A New Dynamic Smart-AC Model Methodology to Enforce Acess Control Policy in IoT layers

Nadine Kashmar*, Mehdi Adda
Département de Mathématiques, Informatique et Génie
Université du Québec à Rimouski
Rimouski, Québec
kasn0002@uqar.ca*, mehdi_adda@uqar.ca

Mirna Atieh
Business Computer Department, Faculty of Economic Sciences and Administration
Lebanese University
Hadat, Lebanon
matieh@ul.edu.lb

Hussein Ibrahim
Institut Technologique de Maintenance Industrielle (ITMI)
Sept-Îles, Québec
hussein.ibrahim@itmi.ca

***Abstract*—Internet of Things (IoT) is the conversion of everyday tangible devices or machines to smart objects. This means that these objects would be able to think, sense and feel. For example, your home devices will be able to detect and feel your absence to turn off the lights of empty rooms, close doors, lock the gates, and other tasks. Thus, would it be acceptable to find intruders who might mess up your daily life style or control your home appliances? Absolutely not! The same idea for factories, they definitely reject to detect any unacceptable access from any foreigner to their logical/physical assets or machines who might be able to locally or remotely control, for example, any machine operation. This would cause a significant loss for their reputation or investments, since any vulnerability or attack can produce, for example, fault products. So far, IoT is considered as one of the most essential areas of future technologies, especially for the industries. Hence, finding an environment full of smart devices needs a smart security methodology to prevent any illegal access. In this domain, various researches are conducted to find Access Control (AC) models to enforce security policies that prevent any unauthorized detection of sensitive data and enable secure access of information. For this purpose, we present a new dynamic Smart-AC model methodology to enforce security policy in IoT layers.**

Keywords-IoT; access control; smart; security; model; policy

I. INTRODUCTION

In literature various Internet of Things (IoT) definitions are provided due to the integration of different technologies. The significant amount of IoT definitions can be summarized as a huge number of objects and devices with different technologies and platforms that are connected to the internet via heterogeneous networks (3G, LTE, WiFi, ZigBee …). Figure 1 illustrates this definition. It is the integration of several technologies, such as wired and wireless sensor networks, identification and tracking technologies, communication protocols shared with the next generation internet, and distributed intelligence for smart objects [1].

The big question in IoT is how to allow a variety of objects, such as PCs, mobile phones, sensors, etc. to interact and cooperate with each other transparently and securely to attain certain tasks related to consumers, companies or industry sectors. In this domain, the main concern for them is to keep their zone of interconnected devices and which are connected to the internet, secure, private and controlled only by them. Thus, finding an environment full of smart devices needs a smart security methodology to prevent any illegal access and enforce policy and security requirements. In this paper, we tackle IoT security and Access Control (AC) related issues and present a new methodology to enforce AC policy in different IoT layers.

The paper is organized as follows: section II briefly presents IoT limitations and challenges. Section III summarizes the existing AC models for IoT. The architecture of IoT layers and our methodology of integrating Smart-AC model in IoT are explained in section IV. Section V concludes this paper and presents future perspectives.

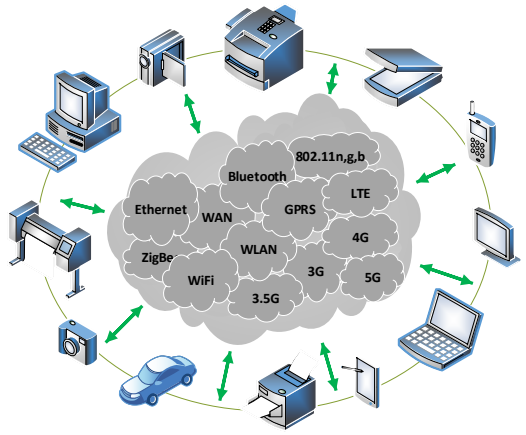

Figure 1. Heterogeous IoT platforms, devices and internet networks

II. IOT LIMITATIONS AND CHALLENGES

The IoT is penetrating a wide range of domains including cities, homes, industry, healthcare, appliances, and much more, to make everything smart, adaptable and easy. In each area there are various opportunities and challenges. For this purpose, different plans are conducted, various applications are developed, and different software and hardware technologies are cooperatively used. The core

player in IoT technologies are the wireless technologies, where sensor networks play a critical role for linking the physical world with the digital world. For example, e-health applications, environmental monitoring (temperature, plants, weather), intelligent transportation systems, etc.

