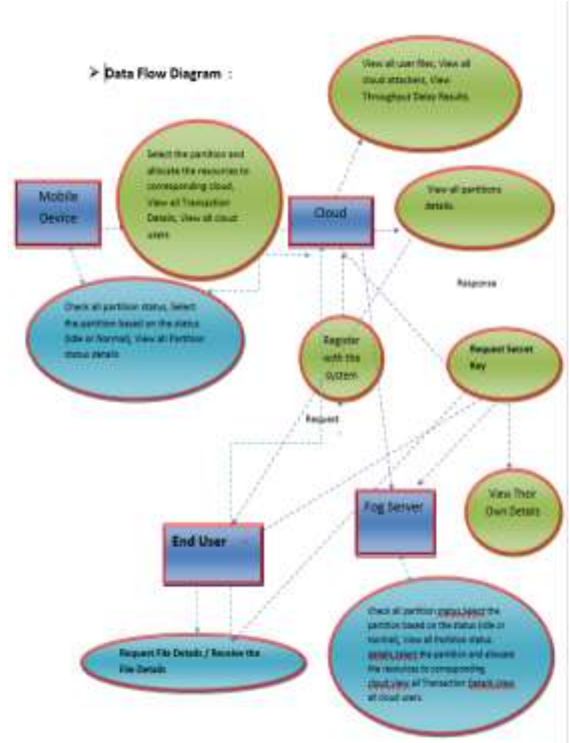
Data Flow Diagram :
View all user files, View all cloud attackers, View Throughput Delay Results
Mobile Device
Select the partition and allocate the resources to corresponding cloud, View all Transaction Details, View all cloud users
Cloud
View all partitions details
Response
Check all partition status, Select the partition based on the status (Idle or Normal), View all Partition status details
Register with the system
Request Secret Key
Request
Fog Server
View Their Own Details
End User
Request File Details / Receive the File Details
Check all partition status,Select the partition based on the status (idle or normal), view all Partition status details,Select the partition and allocate the resources to corresponding cloud,View all Transaction Details,View all cloud users.

Figure 1: Data flow diagram

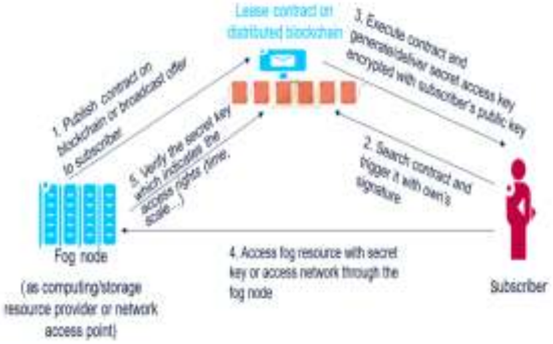
Lease contract on distributed blockchain
1. Publish contract on blockchain or broadcast offer to subscriber
3. Execute contract and generate/deliver secret access key encrypted with subscriber's public key
5. Verify the secret key which indicates the access rights (time, scale...)
2. Search contract and trigger it with own's signature
Fog node
(as computing/storage resource provider or network access point)
4. Access fog resource with secret key or access network through the fog node
Subscriber

Fig. 2 Working procedure of fog resource access.

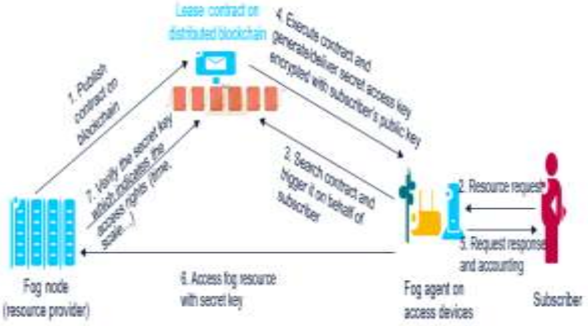
Lease contract on distributed blockchain
1. Publish contract on blockchain
4. Execute contract and generate/deliver secret access key encrypted with subscriber's public key
7. Verify the secret key which indicates the access rights (time, scale...)
2. Search contract and trigger it on behalf of subscriber
2. Resource request
3. Request response and accounting
Fog node
(resource provider)
6. Access fog resource with secret key
Fog agent on access devices
Subscriber

Fig. 3 Fog agent deployed on access devices.

The existing access authentication and requirements of geographically distributed fog nodes. For example, it cannot support peer-to-peer authentication between a requestor/subscriber and resource granting solutions in cloud computing are not adaptive to the unique a provider/fog node. In addition, it lacks the capability of secure access with traceable and irreversible record.

The smart contract concept is introduced to enable dynamic, automatic credential generation and delivery for independent fog resource access and permit. In our design, a smart contract is a series of software codes intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract on fog resource access and permit. A private blockchain was built up with several Go-Ethereum clients [15], which serve as miner nodes and transform the devices into an Ethereum node[16]. When a fog node is willing to share its resources, it can submit an independent lease contract on the Ethereum-based blockchain.

IV. RESULT

Fog computing plays a crucial role in satisfying the requirements of delay-sensitive applications, such as VR, AR, and industrial production lines. Fog nodes are also a type of network resource, but they have unique characteristics: geo-distributed, autonomous, and independent offerings. Traditional network control and resource granting methodologies usually assume that the relevant resources are placed behind a certain authentication/accounting point, which may not be suitable for fog computing cases. Furthermore, in some cases, fog nodes may belong to different owners or individuals who would sell the resources at a very different price and may dynamically adjust the resource offer. Addressing these new requirements, we propose a smart-contract-based fog resource access and granting mechanism to enable decentralized authentication and independent resource offering/granting for each fog node.

V. REFERENCE

[1]. T. M. Fernandez-Caram ´ es and P. Fraga-Lamas, A review ´ on the use of blockchain for the internet of things, IEEE Access, vol. 6, pp. 32979–33001, 2018.

[2]. O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, ControlChain: Blockchain as a central enabler for access control authorizations in the IoT, in Proc. 2017 IEEE Global Communications Conf., Singapore, 2017, pp. 1–6. [1] T. M. Fernandez-Caram ´ es and P. Fraga-Lamas, A review ´ on the use of blockchain for the internet of things, IEEE Access, vol.