Decentralized Secure Fog Computing in Cloud-Fog-IoT Infrastructure Using Blockchain

Bhabendu Kumar Mohanta
IIIT Bhubaneswar
Odisha, India 751003
C116004@iiit-bh.ac.in

Debasish Jena
IIIT Bhubaneswar
Odisha, India 751003
debasish@iiit-bh.ac.in

Soumyashree S Panda
IIIT Bhubaneswar
Odisha, India 751003
C117011@iiit-bh.ac.in

Debasis Gountia
CET Bhubaneswar
Odisha, India 751003
dgountia@gmail.com

***Abstract*—Fog computing is decentralized scalable architecture where the fog nodes can join and leave the network arbitrary way. The IoT devices connected to the fog network can also have the connectivity issue. As all the fog nodes and IoT devices are connected in a distributed way it is hard to build a secure infrastructure in the absence of a trusted central server. First, as there is no trusted leader present in the fog architecture, it is impossible to maintain network stability, services and operations in the presences of malicious fog nodes. Secondly, existing security protocols are inefficient in low-end fog computing and IoT devices. Thirdly, how to check the correctness of the computation results obtained from multiple fog nodes in a distributed environment as all fog nodes are not trusted. Security and privacy of the fog computing are explained in this paper. The paper proposed Blockchain technology derived from bitcoin cryptocurrency can be used to provides a distributed secure infrastructure between fog node and IoT devices for secure communication. Blockchain can be used to store the log file as a transaction in an open ledger by recording all the transaction between Cloud, Fog and IoT devices. The recorded block can also be used to a validated transaction so malicious fog nodes can be identified by the honest fog node. Lastly, we have shown that blockchain technology can also be used for authentication of the fog nodes and IoT devices using permissioned architecture.**

***Index Terms*—Decentralized; Fog Computing; Blockchain; Security; Privacy; Consensus Algorithm**

I. Introduction

In the last decade Internet of Things (IoT) technology which is inter networking of various things/objects and connected through mostly wireless allows these objects to exchange information. There are large numbers of low-end IoT devices having less memory space and processing power is available. The interconnection of these devices makes possible to build IoT application. IoT has many applications like smart home automation, smart city, smart transportation, supply chain management, product tracking, environment monitoring, patient monitoring, energy monitoring. The IoT has grown rapidly producing a huge amount of data generation which requires large storage space, immense computing resources, and communication bandwidth [1]. Some of the IoT application like Healthcare system needs a fast response in real time to make the monitoring of the patient efficient way, so in this case processing need to be done in locally or at the user end. The computing paradigms gradually are gone change from distributed, parallel, grid to cloud computing. Cloud computing has three key service model: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Because of these three services cloud computing is widely used. However, it has some of the issues like connectivity with end devices, latency, location, bandwidth [2]. Fog computing has the ability to tackle some of the cloud computing problems. With the evolution of Fog computing technology which is proposed by Cisco, it is possible to have processed locally or at the user end. Fog computing extends the cloud computing to the edge of the network. Some promising properties of Fog computing are [3]:

- Access through wireless.
- Supports mobility of end-user.
- Supports heterogeneity.
- Supports a large number of nodes in the processing.
- Supports low latency and localization.
- Decentralization.

The integration of Cloud-Fog-IoT would solve the latency, bandwidth issue. So in IoT application processing can be done at end devices and the corresponding action can be triggered which makes application more efficient and valuable. During processing at the user end through Fog computing it may happen that some of the Fog nodes behave malicious. In a collaborative decision making process majority of node must agree with the decision. Here come the Blockchain technology if it apply in Fog computing case as it is distributed architecture computation could be done in secure way. Any malicious Node can be identify and that can be ignore. All the transactions are verified and validated before recorded in the block wise.

A. Related Work

The Fog computing has lots of potential like storage and processing at the edge of the network. In IoT application use of Fog, computing solved the latency and bandwidth issue of IoT-Cloud environment. The Fog computing exists some security issue. In the paper [4] and [5] , authors have come up with machine learning technique and physical layer security solution to address the impersonation attack. As Fog network consists of multiple nodes, in the collaborative decision-making process all the nodes must be trusted to the network. In [6], authors use the two-stage Markov model to identify the malicious node. Similarity in papers [7], [8] and [9] address

the security issue present in Fog computing. As Fog computing is highly decentralized security issue need to be addressed.In this [10] paper, Blockchain is used to protect the privacy and manage the user data through authentication.In paper [11] and [12], authors described the internet of Things privacy and data traceability issue using Blockchain.

