Interoperability and Decentralization as Key Technologies for Future Smart Urban Environments

Marcin Plociennik*, Mario Drobics†, Ivana Podnar Žarko‡,
Konstantinos Katsaros§, Sergios Soursos§, and Ivan Gojmerac†
*Institute of Bioorganic Chemistry Polish Academy of Science (PSNC), marcinp@man.poznan.pl
†AIT Austrian Institute of Technology GmbH, Austria, mario.drobics|ivan.gojmerac@ait.ac.at
‡University of Zagreb, Faculty of Electrical Engineering and Computing, Croatia, ivana.podnar@fer.hr
§Intracom SA Telecom Solutions, Greece, souse|konkat@intracom-telecom.com

***Abstract*—In the current Internet of Things (IoT), centralized IoT structures greatly limit the direct, efficient and privacy preserving interaction with the locally available resources. A sustainable path for the future development of Smart Urban Environments, from Smart Homes and Offices, to Smart Neighborhoods and Cities, requires next-generation IoT solutions which are interoperable and decentralized. Building on direct device-to-device interactions and the existing infrastructure operated by open and interoperable platforms, a novel decentralized IoT architecture is required to offer both privacy-preserving and smart real-time interactions in Smart Spaces, leading thus to truly trustful ambient intelligence serving ordinary citizens in everyday situations. We present the key interoperability and security-related aspects which are designed and implemented within the H2020 project symbIoTe to pave the way for such decentralized IoT solutions. Furthermore, we analyze the requirements and technologies, namely Distributed Ledger Technology (DLT), intelligent agents and edge technologies, as the building blocks for the next-generation IoT solutions.**

I. Introduction

Over the last ten years, Moore's law has fostered the creation of small microelectronic devices that are highly effective in terms of computational power and efficient in terms of energy consumption, naturally leading to the widespread emergence of sensors and actuators that are energy-autonomous and that feature advanced wireless communication as well as backend integration/control [1]. Due to their still limited resources, such sensors and actuators typically cannot be exposed to the full spectrum of IP networking requirements and peer-to-peer interaction with classical Internet devices, necessitating the emergence of dedicated gateways, which are capable of communicating with the small devices in an efficient manner [2]. Completing the picture, such sensor/actuator gateways have so far mostly been addressable only through dedicated Internet-connected platforms, where virtual entities representing actual IoT devices enable indirect accessibility of sensors and actuators from the public, open Internet. Most IoT deployments enable the secure interaction between users and the environment via an indirect path: sensors and actuators are registered to IoT platforms, and the user interacts with the platforms' backend, which may even be very far away, e.g., in a central cloud in a foreign country [3]. The great majority of current commercial IoT solutions are clear examples of this case: Amazon AWS IoT, IBM Watson IoT platform, Microsoft Azure IoT Suite, Google Cloud Platform, and Apple Homekit represent cloud-based services acting as hubs of enterprise and home IoT. This model (or best practice) may definitely work well for many IoT applications, but there are scenarios in which a direct and dynamic, while still seamless and secure interaction with the things is clearly more appropriate (e.g. indoor ambiental control) [4]. Our current understanding of the Internet of Things (IoT) mostly corresponds to this sketched picture, which is actually in stark contrast with the original intention behind the concept of the Internet as an intrinsically distributed network of peering computers/machines that communicate with each other in an efficient, connectionless manner. Instead, in the current IoT world, centralized structures are being designed and implemented that greatly limit the direct, efficient and privacy preserving interaction with the locally available resources.

In order to create a sustainable path for the future development of the world of the Internet of Things, this paper proposes a decentralized Internet of Things (IoT) approach, which will leverage the present spectrum of open IoT-platforms and interoperability frameworks and propose a novel, completely decentralized IoT concept which will enable humans to directly engage with heterogeneous devices in complex and dynamic environments in a scalable, and secure manner.

II. Challenges

The advent of the IoT realizes the deployment and orchestration of a multitude of sensing and actuation devices increasingly shapes new cyber-physical environments. The volume of these devices and the corresponding richness of applications/services have so far resulted in architectural solutions largely relying on a two level hierarchical approach, where data and functions are aggregated at the IoT gateway and/or the cloud. Similarly, device resource constraints motivate the mediation of IoT gateways for the collection of data and/or coordination/support of the application logic. At the same time, security features such as Authentication, Authorization and Accounting (AAA) have been largely facilitated and have

978–1–5386–1478–5/18/$31.00 © 2018 IEEE

built on centralized approaches borrowed from the cloud service domain.

