SCDIoT: Social Cross-Domain IoT enabling Application-to-Application Communications

Yasir Saleem[a], Noel Crespi[a], Pasquale Pace[b]
[a]Institut Mines-Telecom, Telecom SudParis, Evry, France
[b]University of Calabria, Rende, Italy
yasir_saleem.shaikh@telecom-sudparis.eu, noel.crespi@it-sudparis.eu, p.pace@dimes.unical.it

***Abstract*— Achieving global interoperability among IoT systems has become a very real possibility due to the heterogeneity at all levels of IoT. Besides achieving interoperability, it will become very important to establish social relationships and communications among IoT devices (or things), humans and applications. Social relationships in IoT have been realized through the Social IoT (SIoT) paradigm which is one of the trending feature in the IoT. The SIoT is currently consisted of two types of communications: things-to-things and things-to-human communications; in addition, we propose social cross-domain IoT (SCDIoT), a third type of SIoT communication at a global level which enables application-to-application communication in the IoT. Although interoperability allows the exchange and reuse of data among various applications, it does not focus on the social relationships among IoT applications through which those applications can closely collaborate with each other. SCDIoT fills this gap by operating one level above interoperability. It allows collaboration among IoT applications by enabling them to talk to each other, building social relations and benefitting from each other via various useful services, truly exploiting the advantages of interoperability. We present the concept of SCDIoT, its logical framework and some potential use case scenarios, together with the challenges and possible future research directions.**

***Index Terms*— Internet of Things, Social Internet of Things, interoperability, cross-domain applications, application-to-application communication.**

I. INTRODUCTION

The Internet of Things (IoT) provides connection to various network-embedded devices via the Internet [1]. It allows the interaction among devices (e.g., sensors and actuators) dedicated to and deployed for an application to fulfill common objectives. The IoT paradigm is built on three main concepts: things-oriented, Internet-oriented and semantic-oriented. The things-oriented concept deals with smart objects (e.g., sensors and actuators). The Internet-oriented concept allows smart objects to communicate with other objects through various communication technologies (e.g., Z-wave, ZigBee and LoRa) and connects them to the Internet. The semantic-oriented concept deals with applications that are built using smart objects or devices. There are various IoT applications, such as traffic management, weather forecasting, crowd management, smart cities and smart homes, which are automated, thanks to the IoT. However, the main limitation is that such IoT applications are developed in a vertical manner and for a specific use case or scenario. They do not exchange and reuse data among each other due to the lack of interoperability, and therefore they miss the opportunity of providing useful services when combined with the services offered by other IoT applications. Much work is now being focused on achieving interoperability in the IoT [2], paving the way for cross-domain data sharing and reuse among IoT applications.

Moreover, there has been a trending feature of Social IoT (SIoT), which enables social relationships and circles in the IoT. SIoT is the convergence of the IoT with social networks, allowing the intelligent and useful exploitation of the devices used in our daily life. The SIoT has shifted the IoT from a network of connected smart objects to a network of social objects. The SIoT seeks to ensure network navigability for objects, services and resource discovery, as well as to establish trust among objects by considering them as friends, and exploits social networking models in order to solve the issues of interconnected IoT objects [3].

Traditionally, in the SIoT, there are two types of communications: things-to-things communication and things-to-human communication. The SIoT builds profiles using various IoT applications' data which are exchanged within a SIoT network and are accessible to other IoT applications. There are three main aspects in which the SIoT differs from social networks and the IoT. Firstly, the SIoT builds social relationships among things (or objects), rather than exclusively among humans. Human involvement is for the purpose of mediation, but the main tasks are performed by things themselves. Secondly, objects have social relationships with other objects and the IoT; they can perform resource and service discovery by themselves in a distributed and autonomous manner, reducing human efforts. Finally, the SIoT is not mainly dependent on Web technologies, rather it is a social networking services (SNSs) platform that deals with objects instead of dealing only with humans [4].

