International Journal of Advances in Computer Networks and Its Security– IJCNS
Copyright © Institute of Research Engineers and Doctors
Volume 8 : Issue 1- [ISSN : 2250-3757] - Publication Date: 10 May, 2019

A Scalable Distriubuted Ledger for Internet of Things based on Edge Computing

Rahim Rahmani, Yuhong Li, Theo Kanter

Abstract—Internet of Things (IoT) is becoming necessities of people's daily life and establishing itself as an essential part of future Internet. One of the challenges for using IoT is the security of data collected by trillions of IoT devices and used by millions of services. Distributed ledger technology (DLT) provides a distributed security method which can benefit IoT. Yet challenges are put forward when integrating DLT with IoT, such as scalability and heterogeneous capability of IoT devices. In this paper, we propose a mechanism for integrating DLT in IoT by using edge computing technology, taking the scalability and heterogeneous capability of IoT devices into consideration. IoT devices are clustered dynamically into groups based on various proximity context information. A cluster head is used to bridge the IoT devices with the blockchain network where smart contract is deployed. Through this way, the security of the IoT is improved and the scalability and latency are solved. We elaborate our mechanism and discuss issues that should be considered and implemented when using the proposed mechanism.

***Keywords*—Distributed Ledger, Blockchain, Internet of Things, Edge Computing, Security**

I. Introduction

Most IoT devices of today are simple devices such as sensors and actuators that are dependent on controllers in the cloud for analysis of recorded data, logical reasoning, and management. This may cause potential latency issues where the Internet connections of devices could become a bottleneck for performance and cause the devices to be sensitive to connectivity problems. There have been attempts to move some of the management closer to the devices with the help of gateways, so called edge computing [1][2]. These limitations mandate an alternative approach intelligently moving management to the edge devices. There is related work and research being carried out in edge computing and capillary networks, in-line with the 5G architecture [3][4].

Rahim Rahmani
Department of Computer and System Sciences, Stockholm University
Sweden

Yuhong Li
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications
China

Theo Kanter
Department of Computer and System Sciences, Stockholm University
Sweden

However, these approaches maintain control at the edge of managed network infrastructure. Control at the edge of the network disregards requirements of scenarios where edge devices need to achieve a task, and possible cooperate with flexibility that is possible only with local management and decision-making.

As a rapidly increasing and vast number of "things" will be connected to the Internet, in all sectors of society (people, places, sensors, homes, industry, government services, etc.). We need to build agile, intelligent and effective solutions in various application areas, such as Health, Transport and Automation. The ability of cloud infrastructure to orchestrate the fine-grained and agile control of "things" is limited. The reason is simply that the communication between a sensor or actuator and a management and controlling function in the cloud (typically hosted in a data center) has to pass a sensor network, access networks (edge devices) and core networks.

Distributed Ledger Technology (DLT) [5] is a key technology that manages and controls nodes in peer to peer applications which are mainly focused on payments and on record keeping. This allows IoT applications and edge computing systems to operate at any points and the IoT application will be able to incorporate heterogeneous context entities in heterogeneous domain, this heterogeneity mandates to look into interoperability reasoning approaches.

Compared with other approaches our approach bring the following advantages by designing DLT for IoT applications:

- A detailed model of a practically DLT with IoT application.
- A regulated mechanism for DLT proximity-context based which covers connection rules to physical proximity, social proximity and temporal proximity.
- DLT incorporating with IoT applications in heterogeneous domains operate as consensus based will makes protocols to be fault tolerant or resilient.

An edge gateway with DLT solutions designed specifically for autonomous cooperative decision-making in massively IoT devices are critical in order to realize an proximity enabled gateway as an edge computational intelligence. But nodes in DLT should include a copy of the DLT record (e.g blocks). That can be considerably large in size and will keep increasing over time and the majority of IoT gateways and or edge devices will not be able to store DLT information due to their constrained. Due to those fact which make a limitation of the DLT in IoT scenarios with limited scalability.

