2019 IEEE 3rd Information Technology,Networking,Electronic and Automation Control Conference (ITNEC 2019)

A survey on mobile edge platform with blockchain

Yujin Zhu
Shanghai Jiao Tong University
Shanghai, China
zhuyujin@sjtu.edu.cn

***Abstract*—As the Internet of Things (IoT), 5G and embedded artificial cloud computing develop, cloud computing is encountering growing challenges such as stringent latency requirements, network bandwidth constraints, etc. Edge computing proposes to bring computing and storage closer to user ends (UEs). Furthermore, mobile edge computing (MEC) aims to combine edge computing and cloud computing to offer better latency and user experience. However, cloud computing exists some inherent weakness, such as data loss and leakage, threats to data privacy, etc. We propose a blockchain-based MEC platform, called BlockMEC, that consists of unknown devices to distribute computing, control, storage, and networking functions to the edge of network without involving any central controllers. The survey paper also summarizes typical MEC concepts and makes comparisons between them and BlockMEC.**

***Index Terms*—Edge Computing, Blockchain, Internet of Things (IoT)**

I. Introduction

Over the past few decades, moving computing, control, and storage into the cloud has been an important trend. Many companies, such as Amazon, Google, Microsoft, etc., have established their cloud computing platforms. Cloud computing platform distributes tasks to hundreds of thousands of commodity PCs or servers in data centers, which tolerates the failure of parts of nodes and ensures long-term operation without system crash. Also, the data centers are equipped with the standard and modularized machine room, which has reserve power supply, cooling equipment and secure network, to provide stable and reliable service. As a result, computing, storage, and network management functions are shifted to centralized data centers, backbone IP networks, and cellular core networks.

However, cloud computing is encountering growing challenges in meeting new requirements in the Internet of Things (IoT), 5G and embedded artificial intelligence, such as stringent latency requirements, network bandwidth constraints, resource-constrained devices, cyber-physical systems, uninterrupted services with intermittent connectivity to the cloud, and new cyber security challenges [3]. Except for the above issues, data security challenges in the cloud are also the key concern, including data loss and leakage, and data privacy [11], [12].

To fill the technology gaps of cloud computing in supporting IoT, the fog computing distributes computing, control, storage, and networking functions closer to end user devices [3]. It covers both mobile and wireline scenarios, traverses across hardware and software, resides on network edge but also over access networks and among end users, and includes both data plane and control plane. The idea behind the fog computing is to place real-time processing, rapid innovation, user-centric service and edge resource pooling, which are not inadequate to the cloud, at user ends (UEs).

The first edge computing concept, which is to bring the computation/storage closer to end user devices, is cloudlet proposed in 2009 [2]. Also, the concept, known as mobile edge computing (MEC), is developed by the newly created (2014) industry specification group (ISG) within European Telecommunications Standards Institute (ETSI). ISG MEC proposes to provide an IT service environment and cloud-computing capabilities at the edge of the mobile network [1]. ISG MEC aims to reduce latency, ensure highly efficient network operation and service delivery, and offer an improved user experience. Different from ISG MEC, some MEC concepts, such as MMC and MobiScud, try not to introduce any centralized control entity into the network and the controller is assumed to be fully distributed.

Edge computing focuses on distributing computation and storage closer to end users, and separates the control plane to the cloud or a distributed manager [4]. A control plane based on the cloud should inherit the inside weakness of cloud computing, such as data security challenges, limited resources, etc. A distributed manager relies on a consensus algorithm to reach an agreement among the whole nodes without involving any centralized controller. In addition, the Byzantine Generals Problem[8] is to reach consensus without any assumptions about failures; participants may stop, omit messages, deliver them in wrong order, lie, or collude. Byzantine Fault-Tolerant (BFT) consensus algorithm aims to seek solutions while participants in the system can behave maliciously. Also, the conventional BFT consensus algorithm, such as Paxos, assumes a static network of known participants.

Blockchain is an emerging distributed technology that is well scalable on a network of unknown participants, such as the ad-hoc, P2P or dynamic network. It is known as distributed ledger technology, first proposed as Bitcoin by Satoshi Nakamoto in 2008 [9]. Ethereum [7], [8] is a blockchain with a built-in Turing-complete programming language that allows anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions. Smart contracts make blockchain beyond a distributed network and become a distributed manager, which is well-suited with edge computing.