We propose a third type of communication for the SIoT at a global level which enables application-to-application communication called social cross-domain IoT (SCDIoT). SCDIoT allows collaboration among IoT applications by enabling them to talk to each other, build social circles and relationships among each other, and to benefit from various useful services in order to completely exploit the advantage of interoperability. We have seen the significant benefit of things-to-things and things-to-human communication in traditional

SIoT. With social application-to-application communication, enabled by the SCDIoT, the benefits can increase to many-fold by bridging the gap of IoT applications' isolation. We present the framework and some potential use case scenarios, together with some challenges and future research directions for SCDIoT.

The paper is organized as follows: section II provides an overview and related work on the SIoT. Section III discusses our proposed framework, SCDIoT, together with some potential use case scenarios. Section IV presents some challenges and future research directions, and section V concludes the paper.

II. SIoT Overview and Related Works

A. Overview

The application of social networking concepts to the IoT (i.e., SIoT), initially proposed by Atzori et al. [3], is attracting much attention these days, as it establishes social relationships among smart objects (or things) so that they can collaborate with each other autonomously without human intervention. The motivation behind the SIoT is to enhance the selection, discovery and composition of resources through social relationships and circles among objects in the same manner as in social relationships among humans in a social network [3], [5].

In the SIoT, there may be five types of relationships for defining relationship profiles within an SIoT network: social object relationship (SOR), ownership object relationship (OOR), co-work object relationship (CWOR), co-location object relationship (CLOR) and parental object relationship (POR) [3], [6]. An SOR is established when objects are in direct contact with each other. This direct contact can either be continuous or sporadic and is among the objects' owners (such as devices associated with friends). An OOR is established between heterogenous objects having the same owner. A CWOR is established among objects collaborating with each other to achieve some common goals. A CLOR is established among objects (can be either homogeneous or heterogeneous) that operate in the same environment (such as smart cities, smart buildings and smart homes). CWOR and CLOR are built among objects in a fashion similar to how humans share their public or personal experiences. A POR is built among heterogeneous objects belonging to the same owner/manufacturer having the same period in which the production batch acts like a family.

These relationships are established and updated according to the characteristics of objects (such as battery life, computational power, type and brand) and activities, and are used by resource discovery components to find the objects that can offer the required services (similar to how humans look for friendships and information). Additionally, to manage the relationships, a relationship management component is required by SIoT architecture to enable cognition and intelligence into the SIoT which can allow the objects to establish, maintain and terminate the relationships as needed. These relationships may be built based on several parameters, such as required services, providing connectivity to disconnected objects, a publish-subscribe model and the distance between objects. In this context, Nitti et al., [6] present a scheme of friendship selection in the SIoT to improve information diffusion.

B. Related Works

In the last few years, a large number of research studies have been focused on the SIoT, however, to the best of our knowledge, none of them has focused on social cross-domain IoT. We present the state-of-the-art on the SIoT in this subsection.

An early proposal on building social relationships among objects is provided by Holmquist et al., [7]. It builds temporary relationships using wireless sensor nodes and focuses on how the owners of sensors can control this relationship construction. However, it was a very early work performed in 2001, when both social networks and the IoT were in their infancy stage.

Mendes [8] formulates a proposal to enable objects to participate in conversations similar to those of humans. Such objects should be context-aware and be capable of constructing a network based on the distributed exchanged information, rather than based only on the local information stored on the objects.

Guinard et al., [9] introduce the main convergence of social networks and the IoT in which the social network is a social network of humans exploited by IoT objects as an infrastructure for resource discovery. Similarly, the integration of social networks with the IoT is investigated by Kranz et al., [10] who also present some sample applications. However, this work neither investigates how social relationships can be built nor proposes any solution for the required architecture and protocols.

Kim et al., [11] propose "Socialite", an end-user programming tool for the SIoT, by exploiting semantic technologies. The authors identified eight desired features of the SIoT through an online survey and clustered them into four rule categories which can be programmed by end users. These rules were then used to reason about devices and people in their social circles to support automated decisions at runtime. Socialite uses semantic technologies for knowledge representation and for encapsulating the heterogeneity of devices belonging to different manufacturers. Additionally, Socialite's rules allow for social relationships and collaboration by sharing information and configurations among social circles (e.g., friends).