In this paper, we discuss a mechanism for realizing distributed ledger in the network edge for IoT devices to solve

the problems of scalability of IoT network and the heterogeneous capability of IoT devices. IoT devices are clustered dynamically into different groups based on various proximity context information, including physical proximity, social proximity and temporal proximity. A cluster head at the edge layer is used to act as an agent to bridge the IoT edges (e.g., an IoT gateway) and the IoT devices connected with the edges in the cluster to the blockchain network in the fog layer. Smart contract is deployed in the fog layer where powerful devices exist (e.g., a 5G base station or an Internet router). The rest of the paper is organized as follows. In section II, we analyze the related work, focusing on methods combining DLT with IoT that deal with problems of scalability of IoT network and heterogeneous capability of IoT devices. In section III, we elaborate our mechanism and discuss issues that should be considered when using the proposed mechanism. We conclude the paper in section IV.

II. Related Work

A distributed ledger is a database that is shared and synchronized across network nodes consensually. Participants at each node of the network can access the recordings shared across the nodes in the network and can own an identical copy of them. By making the recordings public witness, no single participant can alter or reverse the data in the record, unless the change is agreed by all participants in the network in a subsequent transaction. Through this way, DLT provides certain level of security guarantees to the data recorded in the ledger. Therefore, DLT is being used in different IoT areas, such as intelligent transportation [6], [7], [8], Industry 4.0 [9], healthcare [10][11] smart grid[12][13] and supply chain management [14] etc. For example, to preserve the privacy of patients and maintain the, [11] introduced an attribute based signature scheme, using the blockchain technology which can resist to N-1 corrupted authorities collusion attacks, and is unforgeable in suffering a selective predicate attack. Work in [8] proposed a blockchain ecosystem model for electric vehicle and charging pile management, which uses elliptic curve cryptography to calculate hash functions of electric vehicles and charging piles. In the following sections, we concentrate on analyzing work for solving the scalability issue raised by integrating DLT with IoT and work regarding cloud and fog computing which are closely related with the mechanism proposed in the paper.

A. *Scalability for DLT Integrating with IoT*

Among these work, [15] proposed a distributed IoT network architecture called DistBlockNet. DistBlockNet realized scalability and flexibility with the help of blockchain by not using a central controller. In DistBlockNet, all controllers in the IoT network are interconnected in a distributed blockchain network, in this way each IoT forwarding device in the network can easily and efficiently communicate. The architecture involves two type of nodes - the controller/verification node, which maintains the updated flow rules table information; and the request/response node, which updates its flow rules table in a blockchain network. With the help of blockchain, flow rule table can be verified, validated and the latest flow rule table can be downloaded for IoT forwarding devices. Compared with DistBlockNet, the IoT devices in our mechanism can join the blockchain network depending on their capability. In addition, various context information of the IoT devices are also considered during the selection of the head of the clusters.

Work in [16] proposed an architecture for scalable access management for IoT using blockchain technology. The architecture involves six components with different functions, namely wireless sensor networks, managers, agent node, smart contract, blockchain network and management hubs. Management hubs are used to connect blockchain network and sets of IoT devices (i.e., wireless sensor networks), which do not have capabilities to run blockchain technology. The smart contract defines all the operations allowed in the access management system and are triggered by the blockchain transactions. The agent node, which is a specific blockchain node, is used to deploy the only smart contract in the system. Managers are entities responsible for managing the access control permissions of a set of IoT devices, which do not store the blockchain information or verify the blockchain's transactions. With the help of management hubs, different set of IoT devices in the wireless sensor networks can be managed, considering the scalability and capability of IoT devices.

B. *Cloud/Fog/Edge Computing for DLT Integrating with IoT*

Cloud and fog computing have been widely used in IoT. Billions of IoT devices upload their data to the cloud, fog or edge through global or local Internet, and the data are processed and used by using virtualization technology. In the context of integrating DLT with IoT, several work have also been done [17][18][19]. [17] proposed an intelligent resource management method for datacenters in the cloud based on the blockchain technology, in order to reduce the total cost of energy. Users use their private keys to sign and broadcast a transaction, which will be verified by the neighboring users. The block is discarded when it does not pass verification. [18] suggested a blockchain-based data sharing system called MeDShare, for cloud service providers. The suggested system includes four layers namely user layer, data query layer, data structuring and provenance layer, and existing database infrastructure layer. [19] proposed a distributed cloud architecture using three emerging technologies, namely, software-defined networking (SDN), fog computing, and blockchain. The SDN controllers of the fog node are used to provide programming interfaces to network management operators. The blockchain technique is used to provide scalable, reliable, and high-availability services. [20] proposed a fair payment scheme for outsourcing computations of fog devices. This scheme considers the following security metrics of integrity, fairness and accountability based on bitcoin.

