Formulating a Global Identifier Based on Actor Relationship for the Internet of Things

Ausama Majeed, Adil Al-Yasiri

School of Computing, Science, and Engineering, University of Salford
Manchester, UK
a.a.majeed@edu.salford.ac.uk, a.al-yasiri@salford.ac.uk

Abstract. The Internet of Things (IoT) promising a new generation of services been offered to a human being through a world of interconnected objects (called "things") that may use different communication technologies. Objects, in IoT, are seamlessly connected on its owner/user behalf. To offer services, the service providers need to truly identify the effective actor/user rather than the communicated devices. Currently, users have relationships with multiple objects that can also be used to determine their user. These relationships between actors are changeable or may even vanish; however, they are important to distinguish the actual requester of the service. Hence, it is important to consider them when identifying the effective actor of the communicated object. This paper models these relationships, representing them in a general form, and proposes a new semantic identifier format that allows service providers to identify the service requester identity across domains based on those relationships.

Keywords: IoT, Identity, Identifier, Actor Relationship

1. Introduction

The Internet of Things (IoT) represents a technological revolution in the communication and computing fields. The core idea of IoT can be summarised in the sentence "a worldwide network of interconnected entities"[1]. All IoT entities (people, applications/services, and devices) have to be communicated over the Internet. Entities can communicate with each other, either directly or indirectly, oblivious to the underline technology being used. The ultimate goal of these communicated entities is to offer a better service for the human beings. They vary regarding technical specifications, computing and communication capabilities, and deployment fields. Moreover, entities have to be uniquely identified to facilitate entities distinguishing.

To manage and control interaction with those entities, every network domain employs a suitable Identity Management (IdM) system[2]. IdM is considered the cornerstone of the identity lifecycle. The identity is used to describe an entity within a specific context based on the characteristics of this entity, which can be attributed to the entity distinctly in that context. Theoretically, an entity can have several different identity attributes[3]–[5]. IdM processes encompass the management of the entity identities and their authentication, authorization, roles, and privileges and permissions within or across system and enterprise boundaries[6]. IdMs aim to assure that the service provider (SP) will offer services to a trusted requester based on a pre-established

trust relationship with the identity provider IdP to increase enterprises security and productivity.

From a technical point of view, IoT encompasses an enormous amount of connected devices and objects. These devices and objects are interconnected on behalf of other IoT entities (interested parties). For instances, people interact with mobile phones (or tablets), companies' inventory systems interact with RFID (Radio Frequency ID) readers to monitor their assets, insurance companies use telematics devices to monitor the young drivers' behaviour, etc. The interaction requires at least a relationship between two entities. These relationships might not always be static in nature; it could be dynamically established and after a period will be changed or even vanish. One can think of scenarios of how to interact with freely available devices (or things in general) to request services. For example, the interaction between an active RFID tag, which is attached to a rented car, and an electronic toll system reader to pay a parking charge, or many similar scenarios. This means that IoT will change the current ways of interaction with entities from "owner" and "subscriber" to much broader ways such as interact with free devices as discussed in[7]–[9]. However, all IoT entities have to be uniquely identified, hence identifying such relationships has a significant role to the success of the IoT. This is because there are many to many (m:n) interactions between devices in the IoT environment [9] which are communicated on behalf of other entities. The current communications between these IoT things lack the means to identify the relationships. Thus, there is a need for a new identifier format that could lead to identifying the effective entity through its relationship with the IoT communicated device(s). This paper presents an identifier that could be used for global identification of IoT entities that takes into consideration such relationships.

The rest of the paper is organised as follows: Section 2 reviews the state of the art related to IoT identification; Section 3 discusses IoT actors, identify the relationships between them and finally modelling the relationships. These relationships are represented in Global Actor Relationship Identifier format in Section 4, which also includes an example of a typical identifier. Section 5 evaluates the new identifier by comparing the current identifier proposals with the one proposed in this work. Section 6 concludes the paper with references at the end.