Girau et al. [12] propose "Lysis", a cloud-based platform for the IoT using SIoT. Lysis offers three main features: objects have social relationships and they behave like autonomous social agents, it exploits PaaS (Platform as a Service) and considers reusability at various layers, and it allows users to have full control over their data. In Lysis, the SIoT is mainly exploited for its first feature, which enables objects to build social relationships in an autonomous manner, offering the advantages of enhancing both network scalability and information discovery.

Colom et al., [13] propose an IoT framework for the collaborative building of behavioral models by using the SIoT. The SIoT is used to support collaborative applications and to build social dimensions by allowing the addition of computing resources by the user without affecting other ongoing activities offered by IoT devices.

Lee et al., [14] propose a game theory-based vulnerability quantification method by using an attack tree for SIoT. This is consisted of three steps: game strategy modeling, cost-impact analysis and payoff calculation. They also present a case study of an SIoT-based network environment. Their approach can serve as a reference for developing a safer SIoT system.

Other works on SIoT focus on modeling and optimization of features selection in Big Data-based SIoT [15], routing protocols based on source location protection [16], robustness management for customization manufacturing [17], SWARM-based data delivery [18], general overviews of 5G-enabled devices [19], IoT platforms for SIoT [20] and recommendation services [21].

III. SCDIoT: Social Cross-Domain IoT

A. Proposed Framework

In this section, we propose the framework of SCDIoT for social application-to-application communication, illustrated in Fig. 1.

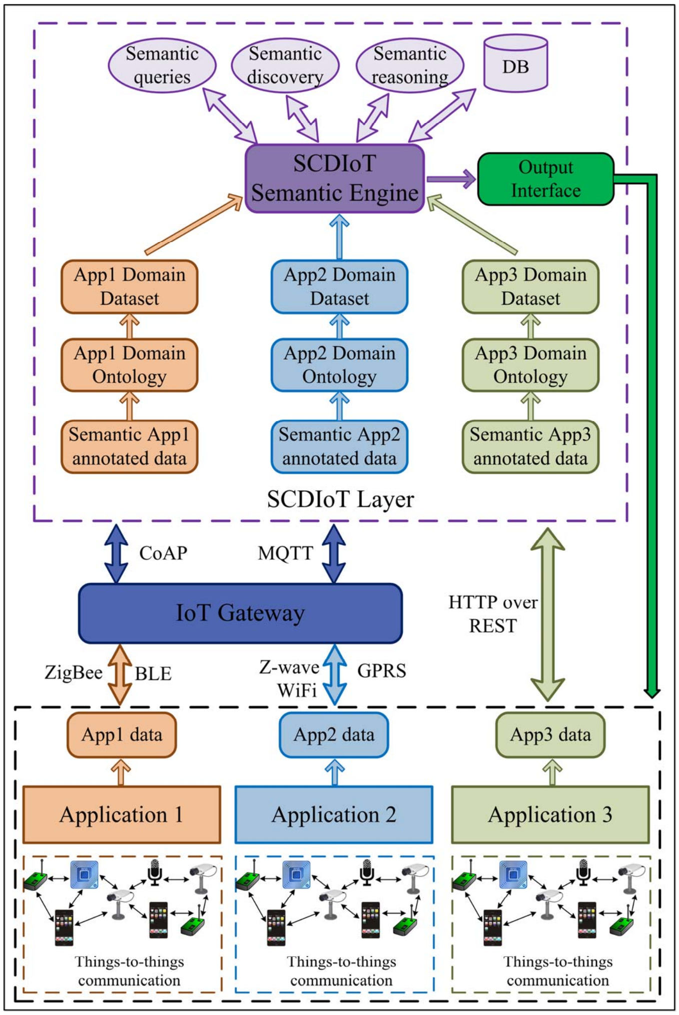

Fig. 1. Proposed framework of SCDIoT.