Compared with these work, our work use the layered cloud, fog and edge architecture to introduce DLT in IoT, solving the scalability and capability of IoT problems. We do not design DLT in order for cloud and fog computing to provide better services.

III. Distributed Ledger for Clustered IoT Devices based on Edge Computing

For the reason of scalability, IoT devices in a cloud-based environment are normally supported in a hierarchical structure, consisting of different layers of equipment performing the computation functions. In our work, we consider two layers of computations. Fog layer is the high layer distributed computations and the edge layer is the low layer distributed computations. The IoT devices are connected to the edge layer equipment.

Fig. 1 illustrates an example of a layered distributed computation architecture for IoT devices supporting DLT. To support DLT for IoT applications in a scalable way, the following issues should be addressed:

- Edge computing with distributed ledger.
- Distributed ledger for clustered IoT devices.

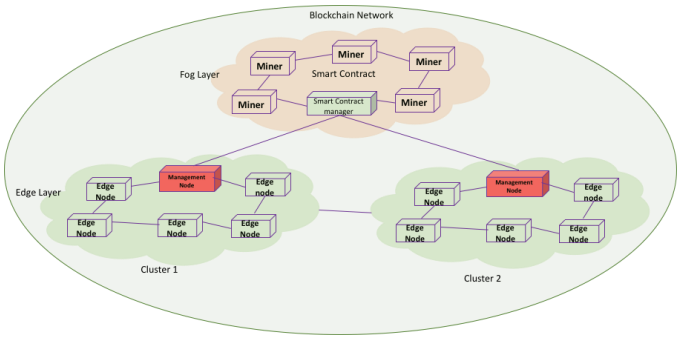

Figure 1. A layered distributed computation architecture supporting DLT for IoT devices

Here, distributed ledger can serve as distributed control in fog and edge nodes, being able to negotiate distributed coordination problems. Sometimes it is assumed that certain global information is available at each individual nodes. This assumption disobeys the virtue of distributed coordination. As an alternative, distributed control methodologies have to be used.

A. *Edge Computing with Distributed Ledger*

As shown in Fig. 1, DLT-Based IoT-Edge nodes can make decisions based on context at two levels in response to a) the unavailability of trusted paths and b) application level events and context changes as well as proximity-context based. IoT sensors are limited in hardware and software resources and only allow the constrained connectivity in IoT applications. Those devices do not belong either the edge or fog layer than the devices will not be uniquely identified globally. Only nodes in edge layer and fog layer can be uniquely identified globally in blockchain network. The edge layer is a device management of IoT devices networks that allows decision making and clustering for proximity in context-based applications.

The system architecture requires interworking between the management node in edge layer with smart contract manger node in fog layer, which in essence, is blockchain network. In support of delegation from a cloud-based blockchain network. We designed a new interworking function which is able to manage a set of IoT devices as a cluster for proximity-context based in edge layer. Smart contract manager in fog layer is responsible for smart contract updating based of the policy changes. To achieve consensus in the DLT-Based IoT-Edge nodes uses Directed Acyclic Graph (DAG) [21], DAGs typically operate as swarm of consensus algorithm which is able to interpret instructions from an edge platform and return the results after delegating it to the swarm of IoT edge nodes.

B. *Distributed Ledger for Clustered IoT Devices*

To realize the above architecture, following things must be considered scalability. In order to address scalability and different from existing approaches which using sharding [22] to improve scalability, sharding splits blockchain network in partitions by that way no all nodes need to process all incoming transaction. We propose Logical clustering in the DLT-Based IoT-Edge as shown in figures 1 and 2. Our approach limit transactions forwarding and do not allow any inconsistency in the smart contract changes. As mentioned in previous section set of IoT devices will be mange as a cluster based on context similarity.