Although IoT is a popular topic, many challenging problems still need to be addressed, specially the technological and social aspects, before being the IoT idea widely accepted. The IoT challenges can be summarized under the following categories: free internet connectivity, security and all related issues, acceptability among the society, storage and computational ability, scalability, and power consumption [2, 3]. Among other challenges that are also mentioned in [4] we have: data management challenge, data mining challenge, privacy and security challenge, and chaos challenge. All these challenges and limitations open wide research issues, suggestions, methodologies, architectures, and others to address each of them. Since all IoT devices are connected to the internet, they are vulnerable to attacks and security threats. Hence, the core concern is the importance of finding methods to enforce AC policies to prevent any untrusted access and control access to the resources. Accordingly, the acceptance or rejection of this technology is determined by security and privacy.

III. Related Work

The challenging IoT heterogeneous environments of interconnected networks and distributed systems, the heterogeneity of platforms and applications, and the diversity of users, force the necessity to design a well coherent AC architecture to enforce AC policy and administer security features in IoT. In this context, several IoT authentication and AC methods are offered by researchers to integrate security features with this technology from two or more AC models. The most famous AC models that are presented comprehensively and reviewed in literature are: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC), Organization Based Access Control (OrBAC), and Attribute Based Access Control (ABAC) [5-7].

However, Ouaddah et. al in [8] propose SmartOrBAC AC framework for IoT environment. It is based on OrBAC, but due to some OrBAC limitations, it is coupled with the RESTFUL web services mechanisms due to its preferability for the low power constrained environment. The result is the use of web service technologies to implement secure collaboration between organizations. The basic AC requirements in IoT are analyzed by Hussein et. al in [9]. The summarized AC requirements are thin clients and server architecture, autonomous and self-contained AC, infrastructure integration, and attributes centric AC. However, authors adopt the community-based AC architecture (COBAC) to administer the AC in IoT, as a solution for these requirements. IoTCollab framework is developed by Adda et. al in [10], its aim is to ease the collaboration and data sharing in IoT. Based on IoTCollab, an extended study of RBAC and ABAC models are proposed in [11] to manipulate the security concerns of a data sharing framework. A collaborative RBAC (CollRBAC) and collaborative ABAC (CollABAC) models are described. Then, CollRBAC and CollABAC are compared in the light of IoT and IoTCollab requirements. Moreover, a model to find a secure communication between things is proposed by Liu et al. [12]. The main idea is to verify identities between two IoT devices by implementing authentication protocol in the presentation layer where identification key establishment occurs. For Authorization, authors adopt RBAC's authorization concept, implement Elliptic Curve Cryptosystem (ECC) for secure key establishment. A smart contract-based framework is proposed in [13] to implement distributed and trustworthy AC for the IoT by applying smart contract-enabled blockchain technology. It contains: multiple Access Control Contracts (ACCs), one Judge Contract (JC), and one Register Contract (RC). For AC between subjects and objects, ACCs are implemented. To judge the unpleasant behavior of a subject during the AC, JC is used. To manage the ACCs and JC, RC is used. In this context authors address different case studies to demonstrate the feasibility of the framework. As well, some researches address the different layers of IoT architecture, then propose an AC model. Authors in [14] mention that, even there is no consensus on a wide IoT architectures, they are generally comprised of three main components: an object layer, a middle layer(s), and an application layer. The difference between these architectures relies in the middle layer(s). Hence, authors propose a cloud-enabled IoT with four-layer AC Oriented (ACO) architecture which are: an object, a virtual object layer, a cloud service layer, and an application layer. Their purpose is to establish a framework to find AC models for cloud enabled IoT.

However, none of the proposed AC models encompass a general structure or methodology. Each model addresses certain case and implemented based on some features of different models (RBAC, OrBAC …), knowing that these models have limitations and deficiencies [5]. Also, none of them consider the continuous technological changes, and it is built for specific IoT architecture or structure. Thus, two key points inspire us to develop a smart AC methodology which can be implemented to find a Smart-AC model:

- The first is the word "SMART". While we think about IoT, we think about the smart objects which are able to sense and communicate within the IoT environment. Hence, we come up with the idea of a "Smart Access Control model".
- The second is the term "HETEROGENEOUS". As we know, IoT world is heterogeneous, starting from the devices, types of networks, platforms, reaching to the applications. As presented in literature, there are various AC models implemented from two or more AC models, for various cases and studies, and they are also heterogeneous. Thus, finding a Smart-AC model that is capable to include all AC features and can be dynamic enough to be implemented in any IoT environment becomes our objective.

The aim is to find a general and dynamic AC model structure which allow building other AC models to enforce AC policies in IoT, regardless of its architecture and type of application (smart home, smart industry …). For example, in

the field of smart industry or industrial IoT, the new factories of electricity rely on IoT applications. Any intrusion for such applications can cause hazardous consequences, such as cutting off the power for hospitals, ministries and even cities.

