Participatory IoT Networks-on-Demand for Safe, Reliable and Responsive Urban Cities

Bechir Hamdaoui, Oregon State University, hamdaoui@oregonstate.edu; **Nizar Zorba**, Qatar University, nizarz@qu.edu.qa; and **Ammar Rayes**, Cisco Systems, rayes@cisco.com

Unleashing the Power of IoT through Blockchains and Cloud Computing Technologies

One key reason behind the recent success of Internet of Things (IoT) is the ever-increasing ability of IoT devices to perform various computation and sensing tasks, with network connectivity allowing them to communicate data over the Internet in real-time [1]. Such capabilities make IoT devices, especially when considered collectively, great enablers for a myriad of new applications and services that could make urban cities safer and more responsive. To illustrate, consider a large city event, such as the Soccer World Cup, the Olympic Games, or a major concert. An event of such a scale presents city officials with major challenges, merely arising from the arrival and presence of massive numbers of event attendees and spanning various city matters, including surveillance, emergency management, and traffic control. The envisioned IoT-enabled applications will mitigate these challenges.

Each application will involve multiple IoT devices, distributed across the city, that are grouped, *dynamically* and *on-demand*, to collaboratively process a stream of collected data to extract and produce actionable information, as required by the underlying application. In this article, we refer to each collection of IoT devices grouped to support an application as a **Participatory Network-on-Demand (NoD)** instance, where here the IoT devices decide to join and contribute to the application at their own will, and thus the term 'participatory'.

The futuristic vision of smart cities is to consider cloud enabled-IoT as an intelligent infrastructure [2,3], with capabilities far greater than those of today's computing infrastructures, that serves multiple entities/ groups of the city, with each entity or group having its unique interest in collecting and processing data to serve its own mission. In this work, we adopt a *mission-centric space view* for establishing the participatory NoD instances, with each *mission space* constituted by all NoD instances supporting the city groups/entities with the same interest/mission. Considering the large-scale city event, like the Soccer World Cup, again for illustration, multiple NoD instances may, for instance, be needed to serve three different entities, each with a different mission: (i) *Surveillance Mission*, with an NoD instance for monitoring and detecting threats and alerting police in real-time; (ii) *Emergency Relief Mission*, with an NoD instance for routing and guiding ambulances and medical staffs to get to the accident scene as quickly as possible; (iii) *Traffic Control Mission*, with an NOD instance for monitoring traffic and assisting drivers in reaching their target destinations.

In this work, we leverage and combine the merits of both blockchains and cloud computing technologies to enable the deployment and management of NoD instances to serve multiple different city missions. Our blockchains-enabled distributed mechanisms allow: (i) the registration, discovery and management of participatory IoT devices; (ii) enable the creation and mapping of NoD instances on top of the IoT resources; (iii) ensure service delivery and integrity of committed IoT devices; and (iv) reward and secure payments to participatory devices.

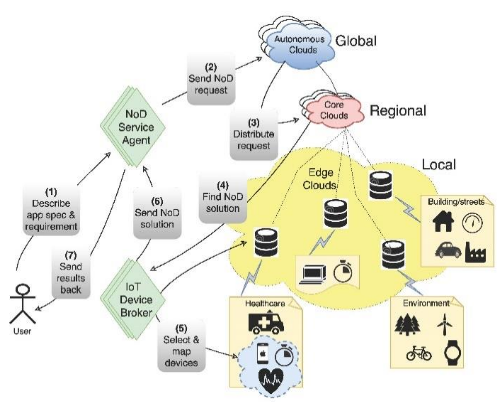

Fig. 1. System Overview: 4-tier IoT/Cloud Infrastructure and Protocol Operations

Participatory Networks-on-Demand: System Components

Scalable IoT/Cloud Infrastructure

Fig. 1 depicts the proposed 4-tier system architecture. The top tier, Tier 1, constitutes the different *Autonomous Clouds*, like AWS and Google Clouds, and serves as an interface/liaison between the end users and the infrastructure. Tier 2 constitutes the *Core Clouds*, which are distributed across different regions in the world and owned by the *Autonomous Clouds*. Each *Core Cloud*, in turn, is associated with multiple *Edge Clouds*, covering the different regions of the city to serve as cloud edges and bring cloud resources closer to the IoT devices [2]. Tier 3 is formed by all the *Edge Clouds*. Finally, Tier 4 is the tier representing the IoT devices, with each device being associated with at least one *Edge Cloud* to manage and handle its Internet connection and service.