Context in sensors clustering has been discussed before, but in all cases definition of context is specific. Moreover, their solution is limited to neighboring sensors. To the best of our knowledge, the concept of logical clustering of sensors based on context is new and [23] was the first attempt of the proposed concept. This new concept will allow resources (data, services) to be shared among different physically distributed sensors. Sensors can share resources through distributed collaboration. Once the clustering is done then each cluster is identified through a context-ID which is defined based on context similarity and published on the internet.

In the system as shown in Fig. 1 and Fig. 2 certain management nodes would process transactions only for certain logical clusters than allowing the throughput of transactions processed in total across all nodes in the fog layer to be much higher than having a single cluster in the edge layer.

To uniformly clustering a set of IoT devices into several clusters with condition that each cluster follows relational proximity which elevates the problem of IoT device organization to multi-dimensional which driving such an

affinity or proximity value [24] could be realized as an extension of context-based proximity approaches by using multi-dimensional metrics as shown in Fig. 2.

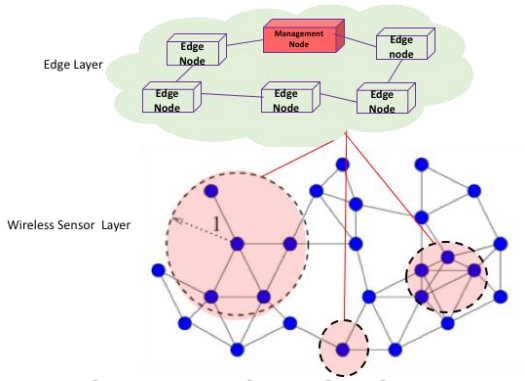

Figure 2. Edge Device with DLT based on proximity-Context

C. *Security of the Distributed Ledger*

For the security of the DLT-Based IoT-Edge gateway environment, first we identify the main possible threads and second provide the solutions overview. Attack targeting the DLT-Based IoT-Edge gateway will apply to smart contract manger node in the fog layer through malicious nodes can modify messages or drop messages than starting to send false messages to nodes in the blockchain network. The well-known eclipse attack, targeting the management node in the edge layer and try to control the node access to information and thereafter monopolizes all of the nodes incoming and outgoing connection [25] by that way isolating the node from the rest of peer in the blockchain network. Th key ideas for solution overview is to make system automatically parallelize the available nodes and dividing them into clusters. Each cluster run a byzantine consensus protocol internally. There will be a consensus cluster which is responsible for shared selected value and other cryptographic digests in all network.

D. *A Use Case*

To support efficient DLT-Based IoT-Edge gateways in a scenario described in Fig. 3 in real application to identify the existing situation by managing and control data about 3 main areas depending of their functionality, the areas are as follows: Surveillance Infrastructure, Communication Path in incident Areas and Public Alerting.

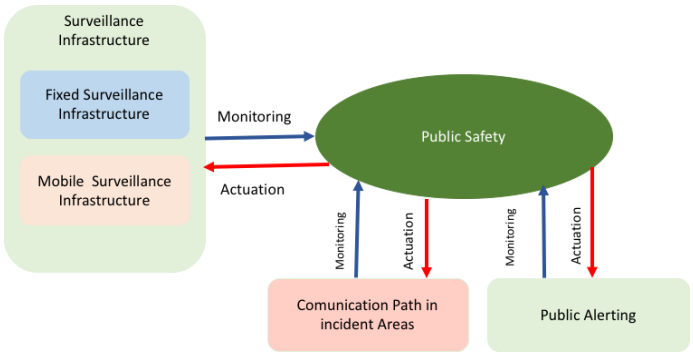

Figure 3. Public Safety and a view of the operation scenario

In response to the scalability improvement of the DLT-Based IoT-Edge gateways than we developed a proof of concept by using in the suggested framework as shown in figure 3. The frame work focuses on the ability of applications and services to make decision about service delivery based on secured and trusted path close to the user from, e.g., sensors and user profiles stored on the edge layer. Control and decision making in services that deliver operations of the smart Contract to the end devices. The main technologies and services, with the integration in public safety framework of those 3 areas contributions, can make our urban environment become sorts of large organisms, in which a variety of innovative tasks and services can support and increasing quality of information sharing. The platform can act and put at play in a globally collaborative way. The system by sensing the needs of a city and of entities, by perceiving who's around that can help by dynamically establishing collaborative activities seamlessly involving devices. The main specificity of the platform is how that is able to jointly overcome the trusted and secure obstacles and challenges that affect those three areas.