More precisely, we currently face a number of challenges when developing next-generation IoT solutions:

A. Interoperability

Interoperability remains an open problem with over 400 IoT platforms in the market that create a highly fragmented and divergent IoT ecosystem. Such vertical IoT solutions still co-exist and occupy the same homes, factories or municipalities, however, they cannot interoperate since they are built using proprietary software without open and standardized interfaces. It is expected that platform interaction and collaboration will exhibit the full potential of IoT services only by enabling cross-domain applications and dynamic smart environments. However, achieving true IoT platform interoperability is rather challenging, not only because of the need to discover devices supporting different protocols across heterogeneous platforms, but because sharing of resources across stakeholders requires semantic alignment, secure and trusted interactions.

B. Trust

In order to support flexible interactions in distributed systems, it is crucial that the interacting elements have a concept of trust to manage their exchange with other parties. To ensure trust in distributed environments, four levels have to be considered: trust in users, trust in data, trust in nodes, and trust in systems.

- Users: Users should ideally be trusted based on locally available information, rather than necessitating cumbersome and impracticable authentication procedures. However, limiting trust to local information naturally also reduces the accuracy of the trust mechanism. Therefore, intelligent solutions to the problem at hand are needed.
- Nodes: To dynamically incorporate new nodes in existing networks, trust has to be assessed dynamically, too. By combining context-awareness with attribute based encryption, systems should be designed that allow (high-level) access to data in the system only for nodes being co-located to other nodes. This corresponds to the issues of network access and participation in joined communication and aims to guarantee communication security and prevent attacks (e.g., MITM, DoS, policy violation).
- Data: Trust in data can be achieved by ensuring that the data is not manipulated (integrity and authenticity) and can only be read by authorized parties (confidentiality). Depending on the type of data, it can also be important to securely identify the user, the data is linked to (authenticity and accountability).
- Systems: Trust between systems partially addressed in the current projects (IoT federation).

C. Privacy

Users require the protection of their personal information related to their movements, habits and interactions. User awareness of the importance of privacy preservation has been on the rise in recent years, and fortunately, the same is true for most serious service providers. Beyond worry and purely ethical endorsement of privacy mechanisms, the newly introduced General Data Protection Regulation (GDPR) [5] in the European Union mandates strict service provider adherence to a number of principles and rules in this realm.

One of the challenge is to provide mechanism for privacy preserving interaction with local sensors and actuators, and complex service composition with almost zero configuration and minimal user involvement. Constant changes of conditions and prerequisites have an impact on the security and privacy of the user – while some decisions shall be automated, others shall be presented to the user so that the user can make an informed decision.

D. Usability

In today's context of abundant service offerings, only those applications which come along with great utility and low user overhead get accepted, leading to a distribution of offered services' usage proportional their excellence regarding these criteria. The simplicity of the analogue world and its intuitive usability for the end-user should represent the objective when designing decentralized IoT ecosystems.

Bringing the user into the loop during the design of security and privacy relevant measures proves to be essential since the user is an important part of every security and privacy enhancing system. An essential part of user empowerment is the assurance of user-control while enabling maximum usability of our cyber-physical habitats.

E. Decentralised system

Users, sensors, actuators, and any other node able to offer some IoT service should be able to interact with each other directly, i.e., without requiring a centralized IoT platform. Context-aware services: the access to resources or the provisioning of services should be allowed if specific conditions, are satisfied. Decentralized IoT systems create new opportunities for value creation. New technological developments (e.g. blockchain) enable not only decentralizing the technical architecture, but also the value creation process.

III. Enabling Technologies

A. Platform Federation

Seven H2020 projects branded under the name of IoT European Platforms Initiative (IoT-EPI) are working towards the goal to create interoperable IoT ecosystems, while focusing on different interoperability aspects. We put forward symbIoTe (https://www.symbiote-h2020.eu/), which is creating an interoperability framework supporting both semantic and organizational interoperability. It allows for flexible interoperability mechanisms across different domains: both at the cloud level and within smart spaces hosting gateways and smart devices operated by various IoT platforms [6]. SymbIoTe focus on interoperability for the creation of environments in which multiple platforms expose resources in a uniform fashion for fast development of IoT applications, and in which