The three different applications at the bottom of the figure deploy IoT devices (e.g., sensors, actuators, RFIDs, cameras, microphones and smartphones); however, in contrast to the deployment of IoT devices in traditional IoT applications where IoT devices do not talk to each other, these applications (1, 2 and 3) support things-to-things communication in which the devices also talk to each other by having social relationships and circles among themselves enabled by the SIoT. This could be useful in various scenarios, such as in calculating room temperature where various temperature sensors are deployed in a room. Sensors can coordinate and collaborate with each other to correct their measurements. For example, if four temperature sensors are deployed in a room and three of them measure 20 degrees Celsius while one of them measures 4 degrees Celsius; it means that there is a problem with the fourth sensor. Thanks to the collaboration, the fourth sensor will identify this problem and it will either not forward its measurement to the gateway or it will take the measurement again, rectifying the problem. Things-to-things communication supported by the SIoT brings the computing one level lower to edge computing (i.e., from cloud to edge to things-to-things); however, it mainly depends upon the application requirements because if the devices are resource-constrained with limited battery and/or processing power, then things-to-things communication would not be desirable. On the contrary, it could be desirable if devices have direct power and good processing capabilities, e.g., in smart home devices.

Each application collects data from its underlying deployment, and these collected data need to be forwarded to the SCDIoT layer to enable social application-to-application communication. Data forwarding could be achieved through various heterogeneous protocols. In Fig. 1, each application uses a different communication protocol to forward its data. Applications 1 and 2 first transfer their data to the IoT gateway using low power radio communication interfaces such as ZigBee, Bluetooth Low Energy (BLE), Z-wave, GPRS (General Packet Radio Service) or WiFi. The IoT gateway then forwards the data to the SCDIoT layer using any IoT communication protocol such as CoAP (Constrained Application Protocol) or MQTT (Message Queuing Telemetry Transport). Application 3 instead transfers its data directly to the SCDIoT layer through REST APIs, bypassing the IoT gateway.

When the data reaches the SCDIoT layer, it needs to be enriched with semantics in order to achieve interoperability and enable social cross-domain IoT. The first step is to apply semantic annotations to the raw data of heterogeneous applications and domains. Semantic annotation is a very important step in the process of understanding and being able to apply logic (i.e., reasoning) to the applications' data because same data from various applications may have different meaning or different data from various applications may have the same meaning. For example, let's assume that all three applications data are related to temperature measurements. However, if they used their own notations to represent temperature, e.g., 't', 'temp' or 'temperature', it can be understandable by humans but not by machines. Therefore, SCDIoT first applies semantic annotations to describe the data in order to make it understandable by the machines. The second step is to find the appropriate domain ontology of the applications' data. For example, temperature could be either environmental temperature or body temperature which corresponds to completely different domains, e.g., environmental temperature belongs to weather ontology while body temperature belongs to health ontology. After obtaining the relevant ontologies, the next step is to retrieve the most relevant datasets in order to acquire additional knowledge. Once the relevant ontologies and datasets have been identified, SCDIoT links the common concepts (e.g., 't', or 'temp' or 'temperature') to the identified ontologies and datasets using OWL (Web Ontology Language) with equivalent keywords, e.g., `owl:equivalentClass` or `owl:sameAs` respectively. Finally, SCDIoT Semantic Engine performs reasoning over the semantic data using semantic queries and resource discoveries, and then it sends the required and relevant data back to the applications through its output interface.

B. Potential Use Case Scenarios

Social application-to-application communication can be advantageous in a number of use case scenarios. We present some potential use case scenarios below.

Traffic lights are generally operated either using fixed time intervals or based on the road load identified through sensors deployed on the roads. However, with the help of social application-to-application communication, traffic lights can be operated based to some extent on the users' profiles. For instance, a user's smartphone can provide that user's route (e.g., the user is using a navigation system) and this route information can be passed to traffic lights management system which can take into account the user's route and operates accordingly. We propose that traffic light management could be enhanced and become more efficient compared to current traffic lights management systems. Assuming an optimal case, let's consider a road intersection where there are four vehicles, one vehicle on each road, and the driver of each vehicle wants to make a turn to the right. In this situation, if all four traffic signals can turn green, there will be no collision and the drivers will not have to wait. If traffic light management system could communicate with users' navigation system and know the users' routes, it could allow all four turns by switching the traffic lights to green so that drivers can take right turn without any collision, which is otherwise not possible in currently operating traffic lights management systems. This is just a hypothetical case to highlight the usefulness of social application-to-application communication.