This paper starts with the range of new challenges of cloud

978-1-5386-6243-4/19/$31.00 ©2019 IEEE

TABLE I
COMPARISON OF EXISTING MEC CONCEPTS

MEC concepts	Control Plane	Control placement	Computation/storage placement
SCC	Centralized	SCMs in RAN (e.g., as close as possible to the cluster) or in CN (e.g., at the MME)	SCeNBs
MMC	Decentralized	Decentralized core entities	Edges (eNBs etc.)
MobiScud	Decentralized	Decentralized MCs	Distributed cloud within or close to RAN
FMC	Centralized	FMC controller in DCs	DCs
CONCERT	Centralized (or hierarchical manner)	N/A	eNBs(RIEs, WDM switches), regional and local servers
ETSI MEC	Centralized	N/A	edge of CN

computing in the emerging IoT. Then, it discusses typical MEC concepts and blockchain protocols, and explains why both concepts are very complementary (Section II). Then, we innovatively propose a new MEC platform based on blockchain that distributes computing, control, storage, and networking functions closer to end-user devices (Section III). We also discuss the characteristics, advantages and challenges of BlockMEC, and make comparisons between conventional MEC concepts and BlockMEC. Finally, we summarize general outcomes and draw conclusions (Section IV).

II. MOTIVATION AND RELATED WORK

A. Cloud Computing

Cloud computing has been popular over the past 15 years. It is attractive to business owners as it eliminates the requirement of users to pre-plan for provisioning, and allows companies to start from small size and increase resources only when there is a rise in service demand.

Nowadays, as the Internet of Things (IoT), 5G and embedded artificial cloud computing develop, we enter the period of Internet of Everything (IoE). According to the prediction of Cisco IBSG, there will be 50 billion devices connected to the Internet by 2020 and 6.58 devices per person [10]. According to the prediction of IDC, the worldwide digital data we create and copy annually will reach 44 zettabytes; the digital data that is generated by mobile devices and people will increase from 17% in 2013 to 27% in 2020; the percentage of mobile devices in the IoT will be more than 75% by 2020 [12].

However, the developing IoT introduces many new challenges, which cannot be adequately addressed by cloud computing, such as 1) IoT devices or systems demand that end-to-end latencies between the sensor and the control node stay within a stringent latency; 2) the vast and rapidly growing of IoT devices is creating data at an exponential rate, which requires prohibitively high network bandwidth; 2) the interactions with the cloud require resource-intensive processing and complex protocols, which brings heavy operations to local resource-constrained devices; 4) the hardware and software in mission-critical systems should not be updated over time; 5) many IoT devices require uninterrupted services with intermittent connectivity to the cloud; 6) there exist many new cyber security challenges, including protecting resource-constrained devices, assessing the security status of large distributed systems in trustworthy manner, etc.

In addition, cloud computing is also critical for its data security. According to the 2018 Cloud Security Report from Crowd Research Partners, nine out of ten cyber security professionals confirm they are concerned about cloud security, up 11 percentage points from last year's cloud security survey [11]. And the top three security challenges in the report includes protecting against data loss and leakage, threats to data privacy, and the breaches of confidentiality.

B. Mobile Edge Computing

Considering the above challenges with cloud computing, edge computing is emerging as a very promising computation architecture by pushing computation and storage closer to end users. MEC aims at reducing latency, ensuring highly efficient network operation and service delivery, and offering an improved user experience. Various MEC concepts, as are shown in Table I, have recently been proposed to bring computation and storage close to the UEs in certain scenarios. Generally, we can divide these solutions into two categories: 1) the hybrid architecture with distributed edge nodes and a centralized controller; the decentralized architecture with distributed edge nodes and a decentralized control manner.