Let's now illustrate the NoD instantiation steps through an example. Suppose that the law enforcement office wants to track a suspected criminal in some area of the city. The office can then issue a request, describing the requirements and specifications of their surveillance application to a NoD Service Agent (Step 1 in Fig. 1). The NoD Service Agent, here, can be perceived as a high-layer service provider that serves as the liaison between the end user (e.g., law enforcement office) and the cloud/IoT infrastructure. It receives the application requests from the different interest groups, translating the interest groups' requirements and specifications into NoD requests, and sending the NoD requests to the *Autonomous Clouds* (Step 2). Once an NoD request is received, it is then disseminated to the *Core Clouds* representing the geographic area of interest as indicated in the request (Step 3), invoking then the running of the NoD instantiation mechanisms by IoT Device Broker (Step 4), which first finds a device mapping solution (Step 5) and then sends it to the NoD Service Agent (Step 6). An IoT Device Broker, here, is a service provider that serves as a broker for IoT devices to handle their registration, manage their payments, advertise their service, etc. Finally, the NoD Service Agent monitors the created NoD instance and sends its configuration information back to the law enforcement officials (step 7).

Blockchain-Enabled NoD Instantiation Mechanisms

We use blockchains [3] to develop distributed mechanisms that enable scalable, fast, and reliable mappings of NoD instances on top of the Cloud/IoT infrastructure. In our framework, the use of blockchains enabled: (i) simplified recordkeeping and management of IoT devices, (ii) distributed NoD mapping and instantiation, (iii) service delivery monitoring and verification, and (iv) secure payments and fund transfers to selected devices. The functionalities and responsibilities of the proposed mechanisms can be captured in five main modules, which constitute our developed blockchains-enabled protocols:

- The first module handles the registration and management of the participatory IoT devices by allowing IoT devices to join, authenticate and register themselves to the network.
- The second module focuses on the discovery of the registered IoT devices and the mapping of the NoD instances onto these discovered devices.
- The third module monitors the committed devices to make sure that they are up for delivering their agreed upon service, and provides backup plans in case of service delivery failure.
- The fourth module builds and maintains a trust system to keep track of devices' reputations vis-à-vis of service delivery quality and timeliness. The second module relies on these reputations to select devices during the mapping phase.
- The fifth module is responsible for service delivery verification, and for securing payments and fund transfers to the devices that deemed to have performed their service successfully as agreed upon.

Conclusion and Open Challenges

We showed the potentials of using blockchains and cloud technologies for easing the establishment and management of participatory IoT networks on-demand to enable situation-awareness city applications. Clearly, the system at hand is very complex, with many unsolved challenges. For the architectural aspects, we envision that with such a complex system, many different types of service providers and deal-making agents will emerge, each interested in different parts of the system and with different needs and requirements. One future challenge would then be to develop unified languages to ease the interactions among these different entities, allowing the entities to express their preferences and to interact with one another in a systematic way. Another related challenge would be to define the functionalities and responsibilities of the different system entities, and to determine and define their interfaces and interactions.

As for the protocol design aspects, new mining and consensus strategies suitable for IoT remain to be developed. IoT devices have limited computation, storage and energy resources, making existing approaches (e.g. Proof-of-Work for Bitcoin) inefficient due to their heavy computation and/or long delay requirements.

Acknowledgement

This work was supported in part by NSF/CNS-1162296 and Cisco.

References

[1] S. Abdelwahab, B. Hamdaoui, M. Guizani, A. Rayes, "Enabling smart cloud services through remote sensing: An internet of everything enabler," *IEEE Internet of Things Journal, June 2014, pp. 276–288*.