it is possible for platform federations to barter and trade resources. Semantic interoperability plays a central role here since platforms and applications need to understand resource descriptions in order to use them [7]. SymbIoTe exposes both sensors and actuators as services managed by actual platforms to third parties, by means of their virtual representation in the cloud. Third parties are granted access to RESTful services to retrieve sensor data or invoke actuator primitives by means of the Attribute-Based Access Control mechanism, a distributed and decoupled mechanism for authentication with token-based authorization [8]. The symbIoTe Smart Spaces (SSP) are environments (e.g., residence, campus, etc.) in which one or more IoT platforms provide coordinated services. Such environments are typically related to a physical space (e.g. house or building), but in a more general case SSP can extend to a broader physical space (e.g., a smart campus or smart city). The key features developed for SSP in symbIoTe are the following: 1) dynamic discovery and automatic configuration of resources that are exposed to other collocated IoT platforms and third party applications, 2) platform interoperability at the SSP level where collocated platforms interact, but only at the gateway level, and 3) support for nomadic devices which are integrated into visited SSPs and are granted local access to certain services within a SSP.

B. Distributed Ledger Technology

Decentralized systems came to life with the rise of peer-to-peer (P2P) solutions at the beginning of the millennium, where the power of many processes distributed over the entire Internet is used to provide dedicated services, from data management to VoIP. Today, we are witnessing the advent of next-generation decentralized solutions: Blockchains and Distributed Ledger Technology (DLT). DLT is promoted as a disruptive technology for orchestrating distributed trustless environments with many actors. It is prophesied to play the role of a decentralized trusted intermediary – a distributed ledger – in many domains, from financial services and banking to supply chain management and Internet of Things. Indeed, the support of smart contracts for transaction execution among a group of processes, while ensuring consensus, transparency and immutability in large scale distributed environments, is indeed a revolutionary one. However, scalability and low transaction rate are currently the main obstacles for the adoption of this technology in IoT deployments. Current DLT approaches specifically designed for IoT try to overcome these shortcomings. Two exmaples of such approaches are IOTA [9], where transactions are stored in a tangle (i.e. an directed acyclic Graph where each new transaction is approved by two existing ones) and RaiBlocks [10].

C. Intelligent Agents

Multi-agent systems based on deep learning have a huge potential to simplify user interactions with complex, distributed IoT environments and to create new types of localized, highly efficient services. We are considering to use both smart agents with learning capabilities and lightweight working agents for executing simple jobs. In order to implement a deep learning agent, the agent needs to acquire information about a user and his/her context within a smart space, thus it must be context-aware. This can be achieved by reinforcement learning based on the agents performance in terms of measurable goals and feedback received from its owner. The goal is that a personal agent learns user preferences and is capable to auto configure, acquire access to smart space infrastructure, and create dynamic services based on those preferences. The learning process should be automatic and with direct interaction with its owner. Finally, the agent can utilize negotiation strategies to obtain access to resources.

D. Edge Technologies

Computing and networking capabilities of new IoT devices are increasingly miniaturized and become networked personal devices, from wearables and smartphones to smart clothing. Sensors and actuators present increasingly powerful connectivity capabilities (e.g., NB-IoT [Qualcomm2015]) and using IoT gateways becomes a common practice to interconnect IoT enabled environments and to host intelligent IoT applications. At the same time, the emerging Mobile Edge Computing (MEC) [11] and fog computing [12] paradigms bring computational power, storage and network resources at the edge of the network, hence closer to the user. This presents new opportunities for embedding services and applications in the proximity of the user, promising tighter integration within their operational context, substantially improved performance, and enabling context specific, localized data processing.

IV. Concept

The proposed concept is build around decentralised IoT spaces which enable flexible and dynamic interaction between different IoT components. Virtualized cyber-phsical agents are used to support users in interacting with these environments. To support the flexibility a lightweight connectivity management and support mechanism is proposed. Finally, a distributed trust and security management concept is proposed.

A. Decentralised IoT spaces

As IoT develops, and services and applications gradually become a commodity, it becomes apparent that IoT goes beyond the mere collection of and reasoning on information about our surroundings. Actuation increasingly closes the loop for a direct interaction with our cyber-physical environment. In order to succeed and ease our everyday lives, in our proposed concept of interaction is seamlessly and securely integrated with our activities. Furthermore, users are increasingly aware of the problems induced by centralized processing of their data and thus are starting to prefer solutions that keep their data (including, e.g., interaction profiles) as local as possible. This translates to an intelligent and responsive IoT environment in which user activities are not disrupted due to the existence and operation of cyber-physical IoT systems, and where explicit engagement in HCI interactions is minimized. E.g., a smart building automatically adjusts light and temperature conditions

to visitors' needs without explicit instructions through some IoT application user interface. In our approach we therefore envision an IoT environment that embraces users and their devices with intelligence embedded in the cyber-physical space, capable of supporting the localised, natural interaction of users with their surroundings, intrinsically however supporting essential security features (such as AAA). This comes to disrupt the established centralised cloud based solution model, calling for a substantial improvement of perceived performance, experienced in the form of system response times, and for the simplification of user interactions with IoT applications. Obviously, centralized cloud solutions cannot alone support this vision, exactly due to their centralized character that inherently detaches them from smart spaces.