1) Hybrid Architecture: A hybrid architecture of MEC enables to include data centers and edge nodes as part of the core network (CN). Complementing the centralized cloud computing, the MEC concept stands out along the following three dimensions: carrying out a substantial amount of data storage near or at UEs (rather than storage data only in remote data centers); carrying out a substantial amount of control and computing functions near or at UEs (rather than performing all these functions in remote data centers and cellular core networks); carrying out a substantial amount of communication and networking near or at UEs (rather than routing all network traffic through the backbone networks) [3]. *Small cell cloud* (*SCC*) requires a controller entity (SCM) to coordinate the overall operations in the cluster of small cells (SCeNBs) [20]. *Follow me cloud* (*FMC*) relies on a FMC controller to smooth migration of an ongoing IP service between a data center (DC) and user equipment of 3GPP mobile network to another optimal DCs with no service disruption [19]. *CONCERT* introduces a control plane entity, called *Conductor*, to develop a converged edge infrastructure for future cellular communications and mobile computing services [15]. *ETSI MEC* includes a mobile edge system level management to process core functionality, such as triggering application termination, and a mobile edge host level management to manage nodes' lifecycle, rules, etc. [16]. Edge computing and cloud complement each other to form a service continuum between the cloud and the UEs by providing mutually beneficial and interdependent services to make computing, storage, control, and communication possible anywhere along the continuum.

2) Decentralized Architecture: A decentralized architecture of MEC does not introduce any centralized controller into the ad-hoc cluster. To facilitate the ad-hoc cluster, several critical challenges need to be addressed; 1) finding proper core nodes in proximity while guaranteeing that processed data will be delivered back to UEs; 2) enabling coordination among core nodes despite the fact that there are no control channels to facilitate reliable computing; 3) motivating core nodes to provide their computing power to other devices that have the battery consumption and additional data transmission constraints; 4) security and privacy issues. *Mobile micro clouds* (*MMC*) envisions a logical network composed of two components, the core and the edge, and tries to deliver situational awareness to the small units (primarily interacting with the edge) in a resource-aware manner [18]. *Fast moving personal cloud* (*MobiScud*) integrates cloud, which acts as distributed MobiScud Controls (MCs), and SDN technologies into mobile (LTE/EPC) network to offload low-latency, compute-intensive applications to the private VM instance [17].

C. Blockchain

The blockchain technology is an emerging distributed protocol that is driven by Byzantine fault tolerant (BFT) consensus algorithm such as proof-of-work (PoW) [9]. It is also known as distributed ledger technology, which allows a digital ledger of transactions to be created and shared between distributed nodes on a network with unknown participants. In addition, blockchain is expected to be well suited with the addition of smart contracts that use computerized transaction protocols to execute the terms of contracts agreed by users of a blockchain [6]. In detail, smart contracts are computer programs, which run on the blockchain, and can be self-executed when the conditions that are written in the source code are met. Ethereum [7], [8] is a blockchain with a built-in Turing-complete programming language that allows anyone to write smart contracts and decentralized applications such as product manufacturing, supply chain management, vehicle provenance, and sharing resources such as electricity.

Blockchain and smart contracts provide us with a decentralized platform with an embedded control plane. Also, the infrastructure of MEC concepts is divided into heterogeneous physical data plane resources and a decoupled control plane component [scc etc.]. Since edge computing only distributes computation and storage to UEs, we get an inspiration that blockchain can support edge computing as a decentralized controller to decouple the cloud from its cluster. A mobile edge platform based on blockchain can implement the functionality of management by smart contracts. Therefore, the performance of the system relies on the efficiency of blockchain protocols. Extensive researches have been conducted to improve the efficiency of blockchain protocols. Bitcoin-NG is a scalable blockchain protocol with latency limited only by the propagation time of network and network bandwidth limited only by the capacity of individual nodes [13]. Casper is BFT consensus mechanism combining proof of stake algorithm to make distributed nodes reach an agreement with less cost of resource [14].

