Annotated Bibliography Access Control for Internet of Things

**Adda, M., Abdelaziz, J., Mcheick, H., & Saad, R. (2015). Toward an access control model for IOTCollab. *Procedia Computer Science*, *52*, 428-435.**

The authors of this article realize the new interconnectedness possibilities that are fostered by IoT. Similarly, they agree with the other authors whose work is reviewed in this paper that authorization and access control forms a focal part of the IoT. As such, as a way of contributing to the knowledge on access and control of IoT, they have proposed a study of role and attribute–based access control frameworks. Their proposed framework is aimed at countering the security concerns of their previously developed data sharing frameworks. The authors cite role based access control (RBAC) as the predominant framework for advanced access control schemes. They indicate that this model was designed to counter the limitations of the traditional access control frameworks.

They also define RBAC and task based access control. They then proceed to evaluate the features of an access control model including scale, massive amount of data, self-organized, minimal energy consumption, just to name but a few.Subsequently, they illustrate the functioning of the CollRBAC and CollABAC, as their two proposed models, and assess them using relevant criterion. Just like Ouaddah et al, (2017), the authors of this article have provided a detailed comparison study of authorization mechanisms. They have described the requirements for internet of things collaboration, and accessed two models in light of internet of things and IOTCollabo. However, their study was not conclusive. Keeping in mind the resource constrained nature of the IoT devices; they intend to conduct further tests in order to ascertain the effectiveness of their two models. Yet, this article is informative on various issues, definitions, and concepts used in designing a model for IoT. It is therefore important in demystifying the literature presented in the papers discussed below.

**Cruz-Piris, L., Rivera, D., Marsa-Maestre, I., de la Hoz, E., & Velasco, J. R. (2018). Access Control Mechanism for IoT Environments Based on Modelling Communication Procedures as Resources. *Sensors*, *18*(3), 917.**

In this article, the authors recognize that among the major challenges of Internet of things is to acquire a safe and uncomplicated access control system for the services provided by the internet of things. The authors thus propose incorporating the IoT devices in access control system, which is designed for web-based services. This would be achieved by modeling various IoT communication aspects as resources. The main aim of the study is to achieve an integrated access control system for assorted devices. This objective would be achieved by modeling the dominant elements that make up a message exchange protocol such as MQTT as resources. when the analyzed results were integrated with the delay and energy consumption measurements, they revealed the viability of the proposed solution. As such, in a regular IoT system that is using cloud-based deployment, the projected costs yielded by the proposed authorization system is bsatisfactory based on the advantages of this method.

**Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling*, *58*(5-6), 1189-1205.**

Just like Cruz-Piris et al (2018), the authors of this article recognize that the protection of resources and information is important in the IoT. However, they are dissatisfied with the current authorization frameworks including the RBAC and ABAC. They argue that these frameworks fail to offer manageable, efficient and easy authorization frameworks. As such, they propose a solution that entails the support for rights delegation, as well as refined access control modifications. The authors have provided details on the access control and delegation characteristics of their proposed solution. They have illustrated how capabilities can significantly make granting access easy with differing granularities to a resource without increasing the complexity of the access control system. This achievement depicts the applicability of Cruz-Piris proposed solution, which entailed obtaining an integrated access control system for differing devices. Already, Gusmeroli, Piccione, & Rotondi, (2013)have an OSGi bundle that implements logic to validate a capability, allowing their system to be used in appliances and small devices.

**Jing, L., Xiao, Y., & Chen, C. P. (2012, June). Authentication and access control in the internet of things. In *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on* (pp. 588-592). IEEE.**

Liu and Xiao join the other authors whose work is reviewed in this paper, in recognizing the intrinsic susceptibility of the internet, security and privacy issues. They propose that these issues should be addressed before the proliferation of IoT. As such, the authors evaluate the current access control techniques. They further design a feasible access control method for the IoT. Their design basically focuses on an easy but effective secure key development based on elliptic curve cryptosystem. The authors adopted the role based access control based on role and application for the access control policy. The analysis of their proposed protocol indicated that their proposed intervention can prevent various attacks; among them “eavesdropping, man- in- the middle, key control, and replay” (591).

**Ndibanje, B., Lee, H. J., & Lee, S. G. (2014). Security analysis and improvements of authentication and access control in the internet of things. *Sensors*, *14*(8), 14786-14805.**

Ndibanje, Lee, and Lee join the unanimous opinion that security network, data and sensor device are elements of significant concern in the IoT. As such the author’s aim in this article is to analyze Jing et al.’s (2012) authentication and access control method in IoT. Jing et al.’s framework entails an authorization methods based on role and application, in the related IoT. Jing et al’s framework is discussed in this paper. Ndibanje, Lee, and Lee found various limitations in Jing et al.’s framework and summed them into: costly message exchange, and weak security assessment, that does not match Jing et al.’s strong protocol. They proposed some enhancement in the registration and authentication phases of Jing et al.’s framework. They also propose the addition of a function they thought was vital which entails password recovery. This article shows how further studies in access control in IoT can be leveraged to define past studies, and to generate an easy to use, efficient, manageable authorization and access control framework of IoT; which basically seems to be the major concern in all the studies reviewed herein.

**Ouaddah, A., Mousannif, H., Elkalam, A. A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, *112*, 237-262.**

In this article, Ouaddah et al. review various access control solutions in the internet of things. Their review is based on objectives, models, architecture and mechanisms (OM-AM). After the evaluation, they offer the advantages and drawbacks of the conventional and current access control models from the point of view of IoT. The challenges that emerge in authorization and access control include invention of novel access control mechanisms to match IoT explicit requirements, and the dilemma of adapting centralized or distributed approach. The authors have listed the pros and cons arising from the options posed by both challenges. After the analysis of the current authorization and access control approaches, the authors have proposed further research in order to come up with a framework based on their OM-AM model. They opine that such a framework would yield an adequate access control framework for IoT. Just like the other authors whose work is described in this paper, Ouaddaha et al’s article has contributed significantly towards the designing of an authorization and access control framework that would cover the limitations of the existing frameworks.

**Guoping, Z., & Wentao, G. (2011). The research of access control based on UCON in the internet of things. *Journal of Software*, *6*(4), 724-731.**

Gouping and Wentao introduce the IoT and its associated architecture and protocols as well as the family of usage control models (UCON). Unlike the other models reviewed in the other sources in this paper, (which are based on role, attribute and application), the UCON integrates authorizations, obligations and conditions. The authors uphold the UCON model, citing its ability to offer flexible and easy access to IoT. They assess various traditional access control models, emphasizing on the architecture, and parts of the model. They also offer various illustrations in order to verify the strong expression of the UCON model in the IoT context. This article offers a strong comparative foundation of the cons and pros of UCON model in relation to the other models reviewed herein.