2. Related Work

There are several proposals to develop an identifier to use in the IoT environment. These can be summarised as follows.

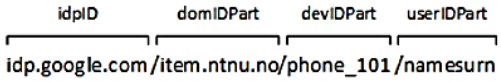
Liu, Yang, & Liu [10] proposed an identifier format used to control the sensor nodes remotely in the IoT. They focused on object identification without considering the owner (or user) identity of that device, nor its relationship with an enterprise (or a real person). Their identifier was composed of a domain identifier, device type and the device identifier using a URL style using 64-bits to formulate their identifier using the format "dev://domain-series/devtype/legacy-name".

Mahalle et. al., [7][11] stated that an entity's identification could be defined by using a collection of three parameters which are: *type*, *identifier*, and *namespace* in which that identifier assigned to the entity. However, the proposal ignores an important parameter which is the Internet connectivity characteristic of the entity. This is because

they built their work on the assumption that all entities with computing capabilities. That means their identification ignores a large community of tiny and low capability objects, which fill the IoT environment. Accordingly, they proposed objects and resources identifier format for IoT, which is composed of a set of permanent or temporary attributes that represent each end-point identification. Object mobility was considered through using a global namespace and local namespace parameters. However, user representation is missing again and in turn, the relationship between the user and the object is missing. The research is limited to the internet protocol (IP) connected devices without considering other communication technologies that use intermediary devices to connect to the Internet.

Batalla et.al. [12] proposed an object/service identifier, which was composed of a chain of all the names, separated by a dot starting from the root; but again it lacked a mention of the users. This identifier was proposed for sensory environments and focused on controlling fixed devices remotely such as controlling a smart home appliance. For example, to communicate with a light on in the first room, a control message could be send using the format (*.floor001.room0001.lightctr*) followed by the control command.

Van Thuan & Butkus [13] proposed an identifier format composed of a set of identities based on URL format. It contained IdP identifier, domain identifier, device identifier, and a user identifier as follows:



This identifier is used to identify the owner of the devices, and the researchers assumed that both of them were registered within the same IdP. Moreover, they only considered devices with computing resources and neglected other devices with low computing capabilities. Again, the research was limited to connected devices with the Internet Protocol and ignored other communication technologies.

Zdravkova [14] proposed an identifier format for the IoT, which was composed of the following parameters: device type, domain identifier, user identifier, and a device identifier as follow: “dtype|gIoTnt|unidomID|unidevID|uniuID”. The identifier used a device type to specify the type of entity that is identified by this identifier; this entity could be a person or device. However, the relationship between user and device was missing again. The domain identifier was used for both the user and the device without considering that they could be different.

As shown from this discussion, a new identifier is required to meet two requirements: firstly, to identify the effective entity that initiated the communication (e.g. a user) which may not be the entity that is connected to the Internet, and secondly to allow dynamic relationships between such entities over the IoT.

3. Actors and Actor Relationships in the IoT

3.1. Actors in IoT

As explained above, the communicated devices are intent to interact with other devices to offer a service to other interested parties. All of them represent actors in the IoT

environment. In our research, we use the *actor* concept of the IoT to refer to widely used terms with different meanings. A number of terms have been utilised in the literature with no clear definitions of these terms. They are entity, object, thing and actor, which are depicted in figure 1. Their meaning is often mixed up and confused by the reader. Therefore, we define them as follows:

- *Entity*: A general term used to describe any identified component in the IoT environment, which has an identity and a set of attributes that describe it. Entities represent a person, a car, a place, an organisation, an application or more that tend to communicate with other entities to send or receive information or control messages.
- *Object*: Any entity that embeds (or attached to) a communication device. The communication device allows entities to communicate with each other and before accessing the Internet. It may use various communication technologies such as Radio Frequency (RF), Near Field Communication (NFC), BlueTooth BT, Wireless Fidelity (WiFi), etc. A person who interacts with a wearable Fitbit or a PC that is not connected to the Internet are examples of the IoT's object.
- *Thing*: An object, which has Internet connectivity. Therefore, the object becomes an active participant in the information network, i.e. a thing, as it is accessible by the Internet and able to share its data with interested parties. The terms "smart object" and "smart thing" are denoting to the same meaning of "thing" [15], [16].
- *Actor*: Represents any entity, object or thing from the IoT environment that interacts with each other to communicate with a (possibly remote) real other object or thing to achieve a goal. The goal could be to monitor, move, manipulate that object, or set/get some interesting information [17], [18].

From the above definitions, all "things" in the IoT are instances of 'entity', but not all entities can become things. For example, a hospital wheelchair, which has a unique identifier to distinguish it from others is an entity in the IoT. To allow this wheelchair become part of the IoT as a thing, it requires having Internet connectivity. By attaching a suitable communication device to the wheelchair, it will be able to communicate within its area using a suitable technology. In the case of using a technology that does not have *Internet Connectivity* (*i.e. IP stack*) such as BT, it is still able to communicate within its domain. In such a case, it will be denoted as an "object". An additional device is used to act as an Internet gateway to connect the wheelchair as an object to the Internet. Next, this object (i.e. the wheelchair with the communication device) has to be accessible by the Internet to call it a "thing" in IoT. By linking it to a patient's smartphone, the wheelchair becomes a thing in the IoT and now can send or receive data through the information network.

From the above scenario, it is clear that there are two relationships: the first relationship is between the wheelchair and the communication device, while the second one is between the communication device and the smartphone being used to access the Internet. These relationships represent interactions between different actors and aim to allow the entity to become a thing in the IoT. Therefore, the wheelchair, communication device, and the smartphone, as an Internet gateway, are represented actors in IoT that have different relationships with each other.

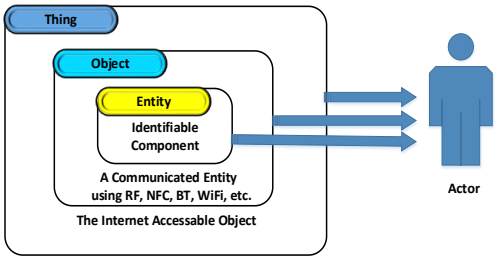


Fig. 1: Entity, Object, Thing, and Actor Demonstration

3.2. Relationship Types between Actors

The IoT things collaborate/interact with each other to serve interested parties that could be a user, a company, etc. Offering the right service requires identifying the actor/user correctly. This interaction could be found between people and their related devices or things, between different communicated devices, between people and applications/services, or between devices and applications/services. Identifying these relationships has a bearing on truly identifying the actual actor of the communicating device(s), as it will lead to offering the right service to a true requester.

Relationships between actors in IoT may be classified into three types as follows:

1. *Permanent relationship*: In this relationship type, objects are collaborated to offer services to only one Actor. Such relationship could be found with patient monitoring devices, personal equipment, etc.
2. *Semi-Permanent relationship*: Objects collaborate to offer services to several actors but one at a time. The relationships have to be pre-established with the actors. The objects need to offer a suitable service for each actor. The automated teller machines and company's assets are examples of this relationship.
3. *Free relationship*: In this case, the objects are collaborated to offer services to any interested actor. No relationship needs to be established with the objects. Using an airport's public personal computer or stores self-check out machines are examples of this relationship.

In the first type of relationship, i.e. a permanent relationship, both of relationship participants have to be able to identify the other party. In other words, each participant has to be linked to the other by precisely registered it with the IdPs. For instance, a patient medical record with a medical centre would be able to attribute a health monitoring device that is attached to the patient and vice versa. Similarly, in the second relationship type, a group of actors has a relationship with a participant. Each participant would be able to attribute the second participant identity and vice versa. However, the free relationship type would not help to identify the relationship participants. This is because it is established without updating the participants' record. Therefore, it could not be used to attribute the identity of the participants.