One step ahead, we could extend this scenario from traffic light management to traffic crowd management. A traffic crowd management system could consider the users route information and directly communicate with user's navigation systems to distribute users onto different routes to avoid traffic jams. Here, we would have two-way application-to-application communication, i.e., navigation systems provide users' routes information to a traffic crowd management system, the traffic crowd management system considers all the users' routes and communicates back to the navigation systems suggesting a different route with low traffic (in a way that the alternative route does not get congested, and so suggesting different routes to for users) to avoid traffic jams.

Another use case scenario could be food recipe suggestions. This application can consider a user's profile (e.g., his/her food preferences), his/her health constraints (via a health monitoring application), the ingredients currently in the kitchen (through the smart home system) and weather conditions (via a weather monitoring application). Taking into account these three types of applications' data, a food recipe can recommend a recipe to a user which is in accordance with his/her health, is suitable for the current weather, for which the user has all the ingredients available in his/her home, and is according to his/her food preferences. When food ingredients run out of the stock, the smart kitchen can take appropriate actions (e.g., informing the user or ordering by itself) to refill those ingredients.

IV. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

In this section, we discuss the challenges and future research directions in SCDIoT, more specifically in social application-to-application communication.

A. Latency

The biggest challenge in an SCDIoT system is the latency. Since social application-to-application communication is possible through the SCDIoT framework, more latency can be incurred because the data must first be sent to the SCDIoT framework, which does the processing and then sends back the required information to the application. Hence, for delay-sensitive applications (e.g., health and emergency systems), this is a serious challenge which needs to be addressed.

B. Privacy, trust, and security

Privacy, trust and security are major issues in the SCDIoT. Since all the applications data passes through the SCDIoT framework, this presents privacy issues for applications which need to comply with strong privacy policies. Therefore privacy solutions for the SCDIoT must be developed or existing ones adapted to the SCDIoT. Trust is also an important parameter to be considered in order to ensure that each application involved in social cross-domain communication can be trustworthy to avoid malicious behaviors. Finally, security is also a very sensitive issue. The access to cross-domain IoT applications' data can lead to fraudulent activity without a secure technology. Existing IoT solutions for privacy, trust and security could be considered as guidelines while developing solutions for the SCDIoT.

C. Autonomous management

The SCDIoT framework receives applications' data, applies semantic technologies, performs reasoning and makes it shareable with other IoT applications. Therefore, all the operations and management need to be autonomous without human intervention [22]. It would also be desirable if the SCDIoT could learn from its environment and adapt itself according to new emerging requirements. Reinforcement learning could be a very beneficial tool for such self-learning from the environment.

D. Network and storage management

The SCDIoT processes applications' raw data, applies semantic technologies and obtains semantic data, as well as performs reasoning to infer new data. Such data must be securely stored and managed in order to be used in the future for enhanced services. Additionally, it is important to consider how the communication and access to the data and resources will be performed. Therefore, network and storage management is another important issue to be addressed.

E. Proof of Concept

The SCDIoT is a novel concept which needs more exploration and investigation. A proof of concept needs to be developed. We have discussed a few of the challenges that should be carefully considered while developing the proof of concept. New challenges may arise during the actual development of the proof of concept, and these will need to be addressed and incorporated. The relevant works [11], [12], and [20] should be considered as a valid starting point toward the proof of concept implementation.

V. CONCLUSION

The SIoT establishes social relationships among objects in the IoT, supporting two types of communications: things-to-things and things-to-human communication. We have proposed a third type of communication at a global level, i.e., a social cross-domain IoT (SCDIoT), which enables application-to-application communication thanks to social relationships and circles through which IoT applications can closely collaborate with each other. We have presented the basic concept of the SCDIoT, the specific framework that achieves interoperability and social relationships, and some potential use case scenarios together with challenges and future research directions.

REFERENCES

[1] X. Chen, L. Sun, H. Zhu, Y. Zhen, and H. Chen, "Application of Internet of Things in Power-Line Monitoring," In *Int. Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2012, pp. 423–426.

[2] Aloi G, Caliciuri G, Fortino G, Gravina R, Pace P, Russo W, Savaglio C. "Enabling IoT Interoperability through Opportunistic Smartphone-based Mobile Gateways." *Journal of Network and Computer Applications*. 2017, 81, pp74-84.

[3] Atzori L, Iera A, Morabito G, Nitti M. "The social Internet of things (SIoT)–when social networks meet the Internet of things: Concept, architecture and network characterization." *Computer Networks*, 2012, 56(16), pp.3594-608.