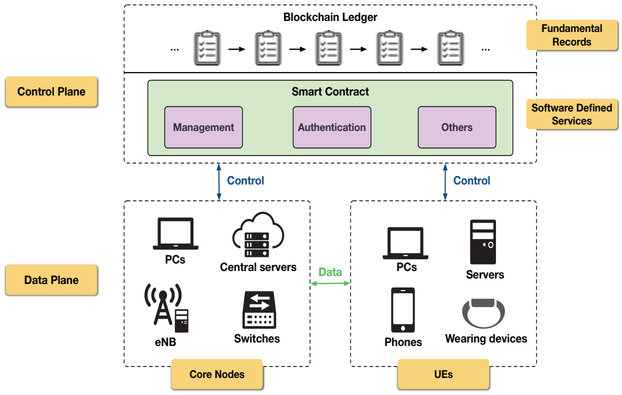

Fig. 1. The architecture of BlockMEC

III. New Mobile Edge Platform

In the section, we present a new MEC platform based on blockchain, called BlockMEC, to distribute computing, storage, control, and networking functions closer to end user devices. Blockchain establishes a decentralized network, which maintains a distributed ledger of transactions driven by BFT consensus algorithm, and provides a Turing-complete programming language to write smart contracts, which can implement any contracts or distributed applications such as vehicle provenance, product manufacturing, etc. Blockchain enables any kinds unknown nodes joining in or leaving the network at will without influencing the operation of the system. In addition, unknown edge nodes, which include base stations (eNBs), personal computers (PCs), Central servers, etc., get the motivation to join in the network and not to harm the system services.

A. Architecture

The proposed architecture of BlockMEC is shown in Figure 1. The infrastructure is divided into heterogeneous physical data plane resources and a decoupled control plane system based on blockchain. Notably, BlockMEC does not introduce any central controller in the system. Blockchain works as the control plane and manages the interactions among edge nodes. In addition, *core nodes* and *UEs* can exchange data with each other. Smart contracts manages the whole control manner with *core nodes* and *UEs*. Next, we describe each component of BlockMEC in detail.

1) Control Plane: The control plane coordinates physical data plane resources. It is based on blockchain and driven by BFT consensus algorithm. Specifically, it consists of *fundamental records* and *software defined services*.

TABLE II
MAIN CHARACTERISTICS OF BLOCKMEC AND HOW IT COMPLEMENTS CLOUD AND MEC

	Cloud	MEC	BlockMEC
Location and Model of Computing	Centralized in several data centers.	Distributed over large geographical areas, closer to users. Controlled in centralized or distributed manner.	Distributed at user ends.
Size	Cloud data centers are very large, usually containing thousands of servers.	A micro cloud node is used to store local data. A large number of micro cloud nodes form a large distributed storage.	Data is distributed over the whole edge nodes and only collected on demand.
Deployment	Require sophisticated deployment process.	While some micro cloud nodes will require pre-planned deployment, most nodes will enable ad-hoc deployment.	Deployment with no or minimal planning.
Operation	Operate in facilities and selected environments and fully controlled by cloud providers. Maintained by technical expert teams. Run in large companies.	Operate in environments that are determined by customers. A MEC system may not be controlled by anyone and maintained by technical experts. System operation may require no or little human intervention. May be operated by large and small companies.	Operate in ad-hoc environment. BlockMEC does not need any human intervention. Each edge node is maintained on their own. Operated by individuals and companies.
Applications	Support predominately, if not only, cyber-domain applications. Typically support applications that can tolerate round-trip delays.	Support both cyber-domain and cyber-physical systems and applications Support significantly more time-critical applications.	Support any kind of system whose operation relies on data exchange. Support significantly more time-critical applications with an additional delay of smart contract function calls.
Internet Connectivity and Bandwidth Requirements	Require clients to keep network connectivity to the cloud for uninterrupted services. Long-haul network bandwidth requirements grow with the amount of data generated by clients.	Operate autonomously to provide uninterrupted services even no or intermittent internet connectivity. Long-haul network bandwidth requirements grow with the amount of data that need to be sent to the cloud after filtered by local edge nodes.	Similar to MEC. Large quantity of edge nodes provides nearly unlimited network bandwidth.

Fundamental records – Fundamental records are on the distributed ledger, provided by blockchain. According to BFT consensus algorithm, the distributed ledger will keep immutable, transparent and traceable to the public. Since any historical change should get approved by most of the nodes on the blockchain network, any malicious node cannot tamper the historical records without notifying others, which means the ledger is similarly immutable. In addition, the ledger is shared with the whole edge nodes on the blockchain network, which means any record is transparent. Moreover, the distributed ledger records transactions in chronological order, which means any action is traceable by reviewing the ledger. The three properties of *fundamental records* establish the trusts among edge nodes and the control plane system.