[2] S. Faieq, R. Saidi, H. Elghazi, and M. D. Rahmani, "C2IoT: A framework for Cloud-based Context-aware Internet of Things services for smart cities," *In Proceedings of International Conference on Mobile Systems and Pervasive Computing, 2017, pp. 151-158*.

[3] C. Formisano, D. Pavia, L. Gurgen, T. Yonezawa, J. A. Galache, K. Doguchi, and I. Matranga, "The advantages of IoT and Cloud applied to Smart Cities," *In Proceedings of International Conference on Future Internet of Things and Cloud, 2015*

[4] S. Abdelwahab, S. Zhang, A. Greenacre, K. Ovesen, K. Bergman, and B. Hamdaoui, "When clones flock near the fog," *IEEE Internet of Things Journal, June 2018, pp. 1914 – 1923*.

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

Bechir Hamdaoui (S'02-M'05-SM'12) is a Professor in the School of Electrical Engineering and Computer Science at Oregon State University. He received M.S. degrees in both ECE (2002) and CS (2004), and a Ph.D. degree in ECE (2005) all from the University of Wisconsin-Madison. His research interests are in the general areas of computer networks, mobile computing, and wireless communications. He won several awards, including the ICC 2017 and IWCMC 2017 Best Paper Awards, the 2016 EECS Outstanding Research Award, and the 2009 NSF CAREER Award. He serves/served as an Associate Editor for several journals, including IEEE Transactions on Mobile Computing, IEEE Transactions on Wireless Communications, IEEE Network, and IEEE Transactions on Vehicular Technology. He also chaired/co-chaired many IEEE conference programs/symposia, including the 2017 INFOCOM Demo/Posters program, the 2016 IEEE GLOBECOM Mobile and Wireless Networks symposium, and many others. He served as a Distinguished Lecturer for the IEEE Communication Society for 2016 and 2017. He is a Senior Member of IEEE.

Nizar Zobra received a B.Sc. degree in Electrical Engineering from JUST University, Jordan, in 2002, the M.Sc. Degree in Data Communications and the M.B.A. degree from the University of Zaragoza, Zaragoza, Spain, in 2004 and 2005, respectively, and the Ph.D. degree in Signal Processing for Communications from UPC Barcelona, Spain, in 2007. He is an Associate Professor at the Electrical Engineering department at Qatar University, and is currently the Vice-chair of the IEEE ComSoc Communication Systems Integration and Modeling Technical Committee. He is an IEEE Senior Member. He has more than 100 publications in journals and conference proceedings, and his work led to 5 patents. His research interests span 5G-IoT networks optimization, crowd management and Blockchain.

Ammar Rayes [S'85, M'91, SM'15] is a Distinguished Engineer at Cisco's Advanced Services CTO Office working on the Technology Strategy. His research interests include Network Analytics, IoT, Machine Learning and NMS/OSS. He has authored over 100 publications in refereed journals and conferences on advances in software & networking related technologies, 4 Books and over 30 US and International patents. He is the Founding President and board member of the International Society of Service Innovation Professionals www.issip.org, Adjunct Professor at San Jose State University, Editor-in-Chief of "Advances of Internet of Things" Journal, Editorial Board Member of IEEE Blockchain Newsletter, Transactions on Industrial Networks and Intelligent Systems, Journal of Electronic Research and Application and the European Alliance for Innovation - Industrial Networks and Intelligent Systems. He has served as Associate Editor of ACM Transactions on Internet Technology and Wireless Communications and Mobile Computing Journals, Guest Editor of multiple journals and over half a dozen IEEE Communication or Network Magazine issues, co-chaired the Frontiers in Service Conference and appeared as Keynote speaker at several IEEE and industry Conferences: https://sites.google.com/view/ammarrayes/home. At Cisco, Ammar is the founding chair of Cisco Services Research and Cisco Services Patent Council. He received Cisco Chairman's Choice Award for IoT Excellent Innovation & Execution. He received his BS and MS Degrees in EE from the University of Illinois at Urbana and his Ph.D. degree in EE from Washington University in St. Louis, Missouri, where he received the Outstanding Graduate Student Award in Telecommunications.