IV. IoT Architecture and the Proposed Smart-AC Model Methodology

A. *IoT Layers*

In [13], authors mention that there is no consensus on a wide IoT architecture. In this context, [3, 14-16] state that IoT architectures, are generally comprised of three components: 1) the object or the perception layer, 2) the middle or network layer(s), and 3) the application or presentation layer (Figure 2). The object layer contains Internet-enabled devices (cameras, sensors, …) to gather and exchange information with other devices through the Internet. The middle layer works as agent to transfer the collected data from an object layer to a specific destination in the application layer. In this layer, different network communication technologies are used for this purpose, such as Bluetooth, ZigBee, WiFi, 4G, etc. The application layer is where information is received and processed. Also, it is proposed that in some IoT architectures, the middle layer consists of two layers: the network and the service layers. Similarly, in some other researches it is proposed that the middle layer consists of three layers: object abstraction, service management, and service composition layers.

B. *Smart-Access Control Model features and methodology*

Various AC models are presented in literature, MAC, DAC, RBAC, etc. each model is developed either to overcome some limitations found in preceding models or as a solution for a specific use case and application. Moreover, some other AC models have some combined features from some models to enhance some service features. Hence, our aim is to find a Smart-AC model with the following features:

- Generic enough to include all features offered by the existing AC models.
- Serves as a basis for specifying any AC policy.
- Eases the migration from an AC model to another.
- Handles multiple AC models and find advanced security features and operations.
- Works as a guard to restrict accesses starting from the physical locations reaching to the end user.
- Dynamic enough to handle the diverse needs, use cases, and applications for AC especially with the rapid propagation and evolution of information technologies (cloud computing, IoT …), and others.

The features of each AC model are summarized in [5]. DAC model includes three key components: a set of objects, a set of subjects, and a matrix. AC rights of subject(s) over object(s) are specified and represented as Capability Lists (CLs) and AC Lists (ACLs), which are represented as a matrix. In MAC, AC policy is managed in a centralized way, where security levels are associated with each subject and object, then permissions and actions are derived. As an alternative for DAC and MAC, RBAC model is developed, where users can be assigned some roles and a role can be associated to many users, and a role is a group of rights to use some object(s). OrBAC model is implemented to overcome some of the limitations in DAC, MAC and RBAC, and to find a more abstract control policy.

However, Figure 3 shows our vision for a Smart-AC model with the above mentioned, and AC models features. It illustrates the features and parameters for all models (subjets, objects …) with the ability to define new ones (e.g. X, Y …) and find the needed mappings and associations between each model entities. Thus, any AC model can be developed by combining features from the existing models, in addition to the ability to add or define new ones. Hence, various models can be implemented, migrated, and used dynamically to enforce AC policy based on the needed security requirements. In IoT, this approach is practical, due to its dynamicity and ability to be upgraded based on the continuous technological changes. Hence, the dynamic and generic properties of such model, if implemented, 1) will help constructing new AC models based on a general AC

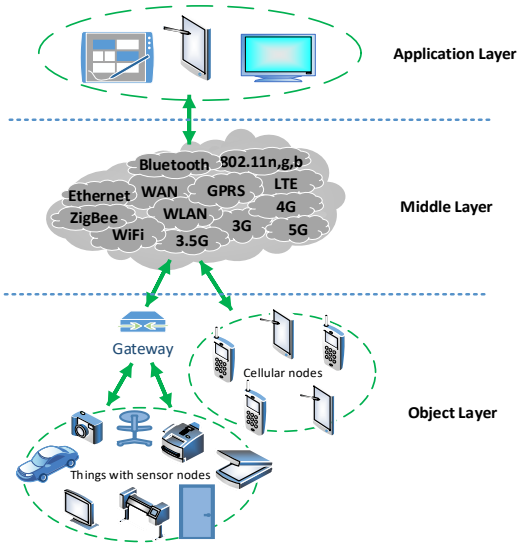

Figure 2. General IoT Layers

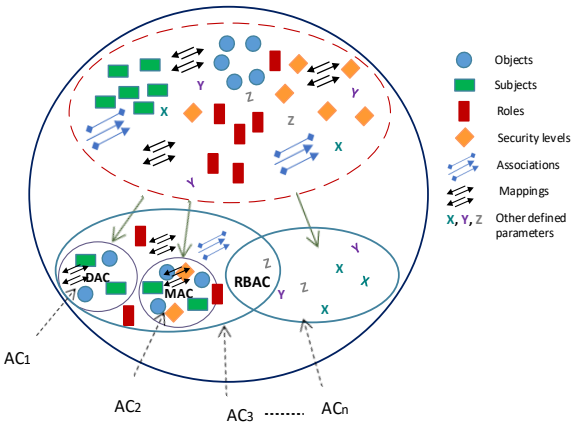

Figure 3. The vision of Smart-AC model

model concept. 2) Migrating AC policies from one model to another will also help companies or industry sectors reduce the complexity and cost in this domain. 3) Different AC models can cooperate within the same company and this would be effective for IoT applications.