B. Contribution

The security issue explained in related work can be addressed by Blockchain Technology. In this paper, integrated of Blockchain technology with the Fog computing are explained in details. Like Authentication problem of the Fog node can be solved using the public and private key concept of Blockchain. Similarly, the trust of the Fog network can be maintained using the digital signature of the Blockchain concept. Finally, the collaborative decision can be taken among Fog nodes using the mining process of Blockchain Technology.

II. Architecture of Cloud-Fog-IoT environment

As shown in Fig.1 three-tier architecture consists of Cloud layer, Fog layer, and IoT layer. The Fog layer acts as a middle layer between the cloud and IoT layer. The communication among their layer takes place using both wire and wireless way. For wireless communication ZigBee, Bluetooth, LTE, NFC, IEEE 802.11 a/b/c/g/n, satellite links are used. For wired communication, Ethernet and optical cable are used. In the IoT, layer consists of different types of IoT devices such as temperature sensor, gas sensor, security Camera, smartwatch, fitness tracker, smart vehicle, smartphones, health monitoring sensors and so on. Some of the equipment is fixed type deploy in an environment to sense or monitor the environment in real time and some of the equipment are movable or wearable devices which are movable along the object moment and record the corresponding information. These devices are resource constrained devices they only sense the environment and send the information to the upper layer for processing and storage. The Fog layer consists of devices which have some computational power as well as some storage space. Apart from the communication of data from a lower layer to the upper layer it also reduces the overhead of the IoT devices. In the Fog layer, Fog nodes communicate among themselves and take a collaborative decision in real time and provide various services without the involvement of the cloud layer. The cloud layer has huge storage space and computing power it can be accessed anytime from anywhere if connect with internet. The Fog node sends all the information to the cloud, after receiving the data cloud can perform different operation on that data to make better business services.

III. Key Issues Associated with Cloud-Fog-IoT infrastructure

Cloud-Fog-IoT infrastructure has several issues exists in each associated system. Cloud computing has a large storage and processing power. It also provides different services like IaaS, PaaS, and SaaS. When cloud is integrated with IoT it has issue arises like latency,privacy protection [13],data traffic

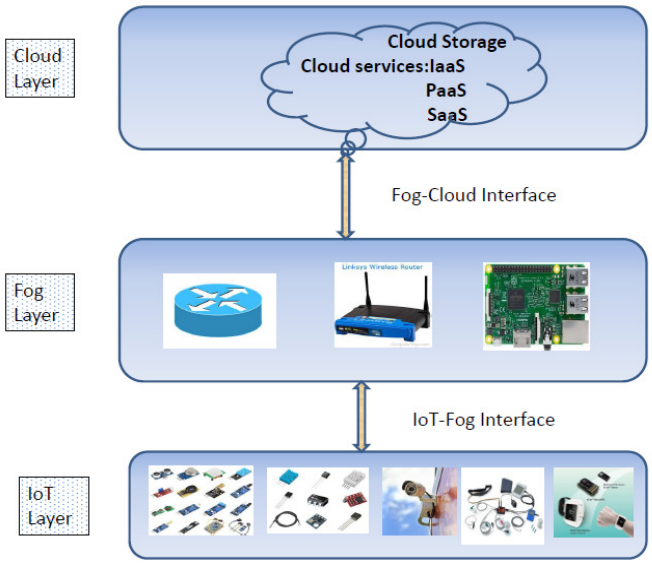

Fig. 1. Architecture of Cloud-Fog-IoT environment

[14], data security [15] and bandwidth.If Fog computing is merged with cloud and IoT system then latency and bandwidth issue can be solved.in paper [16] and [17], authors described the resource management, application offloading, Standardization, Heterogeneity, energy consumption, and storage issue of Fog computing. User privacy, data security, and network connectivity issue are explained in paper [18]. the concept of storage and processing can be performed in a network edge using fog computing are discussed in paper [19]. Security point of view still lots of issues need to be addressed to make an application reliable and efficient. The security issue is authentication, heterogeneity, Quality of service, scalability, Mobility can be addressed by Blockchain Technology.

IV. Security Privacy issue and computation problem in Fog Environment

Cloud computing has capability to compute and store huge volume of data. But its increase the latency and take time to respond to the end devices. As IoT devices generate sensitive and time frame data that require to be computed in faster way to increase the efficiency of the application. If the collected data are temporary store, process and analyzed on local fog device then application become efficient as data are process faster with a time frame. However fog computing has its own security and privacy issue [20] [21].