3.3. Modelling Actor Relationships

As discussed above, the relationships between IoT actors have an essential role to attribute the effective actor of the communicated one. These relationships could be represented as follows.

3.3.1. Definitions

Definition 1. IoT Actor

Let A_{IoT} represents the set of all Actors in the IoT environment.

$$A_{IoT} = \{a_1, a_2, \dots, a_n\} \quad (1)$$

Where,

$\forall\, a_l \in A_{IoT}, a_l = Person \mid Device \mid Application \mid Service;$
$l = 1, 2, \dots, n;\ \ n = total\ number\ of\ things.$

That Actor (a_l) could be a person, a device, an application or a service that interacts with other objects to perform a required task.

Definition 2. Primary Actor

An Actor could be classified into *Primary* or *Secondary* according to the purpose of the communication in IoT. A *Primary Actor (A_P)* represents a subset of A_{IoT} that tend to initiate or consume services with no Internet connectivity. A_P could be defined as follows:

$$A_P \subset A_{IoT} \quad (2)$$

Where,

$\forall\, a_i \in A_P, a_i = entity \mid object;\ i = 1,2, \dots, m;$
$m = total\ number\ of\ primary\ actors$

Definition 3. Secondary Actor

A *Secondary Actor* (A_S) represents a subset of A_{IoT} composed of communication objects (co) being used by an actor (a_i) to perform a required task. Members of A_S could be either object or thing, such as a tag reader, an IoT gateway, a mobile device, a PC, etc.

$$A_S \subset A_{IoT} \quad (3)$$

Where,

$\forall\, co_j \in A_S, co_j = object \mid thing\ ;\ j = 1,2, \dots, p;$
$p = total\ number\ of\ secondary\ actors$

3.3.2. Actor Relationship

A *communication object* (co) can be categorised according to its *Internet Connectivity* (IC) into two types of A_S. The first type is *Active Object*(O_A), which is a (co) with the ability to connect to the Internet (implements the Internet Protocol IP stack), such as a

smartphone. The second type is *Passive Object* (O_P), which is a (co) that does not have Internet connectivity and relies on another O_A member to access the Internet. Typical examples of such objects are a tag (e.g. RFID, BT, or NFC), a body sensor node, application, etc. These O_A and O_P could be defined as follows:

$$O_A = \{co_m : co_m \in A_S \wedge co_m \text{ have the IP stack}\} \quad (4)$$

$$O_P = \{co_n : co_n \in A_S \wedge co_n \text{ does not have the IP stack}\} \quad (5)$$

The *Internet Connectivity* (IC) of A_S members could be defined based on (4) and (5) as follows:

$$IC(co_k) = \begin{cases} Active, & co_k \in O_A \\ Passive, & co_k \in O_P \end{cases} \quad (6)$$

Where,
$\forall\ co_k \in A_S; k = 1,2, \dots, q$

To identify the active actor of any communicated object, in the IoT, the interaction between them is required to be explicitly represented using a relationship. Let an actor relationship, denoted by "AR", represents an interaction of two IoT Actors. The first actor is ($a_i \in A_P$) that interacts with the second actor ($co_j \in A_S$) to allow (a_i) fulfils a required task. The "AR" could be defined as follows:

$$\forall\ a_i \in A_P, \exists\ co_j \in A_S$$
$$AR_{i,j} = \text{Uses}\ (a_i\ , co_j) \quad (7)$$

The $IC(co_j)$ type plays an important role to access the Internet, as previously discussed. Depending on the $IC(co_j)$ we have two cases:

- The *first one* is where the $IC(co_j)$ type is *active*; this means the (co_j) is able to link (a_i) to the Internet directly. Therefore, $AR_{i,j}$, as defined in (7), is able to link (a_i) to the Internet to become part of IoT environment.
- The *second case* is where the $IC(co_j)$ is *passive*, which means the (co_j) is unable to link (a_i) to the Internet directly. Therefore, (co_j) still requires to interact with another *secondary actor*, e.g. ($co_r \in A_s$), to access the Internet. If such a relationship exists between (co_j and co_r) and $IC(co_r)$ is *active,* thus the (a_i) can link to the Internet through a transitive relationship between (a_i and co_r). Then, the *Transitive Actor Relationship* (TR) will show the existence of a relationship between (a_i and co_r), i.e.($AR_{i,r}$), or not.
  Let us assume there exist a ($co_r : co_r \in O_A$), the ($AR_{j,r}$) relationship between $(co_j \in O_P)$ and (co_r) could be defined following the AR relationship in (7) as follows:

$$\text{Let } co_j \in O_P, co_r \in O_A$$
$$Uses\ (co_j\ , co_r) = AR_{j,r} \quad (8)$$

The relationship in (8) represents the interaction between a pair of secondary actors where one belongs to O_P and the other belongs to O_A .

We can now define a *general actor relationship* for the IoT that is composed of *n* Actors using the relationships defined in (6), (7) and (8) as follows:

$$\begin{aligned} &\textit{Let } n = \textit{the number of actors, } n > 1 \\ &\forall\, a_i \in A_{IoT}\,, 1 \le i \le n-1 \\ &AR_{i,i+1} = \begin{cases} Uses\,(a_i, a_{i+1}), & \mathrm{n} = 2, a_{i+1} \in O_A \\ 0, & n = 2, a_{i+1} \in O_P \\ Uses\,\left(a_i, AR_{i+1,i+2}\right), & Ohterwise \end{cases} \end{aligned} \tag{9}$$

4. Global Actor Relationship Identifier Format

Identity means something that describes an "entity" accurately to distinguish it from other entities in a domain. An *identifier* is a way that represents this "entity" by using a series of numbers, characters, or a combination of them, which is meaningful in a specific domain (namespace). The *namespace* represents the application area of the "entity" identifier and can be used to distinguish it from others. The Identity Provider system (*IdP*) is responsible for issuing, assigning, and managing the entity's identifier within a namespace.

Representing the identity of an "actor" in IoT requires an identifier that contains sufficient information to identify it at any visited domain across its registration one. As discussed in section 2, the identity parameters proposed by Mahalle et. al. are insufficient to identify neither tiny actors nor actors across their namespace (domain). To resolve this limitation, the identity of an actor is extended to four parameters instead of three by considering the actor's Internet connectivity. In addition to minor modification of *namespace* parameter to be *IdP* name to facilitate the identity verification process across domains. A new identifier format is developed based on our identity parameters to build the actor identity for the IoT. These parameters are *Type, Internet Connectivity, Identifier* and *identity provider* of the domain that assigned this identifier to the actor. Although it seems obvious, it is important to note that actor with active Internet connectivity can only be of a device actor type as it represents the communication device. Thus, the Identity of an Actor is represented as follows:

$$\begin{aligned} &\forall\, a_l \in A_{IoT} \\ &Identity(a_l) = \{T(a_l), IC(a_l), Id(a_l), IdP(a_l)\} \end{aligned} \tag{10}$$

Where,

$\boldsymbol{T(a_l)}$ Represents the ***actor's type***, as defined in (1);

$\boldsymbol{IC(a_l)}$ Represents the ***actor's ability to access the Internet***, as defined in (5);

$\boldsymbol{Id(a_l)}$ Represents the ***identifier*** that is assigned to (a_l) by the IdP;

$\boldsymbol{IdP(a_l)}$ Represents ***the domain's identity provider*** in which the identifier is assigned to (a_l);

To formulate a *Global Actor Relationship Identifier* $(GARI)$ we have to re-represent the general actor relationship, which is defined in (9), in a way that is able to

show the actor identity parameters defined in (10). Thus, we propose the following ($GARI$) format that is composed of three main parts as follows:

- *Actors_Relation_Specifier,* which is used to specify the characteristics of the relationship participants. These are firstly, the type of (a_i) as it defined in (1). Secondly, $IC(a_j)$ to determine the way of contacting (a_i). Thirdly, (TR) to specify the existence of a transitive actor relationship when $IC(a_j)$ is *passive*, as discussed in (8). Finally, the relationship type, as discussed earlier in 3.2, which will allow the *SP* to decide whether the $IdP(a_j)$ will query to verify the (a_i) identity or not.
- $Identification(a_i)$, it is used to specify the identifier of (a_i) and the $IdP(a_i)$ that assign this identifier.
- $Identification(a_j)$, it could be represented in two forms according to the $IC(a_j)$ type in the first part. The first form is similar to the second part to represent the identification of (a_j) when the $IC(a_j)$ type is *active*. Whilst, the second form is to represent the additional actor relationship (if existent) when the $IC(a_j)$ type is *passive.*

The ($GARI$) format is defined as follow:

$$GARI = \{Actors\_Relation\_Specifier, Identification(a_i), Identification(a_j)\} \quad (11)$$

Where,

$a_i \in A_P \subset A_{IoT}; a_j \in A_S \subset A_{IoT}$;

$$Actors\_Relation\_Specifier = \{T(a_i), IC(a_j), TR, T(AR_{i,j})\} \quad (11.1)$$

$$Identification(a_i) = \{IdP(a_i) : Id(a_i)\} \quad (11.2)$$

$$Identification(a_j) = \{IdP(a_j) : Id(a_j)\} \quad (11.3)$$

$GARI$ contains all the required information that will facilitate identifying the effective actor by the *SP* as the end point of service request. Thus, the *SP's* confidence of offering their services to the right requester will be improved by involving more *IdPs* in the requester identification process based on the relationship type.

To illustrate the actor relationship, in $GARI$, of an entity in IoT, let us consider the wheelchair scenario, discussed earlier in section 3.1 as an example. In this scenario, shown in figure 2, there are three actors (a primary actor and two secondary actors) and two relationships. The first relationship ($AR_{1,2}$) is between the wheelchair as a primary actor and the BT communication device attached to it. However, $AR_{1,2}$ is unable to access the Internet as $IC(a_2)$ is *passive*. Thus, the second relationship is needed to link the wheelchair to the Internet. The second relationship ($AR_{2,3}$) is between the BT device and the smartphone with WiFi technology to access the Internet. Although the $IC(a_2)$ is *passive*, it is obvious that the TR does not exist between (a_1) and (a_3). To allow the wheelchair to be uniquely identified in the IoT, we have to compose a *GARI* identifier based on these relationships.