Each IoT layer needs the integration of AC model(s) to enforce AC policy and find secure communication environment. Various access types might exist in each IoT layer, based on the existing objects and subjects, and the needed security requirement to deny any illegal access and determine who can access what and when. Based on general architecture of IoT layers and our illustrated vision for the Smart-AC model, Figure 4 shows how any AC model can be combined with IoT layers (AC1, AC2, … AC_n...), which is derived/defined from the smart-AC model.

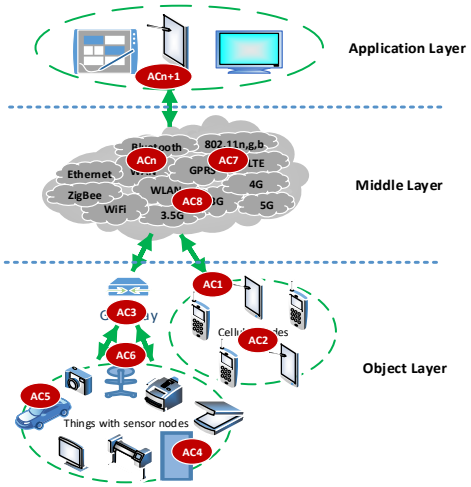

Figure 4. The vision of Smart-AC model

V. Conclusion and Future Perspectives

IoT is an emerging phenomenon, since various technologies and applications are combined to find a real intelligent world. Finding a secure IoT environment is a challenging issue. Various AC models are presented in literature to enforce AC policy in IoT, but they lack the idea of being upgradable or dynamic to follow the progression of technological changes and upgrades. For this purpose, we present the headlines of new methodology to define a generic Smart-AC model, its concept is dynamic enough to define other AC models based on the needed security requirements. As future perspective, our aim is to define the presented headlines, of this paper, as a formal steps or guidelines and develop a general structure of the proposed methodology. Also, we will consider Industrial IoT (IIoT) or Industry 4.0 as an example to implement our methodology.

Acknowledgment

We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) and Fonds Québécois de la Recherche sur la Nature et les Technologies (FQRNT).

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787-2805, 2010.

[2] S. C. Mukhopadhyay and N. K. Suryadevara, "Internet of things: Challenges and opportunities," in Internet of Things: Springer, 2014, pp. 1-17.

[3] K. Ahmad, O. Mohammad, M. Atieh, and H. Ramadan, "IoT: Architecture, Challenges, and Solutions using Fog Network and Application Classification," presented at the 19th International Arab Conference on Information Technology (ACIT 2018), Lebanon, Nov. 2018.

[4] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, vol. 58, no. 4, pp. 431-440, 2015.

[5] N. Kashmar, M. Adda, and M. Atieh, "From Access Control Models to Access Control Metamodels: A Survey," the Future of Information and Communication Conference (FICC) 2019, US, San Francisco, March 14-15, 2019. accepted

[6] V. C. Hu, D. F. Ferraiolo, R. Chandramouli, and D. R. Kuhn, Attribute-Based Access Control. London: Artech Hous, 2018.

[7] M. Ennahbaoui and S. Elhajji, "Study of access control models," in Proceedings of the World Congress on Engineering, 2013, vol. 2, pp. 3-5.

[8] A. Ouaddah, I. Bouij-Pasquier, A. A. Elkalam, and A. A. Ouahman, "Security analysis and proposal of new access control model in the Internet of Thing," in 2015 international conference on electrical and information technologies (ICEIT), 2015, pp. 30-35: IEEE.

[9] D. Hussein, E. Bertin, and V. Frey, "Access control in IoT: From requirements to a candidate vision," in 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), 2017, pp. 328-330: IEEE.

[10] M. Adda and R. Saad, "A data sharing strategy and a DSL for service discovery, selection and consumption for the IoT," Procedia Computer Science, vol. 37, pp. 92-100, 2014.

[11] M. Adda, J. Abdelaziz, H. Mcheick, and R. Saad, "Toward an access control model for IOTCollab," Procedia Computer Science, vol. 52, pp. 428-435, 2015.

[12] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and access control in the internet of things," in 2012 32nd International Conference on Distributed Computing Systems Workshops, 2012, pp. 588-592: IEEE.

[13] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," IEEE Internet of Things Journal, 2018.

[14] A. Alshehri and R. Sandhu, "Access control models for cloud-enabled internet of things: A proposed architecture and research agenda," in 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), 2016, pp. 530-538: IEEE.

[15] S. Talari, M. Shafie-Khah, P. Siano, V. Loia, A. Tommasetti, and J. Catalão, "A review of smart cities based on the internet of things concept," Energies, vol. 10, no. 4, p. 421, 2017.

[16] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645-1660, 2013.