A. Security and Privacy threads in Fog Computing

As shown in table 1 fog computing has different security issue. Fog node may behave as a malicious node and try to mislead others node. Malicious node may also send fake information to the network to consume lots of storage and bandwidth. All the security issues described in the table 1 are about malicious behavior and about changing the collected data from IoT environment. The solution for the malicious fog

TABLE I
SECURITY AND PRIVACY THREADS IN FOG COMPUTING

Issue	Threats
Security	Forgery
	Tampering
	Spam
	Sybil
	Jamming
	Eavesdropping
	Denial-of-Service
	Collusion
	Man-in the-middle
	Impersonation
Privacy	Identity privacy
	Data privacy
	Usage privacy
	Location privacy

none detection or ignoring the malicious node in computing processing can be possible using Blockchain technique. The detail solution approach is explained in Section IV.

In IoT application like smart home, smart healthcare system user privacy is a major concern. Let consider in case of Healthcare system patient personal information need be preserved otherwise leakage of information may lead to user privacy is lost. Similarly in case of smart home system if any attacker get access to the IoT device deployed in the smart home then attacker may get the living habits of the home system. Similarly in case of smart transportation if the sensors deploy in the vehicle are accessed by the attacker then user location privacy can be known to the attacker.

The IoT devices are vulnerable to the fog computing environment in terms of security and privacy issue.

B. Computation problem:

The IoT application requires the received sensors data to be processed and computed in real time. So fog computing provides the facility to process and compute the sense information in collaborative way. But as fog node are compromised by the attackers, secure computation is challenging. Many algorithm are already proposed for the fog computation like [22] and [23] are work on how resource sharing is done among fog nodes. Authors in [24], [25] and [26] explained the task scheduling in collaborative fog computing environment. Although some algorithms are already proposed by different authors till secure computation in presence of malicious fog nodes are not explained. There are some decentralized computation for fog nodes are explained below:

1) Computation verifiable: In fog computing environment after receiving the information from the IoT environment in the computation process must give the correct results. Whatever the computation function executed by all the fog nodes, it should be verifiable by the network in distributed way. As all the fog nodes may not be trusted node so computation process must be verified by the network. This can be possible by the Blockchain technology. In Blockchain technology, each transaction is passed through a validation process before broadcast to all the nodes in a network. If any fog node behaves malicious for computation or broadcast any wrong transaction in the network that can be verified by the other fog node in the network by using the Blockchain technique.

2) Aided computation and big data analysis: As IoT devices are low end devices so computation need to be done either in cloud or fog environment. But in case of IoT application doing computation in the cloud server takes lots of latency and bandwidth. As the number of IoT devices are huge and sense mostly critical information from the environment computation need to be done at fog end. The critical or sensitive data need to be analyzed in the faster way and trigger the corresponding events which make the IoT application useful in real time.

V. PROPOSED SOLUTION USING BLOCKCHAIN

Block chain technology is decentralized computing platform where information are shared among all the nodes in digital ledger openly. Blockchain can be used in a system where the nodes do not trust each other, but they try to make decision in cooperative, collaborate, coordinate way. Being the tamper proof and immutable properties, Blockchain holds the security and privacy of the nodes as well as all the transactions are tamper proof.

A. Design secure fog architecture based on the Blockchain concept

The secured architecture of Fog computing is shown in Fig. 2. The architecture consists of 3 layer, end layer is the IoT which consists of all the sensors and IoT deployed in different applications. The middle layer is the Fog layer where fog nodes collect information from different sensors. Fog nodes sense the environment and then collectively take decision as per the application. For example in a automated smart IoT conference hall each fog node sense the room temperature from temperature sensors (DHT22) and value of different gas sensors. Once data are sensed from the environment fog node try to make a collective decision about where AC will be on or off. That decision is taken mutually among the fog node in a distributed way maintaining privacy of each fog node. As shown in Fig. 2, fog nodes are connected in decentralized way. Fog nodes are authenticated to the trusted server and through that server all the data communication to the cloud server. In case of IoT application sense data are processed and analyzed in the fog layer itself and final data are pushed to the cloud layer.