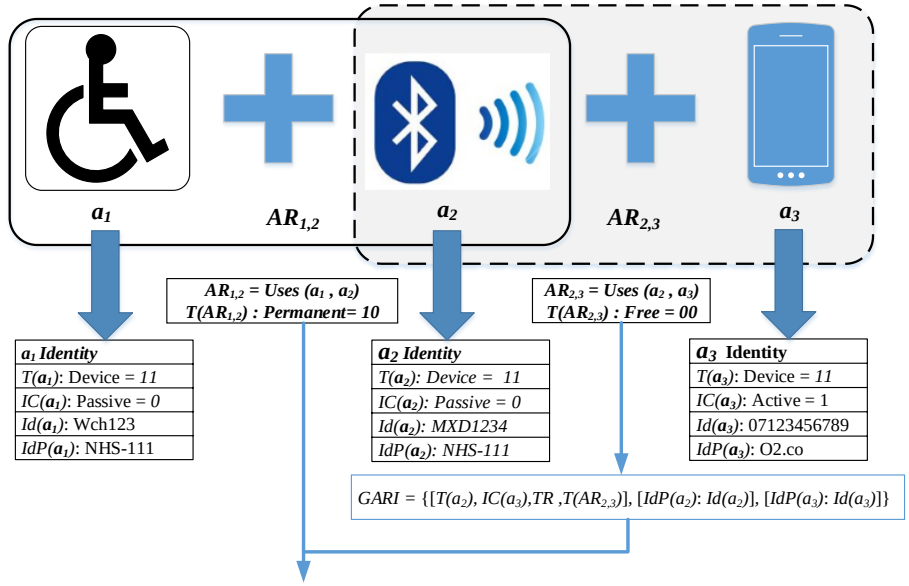


Fig. 2: An example of $GARI$ Composing

As shown in figure 2, the receiver of the $GARI$ message can recognise that the effective actor of this communication is a *passive* device (the 0 value in IC field) and the two relationships between the three actors. Moreover, the *NHS-111* is the only *IdP* that could be used to identify the effective actor because of its permanent relationship type and inexistence of a transitive relationship to use the $IdP(a_3)$. This way, $GARI$ helps the receiver to identify the effective actor.

5. Evaluation

Identifying the effective actor of a communicated device across domains in an open environment like IoT is still an issue facing *SPs*. This is because the nomadic nature of the IoT entities that can freely join and leave different *SPs* to get their services. To solve this problem, *SPs* need a new identification method that can seamlessly interoperate with external *IdP*s based on dynamically establishing trust relationships to identify the actor's identity. This method might improve the *SPs* interoperability as the IoT is a huge community of entities and identifying them requires more dynamic and scalable method. This method requires a special identifier format that contains sufficient information, which is what we focused on in this paper. However, this is a work in progress, and more work is underway to develop an identification method and protocol before the format is thoroughly tested. In this section, we evaluate the proposed format based on its perceived benefits in comparison to other identifiers.

The comparison between existing identifier proposals and $GARI$ is presented in table 1. The table shows that almost all of the proposals encompass the *device identifier* and the *IdP (or domain namespace)* information. However, all existing proposals lack any information related to the *user type* of the communicated device. In addition, none has considered the *user-device relationships,* which we believe to be essential in identifying the effective actors. By specifying these relationships in $GARI$, *SPs* will be able to identify the *IdPs* to be used in the identification of the effective actor, based on the *relationship type* and the *transitive actor relationship* existence. Moreover, all existing methods ignored *Internet Connectivity* of the entities, assuming all devices able to access the Internet. Thus, existing identifiers are unable to identify passive objects globally in comparison with $GARI$.

To sum up, existing proposals fail to distinguish between primary and secondary actors. In other words, it will not be possible for connected parties to make a distinction between those who make a connection on behalf of others. In comparison, GARI makes it possible to use relationships between actors and cross-domain information to identify such entities.

Table 1: State of the art of Identifiers Comparison

Criteria	Liu & Liu	Batalla	Mahalle & et. al.	Thuan & Butkus	Zdravkova	GARI
User type						✓
Device type	✓			✓	✓	✓
User-device relationship						✓
User identifier			✓		✓	✓
User domain / IdP			✓		✓	✓
Device identifier	✓	✓	✓	✓	✓	✓
Device domain / IdP	✓		✓	✓	✓	✓
Mobility/cross-domain support			✓	✓	✓	✓
Internet connectivity						✓
Ability to identifies passive objects						✓

6. Conclusion

The IoT is a technology revolution that will change the relationships between interconnected entities. Identifying these relationships has a direct impact on the identification of the effective actor of the communicated object. The Internet connectivity of the communication object leads identifying its ways to access the Internet as it might require establishing an additional relationship when the object is passive. This will allow a broad range of tiny and passive objects to be part of the IoT and recognise them globally by following these relationships. Although previous work has used multiple parameters to identify these entities, such parameters are insufficient to fully describe how entities collaborate to establish a connection to the Internet. In this work, we argued that the identity of entities in IoT could be sufficiently established based on the existence of four parameters: type, Internet connectivity, identifier and the Idp. Therefore, to identify the entities globally in IoT we need to represent these relationships and all other required information in a semantic identifier format. The

relationships in the IoT are defined and modelled in this research and then represented in a new identifier format (called GARI), to solve this issue. Further work is underway to develop a new identification method and a protocol that will be used to verify the identity of the effective actor of communicated devices across-domains.