[4] Atzori L, Iera A, Morabito G. "SIoT: Giving a social structure to the Internet of things." *IEEE Communications Letters*, 2011, 15(11), pp. 1193-1195.

[5] Nitti M, Girau R, Floris A, Atzori L. "On adding the social dimension to the Internet of vehicles: Friendship and middleware." In *IEEE Int. Black Sea Conf. on Communications and Networking (BlackSeaCom)*, 2014, pp. 134-138.

[6] Nitti M, Atzori L. "What the SIoT needs: a new caching system or new friendship selection mechanism?". In *IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 424-429.

[7] Holmquist LE, Mattern F, Schiele B, Alahuhta P, Beigl M, Gellersen HW. "Smart-its friends: A technique for users to easily establish connections between smart artefacts." In *Int. Conf. on Ubiquitous Computing*, Springer Berlin Heidelberg, 2001, pp. 116-122.

[8] Mendes P. "Social-driven Internet of connected objects." In *Proc. of the Interconnected Smart Objects with the Internet Workshop*, March 2011.

[9] Guinard D, Fischer M, Trifa V. "Sharing using social networks in a composable web of things." In *8th IEEE Int. Conf. on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 2010 Mar 29, pp. 702-707.

[10] Kranz M, Roalter L, Michahelles F. "Things that twitter: social networks and the Internet of things." In *What can the Internet of Things do for the Citizen (CIoT) Workshop at 8th Int. Conf. on Pervasive Computing (Pervasive)*, 2010 May, pp. 1-10.

[11] Kim JE, Fan X, Mosse D. "Empowering End Users for Social Internet of Things." In *Proc. of the Second Int. Conf. on Internet-of-Things Design and Implementation*, 2017 Apr, pp. 71-82.

[12] Girau R, Martis S, Atzori L. "Lysis: A Platform for IoT Distributed Applications over Socially Connected Objects." *IEEE Internet of Things Journal*, 2017 Feb, 4(1), pp.40-51.

[13] Colom JF, Mora H, Gil D, Signes-Pont MT. "Collaborative Building of Behavioural Models based on Internet of Things." *Computers & Electrical Engineering*, 2017, 58, pp.385-96.

[14] Lee S, Kim S, Choi K, Shon T. "Game theory-based Security Vulnerability Quantification for Social Internet of Things." *Future Generation Computer Systems*. 2017, In Press.

[15] Ahmad A, Khan M, Paul A, Din S, Rathore MM, Jeon G, Choi GS. "Toward Modeling and Optimization of Features Selection in Big Data based Social Internet of Things." *Future Generation Computer Systems*, 2017, In Press.

[16] Han G, Zhou L, Wang H, Zhang W, Chan S. "A Source Location Protection Protocol based on Dynamic Routing in WSNs for the Social Internet of Things." *Future Generation Computer Systems*, 2017, In Press.

[17] Song Z, Sun Y, Wan J, Huang L, Xu Y, Hsu CH. "Exploring Robustness Management of Social Internet of Things for Customization Manufacturing." *Future Generation Computer Systems*, 2017, In Press.

[18] Hasan MZ, Al-Turjman F. "SWARM-based Data Delivery in Social Internet of Things." *Future Generation Computer Systems*. 2017, In Press.

[19] Al-Turjman F. "5G-enabled Devices and Smart-spaces in Social-IoT: An overview." *Future Generation Computer Systems*, 2017, In Press.

[20] Afzal B, Umair M, Shah GA, Ahmed E. "Enabling IoT Platforms for Social IoT Applications: Vision, Feature Mapping, and Challenges." *Future Generation Computer Systems*, 2017, In Press.

[21] Saleem Y, Crespi N, Rehmani MH, Copeland R, Hussein D, Bertin E. "Exploitation of Social IoT for Recommendation Services." In *IEEE World Forum on Internet of Things (WF-IoT)*, 2016, Dec, pp. 359-364.

[22] Savaglio C, Fortino G. "Autonomic and cognitive architectures for the Internet of Things." In *Int. Conf. on Internet and Distributed Computing Systems*, 2015, pp. 39-47.