B. Secure distributed computation : Distributed consensus

Blockchain technology emerge from bitcoin cryptocurrency which is mainly permission less environment. In the Permission less environment the consensus algorithm apply are:

- Proof of Work (POW)
- Proof of Stake (PoS)
- Proof of Burn (PoB)
- Proof of Elapsed Time (PoET)

Blockchain Permissioned model based application consensus algorithm are :

- Byzantine Fault Tolerance (BFT)

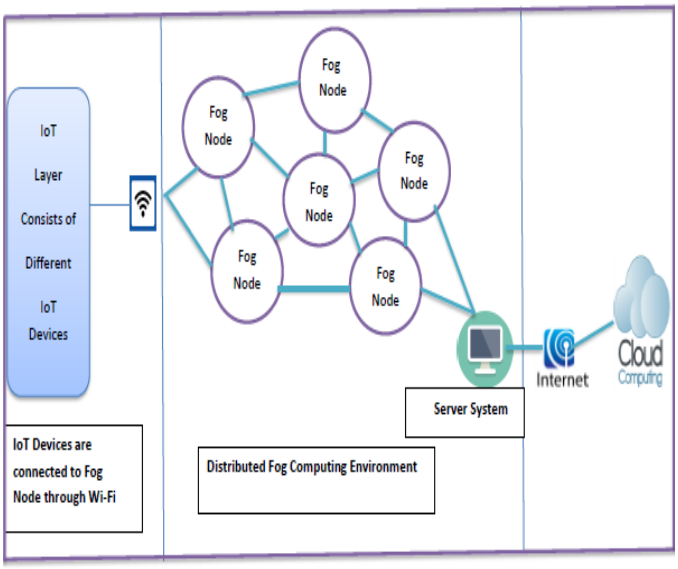

Fig. 2. Distributed Computation architecture based on Blockchain

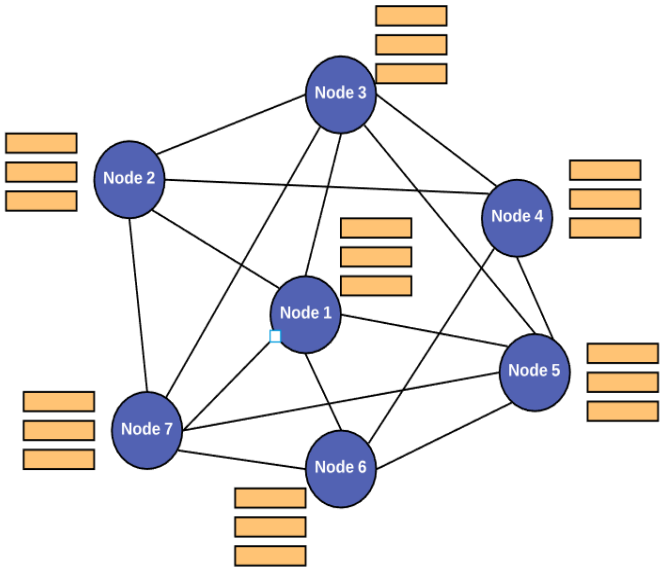

Fig. 3. Decentralized Blockchain System each node having Blockchain database

- Practical Byzantine Fault Tolerance (PBFT)
- PAXOS
- RAFT

In a permissioned model Blockchain architecture nodes are authenticated a priory. Here fog nodes are authenticated through the trusted server. Fog nodes are authenticated to the environment but they are not trusted to each others. So meeting consensus in decentralized environment is challenging.
To meet the consensus algorithm some of the challenges are Crash fault, Network faults and malicious behavior in nodes. In the Fog computing, to take a decision collectively need to be executed a function that is the consensus algorithm. If the most of the nodes agree on the consensus algorithm then that decision is broadcast to all the nodes and store as a transaction. Once that transaction is recorded in the Blockchain system it never be changed. As shown in Fig. 3, each fog node has a digital ledger record or blockchain. A block consists of some transactions. A consensus algorithm must possess following properties:

- Termination: At the end of the algorithm, correct node must agree upon some value and terminate the process.
- Integrity: Each correct node must agree at most one value.
- Validity: All the nodes proposes the same value and they decide on that value.
- Agreement: Every node must agree on same decision.

C. Blockchain base framework for authentication of fog node and IoT nodes

In Permissioned based model, each node is initially authenticated to the network. Normally authentication is done using public key cryptosystem. In a Blockchain model each transaction is signed by the node using digital signature so that identity is maintained. No one can clam the false transaction or no one can deny transaction as each transaction is broadcast to the network after combine with the sender digital signature. Identity of the sender can be validated using the public key cryptosystem. In this proposed system model all the fog nodes are authenticated to the network through a trusted server.