References

1. Roman R., Zhou J., and Lopez J.: On the Features and Challenges of Security and Privacy in Distributed Internet of Things. Com. Netw. 57, 10, 2266--2279, (2013)
2. Fongen A.: Identity Management and Integrity Protection in the Internet of Things. In: 3rd International Conference on Emerging Security Technologies. 111--114, IEEE Press, (2012)
3. Alpár G., Hoepman J.-H., and Siljee J.: The Identity Crisis. Security, Privacy and Usability Issues in Identity Management. arXiv Prepr. arXiv1101.0427, (2011)
4. Angin P., Bhargava B., Ranchal R., Singh N., Linderman M., Ben Othmane L., and Lilien L.: An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing. In: 29th IEEE Symposium on Reliable Distributed Systems. 177--183, IEEE Press, New Delhi (2010)
5. Jøsang A, Golbeck J.: Challenges for Robust Trust and Reputation Systems. In: Proceedings of the 5th International Workshop on Security and Trust Management (SMT 2009). Saint Malo, (2009)
6. Yeluri R, Castro-Leon E.: Identity Management and Control for Clouds. In: Building the Infrastructure for Cloud Security. 141--159, Apress, (2014)
7. Mahalle PN, Railkar PN.: Identity Management for Internet of Things. River Publishers, Denmark, (2015)
8. Gartner: The Identity of Things for the Internet of Things - (G00270277). (2015)
9. Forgerock: Whitepaper: The Identity of Things (IDoT): Access Management (IAM) Reference Architecture for The Internet of Things (IoT). (2015)
10. Liu CH, Yang B, Liu T.: Efficient Naming, Addressing and Profile Services in Internet-of-Things Sensory Environments. In: Ad Hoc Networks. 18, 85--101, (2014)
11. Mahalle PN, Prasad NR, Prasad R.: Novel Context-Aware Clustering with Hierarchical Addressing (CCHA) for the Internet of Things (IoT). In: 5th International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2013). 267--274, IET, Bangalore (2013)
12. Batalla JM, Krawiec P.: Conception of ID Layer Performance at the Network Level for Internet of Things. Per. and Ubiq. Comp. 18(2), 465--480, (2014)
13. Thuan D. V., Butkus P.: A User Centric Identity Management for Internet of things. In: International Conference on IT Convergence and Security (ICITCS). 1--4, IEEE Publisher, Beijing (2014)
14. Zdravkova V.: Identity Management Approach in Internet of Things. Aalborg University (2015)
15. Vujovic V, Maksimovic M, Kosmajac D, Perisic B.: Resource: A Connection Between Internet of Things and Resource-Oriented Architecture. In: Proceedings of Smart SysTech 2015; European Conference on Smart Objects, Systems and Technologies. 1--7, VDE Publisher, Aachen, Germany (2015)
16. Bello O, Zeadally S.: Intelligent Device-To-Device Communication in the Internet of Things. 99, 1--11, IEEE Syst J. (2015)
17. Serbanati A, Medaglia CM, Ceipidor UB.: Building Blocks of the Internet of Things: State of the Art and Beyond. INTECH Open Access Publisher (2011)
18. Bassi A, Bauer M, Fiedler M, Kramp T, Van Kranenburg R, Lange S, Meissner S. Enabling things to talk. Designing IoT Solutions with the IoT Architectural Reference Model. 163--211, Springer Heidelberg (2013)