B. Smart Interactions

In order to support user activities in smart spaces, we embed intelligence in this environment in the form of virtualized cyber-physical agents. Agents are responsible for bringing together users with IoT platforms/applications in their environment. User agents are responsible for monitoring user behaviour as expressed via their interaction with smart spaces in various contexts, e.g., collecting lighting or heating preferences of a user at certain times of the day/year. Profiling information then serves the purpose of offloading user actions to the user agents, i.e., user agents act on behalf of the user, instructing the surrounding actuators and/or sensing devices to behave according to their preferences. For instance, a user agent adjusts the heating for the user, once confidence about a corresponding user profile has been established. User agents are distributed allowing different components to reside at the most appropriate devices. This first includes user devices e.g., smartphones, wearables, but also IT infrastructure of the user environment. The distribution of user agent functional components depends on the device capabilities including processing, storage and network/connectivity, as well as on the availability of application agents (as discussed next). For instance, wearable devices collect user movement or environmental conditions information directly from the environment, from surrounding sensors or even other agents; smartphones provide the connectivity to offload profiling data to an IoT gateway or a MEC/cloud server via WiFi/4G/5G interfaces, while they also interact with actuation devices in the environment directly (e.g., Bluetooth bulbs are already commercially available).

At the same time, this concept also enabled existing and new IoT platforms and applications to embed their logic within the environment via application agents. Application agents intend to bring application logic closer to the user compared to remote cloud environments, thus enabling enhanced performance but also new forms of interaction with other applications. For example, a security control application agent exposes user presence information to a lighting management application agent; the exchange is triggered and supported by the collocation of the two agents. Additionally, contextual and aggregate user profiling information is collected so as to optimize behaviour of applications e.g., an application agent collects information on current traffic conditions, including data submitted by user agents (with the consent of the users), allowing a safe change of the traffic lights in the event of emergency. The potential colocation of application and user agents facilitates the offloading of user-IoT application interactions to the surrounding, agent-hosting environment, e.g., a user agent discovers a lighting application agent and submits an authorised instruction to apply the user lighting profile. In this context, application agents support conflict resolution primitives allowing applications/platforms to take decisions on conflicting user and/or user agent actions in the affected area, e.g., mediating room temperature.

It becomes apparent, that this approach fuses the user and application spaces into a decentralised and distributed interaction space where both application and user logic are co-hosted within the environment to facilitate the interaction of users with their cyber-physical environment. To simplify the design development of cyber-physical agents, core functionality, orthogonal to user and/or application specific objectives need to be provided. This needs to include service and user discovery mechanisms enabling a matchmaking process running in the background to allow user agents to interact with their application counterparts, without necessitating the involvement of the user. At the same time however, this matchmaking process needs to be coupled on the foreground, further allowing user devices to anticipate the presence of user and application agents in the environment, and vice-versa, so that interagent communication closely follows user presence and mobility in the environment.

C. Smart connectivity

A lightweight connectivity management/support mechanisms exposes the existence of cyber-physical agents in the environment through wireless link layer mechanisms, e.g., IEEE 802.11u, WiFi Aware. These mechanisms enable user devices to discover wireless networks tailored for the support of the IoT application/platform at hand e.g., WLAN providing connectivity to application agent. Resource management capabilities facilitate applications/platforms in keeping track of user (agent) access to their resources, enabling features such as prioritized access (e.g., for conflict resolution), resource reservation, etc. Furthermore, since all the aforementioned mechanisms incorporate private user information, e.g., user presence and/or behavior profile, it is vital to guarantee the privacy of the users data, further enabling full control over their data at all times. Putting the described intelligence at the service of users goes then through the establishment of trust within the cyber-physical environment. This becomes of paramount importance in view of both the decentralised character of user interaction with the IoT environment, and the offloading of user and application logic to the cyber-physical agents. In this context, the envisioned trust relationships get a multi-directional nature: users need to trust their surroundings (i.e., applications/platforms), as well as their user agents, and user agents need to develop trust relationships between them; applications/platforms need to mitigate malicious user (agent)

behaviour, but will also need to trust each other so as to enable mobility/migration and/or interoperability.