Software defined services – Software defined services implement various services to provide new features and management to BlockMEC. The services are deployed by smart contracts. And the invocations of services are some smart contract function calls, which are transactions in the distributed ledger. In addition, the code of smart contracts are also recorded in the ledger; thus, either the historical records or the code of smart contracts are trustworthy to the whole edge nodes. The basic service that BlockMEC supports is management and authentication. The management service controls the operation of the system and maintains the status of the network, which can be further utilized to make optimal decisions, access the security status of the distributed system, etc. And the authentication service helps the process of authority check on edge side in case that edge nodes work in a malicious environment. With the Turing-complete programming language in blockchain, smart contracts can deploy any kind of service by a distributed manner, such as load balancing, data sharing, content delivery network (CDN), etc.

2) Data Plane: The data plane consists of *core nodes* and *UEs*. *UEs* are the edge nodes that can access to small quantities of more real-time and dynamic data. *UEs* continuously collect data from the edge of the mobile network and locally complete parts of computation. For example, wearing devices keep collecting users' basic physical data such as heart rate, blood pressure, number of steps, etc., and locally process simple data cleaning and data merging before updating data to core nodes. *Core nodes* are the edge nodes that control access to large quantities of static (and possibly stale) information or possess essential private data or other functions that UEs cannot afford. Each *core node* works as a micro cloud to serve its surrounding UEs. Since UEs have limited computation and storage resource, *core nodes* have to finish the rest computation after receiving data from UEs. Usually, *core nodes* will cooperate with each other to complete a complex task. *UEs* and *core nodes* are separated by dynamic and form a constrained network with a many-to-one relationship between *UEs* and *core nodes*. In addition, BlockMEC does not restrict the specific core nodes and UEs. Unknown devices can resgiter to work as a *core node* or *UE*. However, *UEs* will not interact with a untrustworthy *core node*. And, *core nodes* should judge whether a *UE* is untrustworthy before starting its tasks.

B. Characteristics and Advantages

BlockMEC distributes computation, storage, control and networking functions to the whole edge nodes on the network. Therefore, the architecture of BlockMEC is fully distributed.

In addition, BlockMEC allows any unknown device in anywhere to act as *core nodes*. This can efficiently reduce the round-trip delay between *core nodes* and *UEs* because *UEs* can reduce the need for the remote cloud and *UEs* have more choices of micro cloud nodes. With smart contracts, BlockMEC removes the dependence on central controllers. And the Turing-complete programming language makes smart contracts be able to implement any service. Table II outlines the main characteristics of BlockMEC and how it complements cloud and MEC.

BlockMEC's main advantages can be elaborated as follows:

1) Efficiency: BlockMEC can distribute computing, storage, control and networking functions around UEs to take full advantage of the resources available and short routing path. The system motivates individuals and companies to share their idle resources, such as tablets, servers, laptops, network edge routers, connected vehicles, etc., available on the network. Distributed applications can leverage approximately unlimited resources on BlockMEC to provide better services to the public.

2) Agility: Conventional MEC concepts require to pre-plan the location of parts of core nodes to better carry out the computing, storage, and control functions along the cloud-to-thing continuum. BlockMEC allows any unknown devices to join in the network as a core node, which brings more core nodes and better distribution of resources. Therefore, BlockMEC has not to be aware of and closely reflect customer requirements for shortening routing path.

3) Latency: BlockMEC enables data analysis around UEs and provides a large number of core nodes to UEs for selecting more suitable nodes. Therefore, BlockMEC can process tasks from UEs without the cost of round-trip latency. Since it allows any unknown devices to be core nodes, it also has more core nodes compared with the current MEC concepts.

C. Challenges

BlockMEC proposes to establish a MEC platform without involving the cloud or any centralized controller. Therefore, we have to establish the system from the start-up. We address several challenges in BlockMEC during the procedure. First, we have to implement the functions or services, which are already provided by the cloud, in smart contracts. For example, BlockMEC must have an authentication mechanism to validate the identity of edge nodes for security. Inspired by Secure Sockets Layer (SSL) protocol, smart contracts can act as an authority institution to help establish trusts among edge nodes. Second, BlockMEC has to design a motivation mechanism to keep idle devices online. For example, BlockMEC can share any value that is generated during the operation of the system with the whole edge nodes on the network by the medium of digital tokens.