IV. Conclusions

In this paper, we discussed a method for supporting DLT for IoT devices in a layered distributed computation environment. The scalability and heterogeneity of IoT devices are considered. Security issues related with distributed ledger are analyzed and a use case of the proposed method is explained.

Our future work is to realize the proposed method and evaluate it by implementing the use cases.

References

[1] OpenFog Consortium, https://www.openfogconsortium.org

[2] ETSI establishes the foundations of Mobile Edge Computing http://the-mobile-network.com/2016/04/etsi-establishes-the-foundations-of-mobile-edge-computing/

[3] Edge computing in IoT; Ericsson Research Blog Konstantinos Vandikas Jul 7, 2015 Internet of Things (about actors) https://www.ericsson.com/research-blog/internet-of-things/edge-computing-in-iot/

[4] Novo O. et al, "Capillary networks - bridging the cellular and IoT worlds", IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015

[5] Consocenti, M. Vetro, A. and De Martin, J.C., " Blockchain for the Internet of Things: A Systematic Litteratur review", IEEE/ACS 13th International Conference on Computer Systems and Applications, 2016.

[6] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, dec 2017..

[7] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," IEEE Trans. Intell. Transp. Syst., pp. 1–17, 2018.

[8] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," IEEE Access, vol. 6, pp. 13 565–13 574, 2018.

[9] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," IEEE Trans. Ind. Informatics, pp. 1–1, 2017.

[10] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" IEEE Cloud Comput., vol. 5, no. 1, pp. 31–37, Jan. 2018.

[11] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," IEEE Access, vol. 6, pp. 11 676–11 686, 2018.

[12] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," IEEE Access, vol. 6, pp. 9917–9925, 2018.

[13] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks," IEEE Trans. Smart Grid, pp. 1–1, 2018.

[14] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in Proc. IEEE 13th Int. Conf. on Service Systems and Service Management (ICSSSM), June 2016.

[15] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," IEEE Commun. Mag., vol. 55, no. 9, pp. 78–85, 2017.

[16] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT", IEEE Internet of Things Journal, Vol. 5, no.2, April 2018.

[17] C. Xu, K. Wang, and M. Guo, "Intelligent Resource Management in Blockchain-Based Cloud Datacenters," IEEE Cloud Comput., vol. 4, no. 6, pp. 50–59, nov 2017.

[18] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.

[19] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," IEEE Access, vol. 6, pp. 115–124, 2018.

[20] H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, "Bitcoin-based fair payments for outsourcing computations of fog devices," Futur. Gener. Comput. Syst., vol. 78, pp. 850–858, jan 2018.

[21] C. Lemahieu, " RaiBlocks: A feeless Distributed Cryptocurrency Network, " pp. 1-8, 2008.

[22] L. Luu, V. Narayanan, C. Zheng,"A Secure Sharding Protocol For Open Blockchains ", CCS '16 Proceedings of the 2016 ACM SIGSAC, Pages 17-30, October 24 - 28, 2016

[23] R. Rahmani, H. Rahman, and T. Kanter: "Context-Based Logical Clustering of Flow-Sensors Exploiting HyperFlow and Hierarchical DHTs, In Proceeding(s) of 4th International Conference on Next Generation Information Technology, 2013 ICNIT, June 2013

[24] J. Walters, T. Kanter and R. Rahmani, "A Relational Context Proximity Query Language", Mobile Networks and Management conference: Springer, 2015, no. 1, pp. 277-289.

[25] Y.Marcus, E. Heilman and S. Goldberg "Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network"Published 2018 in IACR Cryptology ePrint Archive.

About Author (s):

Image

[Type a quote from the document or the summary of an interesting point. You can position the text box anywhere in the document. Use the Drawing Tools tab to change the formatting of the pull quote text box.]