VI. Experimental setup and comparison algorithm

For this work different type of sensors like DHT22, MQ6, MQ9, MQ3 and web camera are used to monitor the smart environment. For build up the IoT devices and to read the value python programming language is used. RASPBERRY PI 3 MODEL B+ used as a Fog node. These fog nodes can access the different sensors deploy in a smart room environment. RASPBERRY PI module have specification like Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC @1.4GHz, 1GB LPDDR2 SDRAM 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE. One high end device having fully tamper proof having large storage and high processing power used to authenticate all the fog node. This high end system is also connected with the cloud through internet.

Blockchain Implementation part smart contract [27] play a vital rule to any application to be developed.Smart contract are self executable program.As shown in Fig. 4 smart contracts are written as per the application service requirement.

To developed and deployed the smart contract Etherum platform is used.In the Fig.5 shown the set up of the Etherum Blockchain environment.

Previous computation works are mostly on different security algorithms and some are on resource sharing and task scheduling. This paper explains that if Blockchain consensus

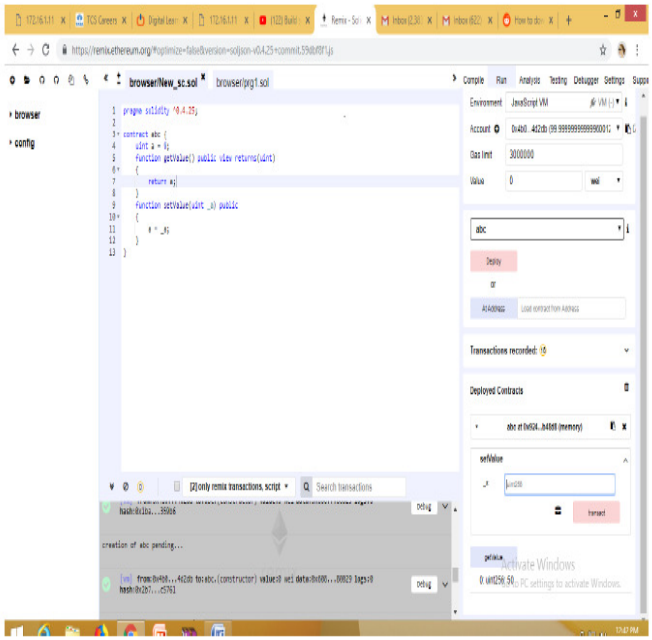

Fig. 4. Environment for smart contract for Decentralized system

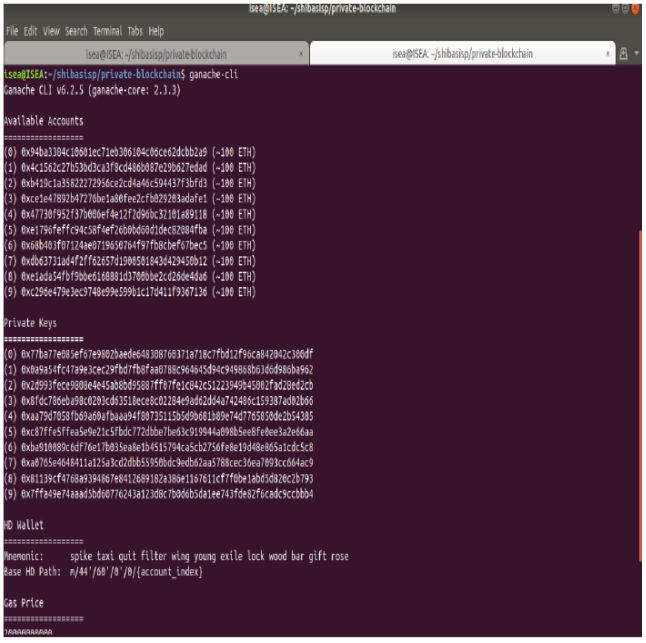

Fig. 5. Environment for Ethereum Blockchain Decentralized system

algorithm used for fog computation then security and privacy issues explained in Section III can be addressed.

VII. Conclusion and Future work

In IoT-Fog-Cloud architecture, computation mostly done on fog computing layer. But fog computing has security and privacy issue. So to performed computation is a challenging task. Fog computing architecture is decentralized architecture. The IoT devices connected to the fog network can also have the connectivity issue. As all the fog nodes and IoT devices are connected in a distributed way it is hard to build a secure infrastructure in the absence of a trusted central server. Paper is initially given the architecture of diagram of IoT-Fog-Cloud. As this paper looks to IoT applications as use for implementation. The secure and correct computation of the IoT application is real challenges. In this paper it is explained that Blockchain technology can be effective solution to carry put computation in fog computing environment. Different consensus algorithm are discussed in section IV which are use in a permissioned model of Blockchain technology. In the future work, authors would like to scalable the fog computing environment using the Hyper ledger fabric.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of internet services and applications*, vol. 1, no. 1, pp. 7–18, 2010.