IV. Conclusion

BlockMEC offers a brand new blockchain-based architecture of MEC, which reshapes the future landscape of industries and individuals. It motivates any unknown device to join in the network to work as core nodes. Smart contracts coordinate core nodes and UEs, and ensure edge nodes to work in a trustworthy environment. Since more devices can act as core nodes, BlockMEC can further improve the performance of the system, such as reducing latency, providing UEs with more storage and computation, etc. Without involving any central controllers, BlockMEC should support better security and scalability while providing real-time processing, rapid innovation, user-centric service and edge resource pooling. BlockMEC proves that blockchain can improve the architecture of edge computing by bringing control and networking functions to the network in a distributed manner.

References

[1] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computingA key technology towards 5G," ETSI white paper, vol. 11, no. 11, pp. 1-6, Sep. 2015.

[2] S. Ibrahim, H. Jin, B. Cheng, H. Cao, S. Wu, L. Qi, "Cloudlet: towards mapreduce implementation on virtual machines," the 18th ACM international symposium on High performance distributed computing, pp. 65-66, Jun. 2009.

[3] M. Chiang, and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854-864, Dec. 2016.

[4] P. Mach, and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," arXiv preprint arXiv:1702.05309, Feb. 2017.

[5] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," IEEE Communications Magazine, vol. 56, no. 8, pp. 33-9, Aug. 2018.

[6] S. Underwood, "Blockchain beyond bitcoin," Communications of the ACM, vol. 59, no. 11, pp. 15-7, Oct. 2016.

[7] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, Apr 2014.

[8] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum project white papers, Jan 2014.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[10] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," CISCO white paper, vol. 1, no. 2011, pp. 1-1, Apr. 2011.

[11] Crowd Research Partners. 2018. CLOUD SECURITY REPORT. (2018). Retrieved November 17, 2018from "https://crowdresearchpartners.com/portfolio/cloud-security-report/".

[12] V. Turner, J. F. Gantz, D. Reinsel, and S. Minton, "The digital universe of opportunities: Rich data and the increasing value of the internet of things," IDC Analyze the Future, vol. 16, Apr. 2014.

[13] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," NSDI, pp. 45-59, 2016.

[14] V. Buterin, and V. Griffith, "Casper the friendly finality gadget," arXiv preprint arXiv:1710.09437, Oct. 2017.

[15] J. Liu, T. Zhao, S. Zhou, Y. Cheng, and Z. Niu, "CONCERT: a cloud-based architecture for next-generation cellular systems," IEEE Wireless Communications, vol. 21, no. 6, pp. 14-22, Dec. 2014.

[16] MECISG ETSI, "Mobile edge computing (mec): framework and reference architecture," ETSI, DGS MEC, vol. 3, Apr. 2016.

[17] K. Wang, M. Shen, J. Cho, A. Banerjee, J. Van der Merwe, and K. Webb, "Mobiscud: A fast moving personal cloud in the mobile network," the 5th Workshop on All Things Cellular: Operations, Applications and Challenges," pp. 19-24, Aug. 2015.

[18] S. Wang, G. H. Tu, R. Ganti, T. He, K. Leung, H. Tripp, K. Warr, and M. Zafer, "Mobile micro-cloud: Application classification, mapping, and deployment," Annual Fall Meeting of ITA, Oct. 2013.

[19] T. Taleb, and A. Ksentini. "Follow me cloud: interworking federated clouds and distributed mobile networks," IEEE Network, vol. 27, no. 5, pp. 12-9, Sep. 2013.

[20] F. Lobillo, Z. Becvar, M. A. Puente, P. Mach, F. L. Presti, F. Gambetti, M. Goldhamer, J. Vidal, A. K. Widiawan, and E. Calvanesse, "An architecture for mobile computation offloading on cloud-enabled LTE small cells," Wireless Communications and Networking Conference Workshops, pp. 1-6, Apr. 2014.