D. Decentralised security management

In order for the decentralised scheme to work, information ownership and transparency in information handling is a key concept. As we target a local and decentralised interaction of users and IoT platforms/applications, decentralised security management gets to the core of the systems functionality. Therefore, to establish trusted interactions, the following security features are provided: secure user-to-device and device-to-device communications, distributed access control mechanisms, monitoring the behavior of the IoT ecosystem, and user awareness of security. The identity and trust management is build using distributed ledger technologies. This enables the network to dynamically grow and operate without a dedicate trust manager.

V. Conclusion

From its early beginnings, the Internet has been designed as a distributed network of devices called hosts which exchange messages in an asynchronous and logically nonhierarchical manner. This inherent equality and independence of network-connected devices has represented the fundamental building block for the Internet's success and its magnificent adoption in recent decades, advancing it to become a critical infrastructure for all developed societies. Due to their limited capabilities in terms of battery, processing power and communications, in the IoT it has been necessary to isolate the devices from direct global IP network exposure. The interaction with things, which are typically either sensors or actuators, has been channeled via software platforms that offer an abstract resource view to the application developers and end-users. Whereas this paradigm works well for a large number of use cases, the direct interaction of the end users with the things has largely been neglected on a conceptual level. Thereby, it is important to mention that we do not suggest that in a novel paradigm the devices should be directly exposed in the Internet; we rather propose to offer direct access to the devices in their local realm, enabling physical world-type, natural interactions with the increasingly proliferating cyber-physical systems. The proposed decentralization thereby comes along with a number of non-trivial challenges, i.e., device heterogeneity, the need for context awareness, trust management, user-centric resource control and privacy. Additionally, the things should of course still be able to participate in the existing IoT platform ecosystems in parallel, continuing to offer added value to their existing user base. Whereas the outlined challenges may at first seem utopic, there is currently a critical mass of innovation in related science and industry which will enable the foreseen paradigm shift: The existing IoT platforms are federating, enabling greater system flexibility, the distributed ledger technology offers new ways of forming contracts and assuring for system accountability and edge computing enables the migration of heavy computational problems away from low-power devices. Based on these enabling technologies, in the present paper we outline our concept for an interoperable and decentralized IoT of the future, which will offer seamless, local resource usage to the citizens as its users. Importantly, we argue that only decentralized and intuitive-to-use concepts truly empower the citizens in the cyber-physical agora of the future as the common space for their mutual interaction and exchange.

Acknowledgment

This work is supported by the H2020 symbIoTe project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688156. The authors would like to cordially thank the entire symbIoTe consortium for their valuable comments and discussions.

References

[1] M. Alioto, *Enabling the Internet of Things: From Integrated Circuits to Integrated Systems*, 1st ed. Springer Publishing Company, Incorporated, 2017.

[2] S. K. Datta, C. Bonnet, and N. Nikaein, "An iot gateway centric architecture to provide novel m2m services," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, March 2014, pp. 514–519.

[3] J. G. et al., "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[4] L. Atzori, A. Iera, and G. Morabito, "From "smart objects" to "social objects": The next evolutionary step of the internet of things," *IEEE Communications Magazine*, vol. 52, no. 1, pp. 97–105, January 2014.

[5] "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)," *Official Journal of the European Union*, vol. L119, pp. 1–88, May 2016.

[6] I. P. et al., "Towards an IoT framework for semantic and organizational interoperability," in *2017 Global Internet of Things Summit (GIoTS)*, June 2017, pp. 1–6.

[7] M. J. et al., "Semantic interoperability as key to iot platform federation," in *LNCS 10218: Interoperability and Open-Source Solutions for the Internet of Things*, 2017, pp. 3–19.

[8] S. S. et al., "Attribute-based access control scheme in federated iot platforms," in *LNCS 10218: Interoperability and Open-Source Solutions for the Internet of Things*, 2017, pp. 123–138.

[9] S. Popov, "The tangle," *cit. on*, p. 131, 2016.

[10] M. Bottone, F. Raimondi, and G. Primiero, "Multi-agent based simulations of block-free distributed ledgers," 2018.

[11] Y. C. H. et al., "Mobile Edge Computing A key technology towards 5G," European Telecommunications Standards Institute White Paper (2015), 2015.

[12] 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*, ser. MCC '12. New York, NY, USA: ACM, 2012, pp. 13–16. [Online]. Available: http://doi.acm.org/10.1145/2342509.2342513