[3] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. ACM, 2012, pp. 13–16.

[4] S. Tu, M. Waqas, S. U. Rehman, M. Aamir, O. U. Rehman, Z. Jianbiao, and C.-C. Chang, "Security in fog computing: A novel technique to tackle an impersonation attack," *IEEE Access*, vol. 6, pp. 74 993–75 001, 2018.

[5] M. Moh and R. Raju, "Machine learning techniques for security of internet of things (iot) and fog computing systems," in *2018 International Conference on High Performance Computing & Simulation (HPCS)*. IEEE, 2018, pp. 709–715.

[6] A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments," *Computers & Security*, vol. 74, pp. 340–354, 2018.

[7] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," *Future Generation Computer Systems*, vol. 88, pp. 16–27, 2018.

[8] X. Liu, Y. Yang, K.-K. R. Choo, and H. Wang, "Security and privacy challenges for internet-of-things and fog computing," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[9] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[10] S. H. Lee and C. S. Yang, "Fingernail analysis management system using microscopy sensor and blockchain technology," *International Journal of Distributed Sensor Networks*, vol. 14, no. 3, p. 1550147718767044, 2018.

[11] Q. He, Y. Xu, Z. Liu, J. He, Y. Sun, and R. Zhang, "A privacy-preserving internet of things device management scheme based on blockchain," *International Journal of Distributed Sensor Networks*, vol. 14, no. 11, p. 1550147718808750, 2018.

[12] R. Qiao, S. Zhu, Q. Wang, and J. Qin, "Optimization of dynamic data traceability mechanism in internet of things based on consortium blockchain," *International Journal of Distributed Sensor Networks*, vol. 14, no. 12, p. 1550147718819072, 2018.

[13] G. Zhang, Y. Yang, X. Zhang, C. Liu, and J. Chen, "Key research issues for privacy protection and preservation in cloud computing," in *Cloud and Green Computing (CGC), 2012 Second International Conference on*. IEEE, 2012, pp. 47–54.

[14] M. Peng, Y. Sun, X. Li, Z. Mao, and C. Wang, "Recent advances in cloud radio access networks: System architectures, key techniques, and open issues." *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 2282–2308, 2016.

[15] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data security and privacy in cloud computing," *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, p. 190903, 2014.

[16] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Communications Surveys & Tutorials*, 2018.

[17] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 416–464, 2017.

[18] R. K. Naha, S. Garg, D. Georgakopoulos, P. P. Jayaraman, L. Gao, Y. Xiang, and R. Ranjan, "Fog computing: survey of trends, architectures, requirements, and research directions," *IEEE access*, vol. 6, pp. 47 980–48 009, 2018.

[19] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K.-K. R. Choo, and M. Dlodlo, "From cloud to fog computing: A review and a conceptual live vm migration framework," *IEEE Access*, vol. 5, pp. 8284–8300, 2017.

[20] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2017.

[21] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[22] S. F. Abedin, M. G. R. Alam, N. H. Tran, and C. S. Hong, "A fog based system model for cooperative iot node pairing using matching theory," in *Network Operations and Management Symposium (APNOMS), 2015 17th Asia-Pacific*. IEEE, 2015, pp. 309–314.

[23] J. Oueis, E. C. Strinati, S. Sardellitti, and S. Barbarossa, "Small cell clustering for efficient distributed fog computing: A multi-user case," in *Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd*. IEEE, 2015, pp. 1–5.

[24] K. Intharawijitr, K. Iida, and H. Koga, "Analysis of fog model considering computing and communication latency in 5g cellular networks," in *Pervasive Computing and Communication Workshops (PerCom Workshops), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1–4.

[25] D. Zeng, L. Gu, S. Guo, Z. Cheng, and S. Yu, "Joint optimization of task scheduling and image placement in fog computing supported software-defined embedded system," *IEEE Transactions on Computers*, vol. 65, no. 12, pp. 3702–3712, 2016.

[26] M. Aazam and E.-N. Huh, "Fog computing micro datacenter based dynamic resource estimation and pricing model for iot," in *Advanced Information Networking and Applications (AINA), 2015 IEEE 29th International Conference on*. IEEE, 2015, pp. 687–694.

[27] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2018, pp. 1–4.