Delegated Anonymous Credentials for IoT Service Chains

Sandeep Kiran Pinjala[1,2] and Krishna M. Sivalingam[1]

[1]*Dept. of Computer Science and Engineering, Indian Institute of Technology Madras, Chennai, India*
[2]*HCL Technologies, Chennai, India*

Email: sandeepkiranp@gmail.com, cs16s001@smail.iitm.ac.in, skrishnam@iitm.ac.in,
krishna.sivalingam@gmail.com

Abstract—The abstract goes here.

Index Terms—

I. INTRODUCTION

Internet of Things (IoT) enables physical objects also called *Things* to communicate with each other and to their human operators. This opens up a myriad of use cases such as smart homes, smart factories, smart cities, smart healthcare, smart grids etc [1]. It is also expected that such connected devices could reach upto 50 billion by 2020 [2]. The IoT devices (for example, a smart bulb or a temperature sensor) are very constrained in terms of memory, processing power, storage and most often are battery powered. Unlike the traditional computers these devices cannot perform computationally intensive tasks and are intended for minor operations of sensing and actuation. Also most of these devices are out in the open without any physical supervision making them easily susceptible to physical attacks.

Owing to the resource constraints and physical openness, IoT devices have been targets of various attacks [3] at physical, network and application layer. IoT devices also collect lot of personal information like user's location, eating habits, medical history etc because of which there has been a growing concern among consumers of such services. Unlike normal computers, these devices cannot provide an interface where the user can look up what personal information is being shared and with whom. In [4] the authors define privacy in IoT as a guarantee for the subject

  a) To be aware of the privacy risks imposed by smart things.
  b) Control over collection and processing of personal informatin
  c) Control over subject's personal information being dissimenated outside of his control sphere.

They then categorize privacy threats and challenges of IoT into a) Identification b) Localization and tracking c) Profiling d) Privacy-violating interaction and presentation e) Inventory and life cycle tracking and f) linkage.

IoT services do not act in silos. They interact with each other and with external entities to provide a complete package of services to the user. For example, in Home Automation, based on the user who is entering the house (say Owner

vs Guest), a completely different set of services may get invoked. The service interactions and invocations depend on the roles and capabilities of the user invoking them. We call the sequence of services that get invoked as *IoT Service Chain*. In this paper we look at providing security and privacy to users and IoT devices that invoke IoT service chains. The rest of the paper is organized as follows. Section 2...... Section 3... Section 4..

II. MOTIVATION AND RELATED WORK

1) IoT Service Chains: We introduced *IoT Service Chains* in section I to refer to the chain of services invoked when an event occurs. Individual services in the chain interact with each other, on-behalf of the initiator towards a common goal. Initiator could either be a human or an IoT device. Each service in the chain would in-turn validate the user/IoT device's credentials for the desired service functionality. IoT devices can either act on behalf of their operator or can be independent of it. For example, if a smart Heart Monitoring System (HMS) detects a low pulse rate for a patient, it immediately needs to initiate the Advanced Cardiac Life Support (ACLS) by injecting an IV of an antidote, reading and interpreting the ECG, starting CPR, inform the doctor etc. The HMS in this case acts as an independent device and does not impersonate the patient. But in case of a smart fridge, which keeps track of the stock of milk, it automatically places an order for replenishment by using the owners credit card details. In this case, the smart fridge acts on behalf of the owner.
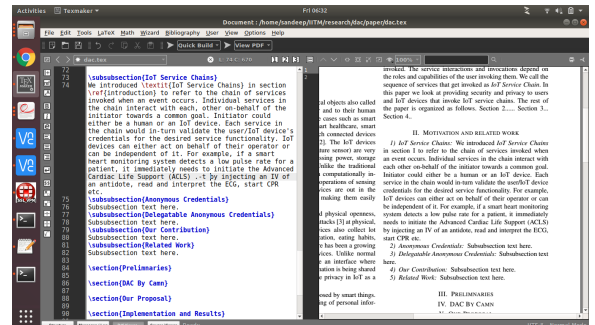

Fig. 1. IoT Service Chain

As can be seen in Fig. 1 there are 5 services in the IoT service chain. xxxx explanation of HMS, ACLS etc interactions among services, authentication etc

One thing to notice from the above figure is that while the service chain is being invoked, the user/IoT device has to be online so that it supplies the necessary credentials for authentication and authorization. This isn't a huge burden if the initiating entity is a user (having a smart phone or a tablet). But for a constrained IoT device generating authentication and authorization information for each service in the chain would result in draining of its resources very quickly. Also, most of the IoT devices are duty cycled and may not remain active till the chain completes. This again results in loss of packets or in retransmission. It will be even more challenging if the user/device's privacy needs to be proected through out the chain. In this paper we focus on some of the options on how device privacy can be ensured when invoking the service chain without pushing the device to its resource limits.

2) Anonymous Credentials: Subsubsection text here.

3) Delegatable Anonymous Credentials: Subsubsection text here.

4) Our Contribution: Subsubsection text here.

5) Related Work: Subsubsection text here.

III. PRELIMNARIES

IV. DAC BY CAMN

V. OUR PROPOSAL

VI. IMPLEMENTATION AND RESULTS

VII. CONCLUSION

The conclusion goes here.

REFERENCES

[1] Ala I. Al-Fuqaha, Mohsen Guizani, Mahdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, 17:2347–2376, 2015.

[2] D. Evans. The internet of things-how the next evolution of the internet is changing everything. April 2011. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf3, last accessed on 01/01/20.

[3] Ioannis Andrea, Chrysostomos Chrysostomou, and George Hadjichristofi. Internet of things: Security vulnerabilities and challenges. pages 180–187, 07 2015.

[4] Jan Henrik Ziegeldorf, Óscar García-Morchón, and Klaus Wehrle. Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, 7:2728–2742, 2014.