An a Technique to Identity Management Approach by an Internet of Things: An a Review Study

Anirudh Kuma Tiwari[1], Rahul Kumar Chawda[2]
[1]Student of MCA, [2]Assistant Professor
Department of Computer Science, Kalinga University, Raipur.

Abstract - Nowadays, 'people are united in their need to be connected to the Internet anywhere, anyhow, anytime. Thanks to the evolution of Information communication technologies (ICT) more and more exclusive services (smart homes, telemedicine, e-Health applications etc.) are available for the users through heterogeneous Internet of Things (IoT) networks, driven by machine to machine (M2M) communication. Although, the communication is established primarily by using devices, the human users are real "generators" and "consumers" of the input and output information. Thus, the human user has to be considered as a "smart" IoT object, thus he/she should be identified, authenticated, authorized. The process of user identification is considered to be very delicate due to the concerns for the people's willingness of sharing private information and data. At the same time, the utilized by a certain user devices, should be taken into consideration. Within this context there is a need of attractive user identification and Identity Management (IdM) mechanisms, involving all of the objects in IoT. Furthermore, the active role of the user in the creation of the rules of identification, and having always responsive services, are extremely important and slightly moving the focus to the concept of 'Internet of People'.

Keyword - Information communication technologies, unique identifier, Identity Management

I. INTRODUCTION

The Internet presents a unique interconnected system which enables devices to communicate globally using set of standard protocols and connecting various heterogeneous networks - academicals, business, governments etc. In the first years, the Internet was represented by static web sites and email communication. Nowadays, different forms of Internet implementation could be seen everywhere around us, part of many different aspects of our lives providing plenty of services and applications, and trying to meet each user's needs no matter time and place. The main "secret" is hidden behind the digitalization of the user and all of the user-friendly and automated mechanisms.

The demand of using internet technologies reflects respectively into all of the users' devices in one way or another, and they have become mobile and closer to the users than ever. Today, the presence of smart devices providing connectivity to the world at each second is considered as mandatory part of our life. Thus, the number of connected devices rapidly increases each year. That requires an autonomous device communication to be created. One of the promising solutions today is known as the Internet of things (IoT). IoT is an informational network that allows the look-up of information about real-world objects interact directly with each other by means of a unique identifier (ID).

Literature Review

Back in 1988, Weiser introduced the "Ubiquitous Computing". He suggested the following forms of ubiquitous computing devices which can provide services to the end user regardless of time or location: tab, pads, and boards. Since then, a lot has changed in terms of computational power and integrity of the computing devices as today they may be found in almost every "thing" around us, being interconnected and capable of exchanging data.

Moving the focus towards today, IoT is "ubiquitous concept where physical objects are connected over the Internet and are provided with unique identifiers to enable their self-identification to other devices and the ability to continuously generate data and transmit it over a network". Hence, the security of the network, data and sensor devices is a paramount concern in the IoT network as it grows very fast in terms of exchanged data and interconnected sensor nodes.

Alongside with the increasing number of network services and applications which constantly provide different types of information, the opportunity of the user to interact with the "things" and "objects" increases constantly and that trend is predicted to continue. The things in IoT may refer to a myriad of connected devices, objects or sub networks for example sensors and actuators connected over Zigbee, Bluethoot, etc.

The architecture supporting interconnected devices evolve further and find implementations in areas like logistics, farming, industry, home automation and many others are already a fact but the restrictions in terms of interconnection solutions from different vendors, communities and standard groups become more obvious. Referring to the business aspects, the IoT enables a plethora of new opportunities, disruptive business models and use case scenarios. In many cases those connected devices and objects are not Hypertext Transfer Protocol (HTTP) driven and that is why there is a lack of decent application integration layers and the applications development is hard to be achieved.

Being more focused on the issues in IoT, the next logical step toward the ubiquitous deployment of applications is the building on top of the already widely used Web technologies. Concerning the importance IoT related open issues, the IdM is recognized as one of the main enablers of the technology. A lot of research has been conducted, but there is no overall framework for identity recognition and management across different solutions.

The high level overview of the IoT is illustrated in Figure 1. It consists of cauterized infrastructure of sensors, exchanged routing data between the nodes, which nodes might be used as gateways in the sub-network of sensors.

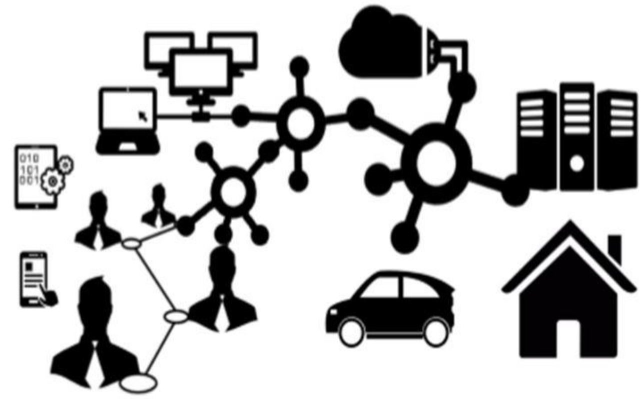

Figure 1: High level view of IoT

The IoT vision for global network of interconnected devices and objects and their real-time communication has been prompted by the M2M paradigm. As a result of the M2M technology, plenty of applications possibilities are available in different aspects - automation processes, tracking, monitoring and control, entertainment etc

Very similar to IoT, "The M2M communications is a broad term describing any technology that enables networked devices to exchange information and perform actions without manual assistance of human personnel"

The M2M devices are performing specific tasks corresponding to their functionalities. These devices also act as independent network nodes, capable of communication over different types of messaging protocols as well as responding to incoming requests.

M2M communication is expected to deploy a technology in order to create intelligent applications and services that are scalable, reliable and embedded, thus the M2M term is closely related to the IoT technology. M2M and IoT are being expected to enable automation and self-network management which is needed to support the large number of connected nodes.

The scope of applications deployed by M2M technology is broad. Some of the areas expected to utilize M2M and IoT concern smart metering, automation, ambient assisted living applications, ambient environment or large-area automation, e-health, etc. Working in different environment and context it should be noted that the solutions for user identification and user identity management are considered to be among the enables of the technology.

II. AUTHENTICATION

A. Human user authentication - The user identity is validated by the process of authentication whereby the provided from the user evidence is verified, it is real or not, by requests for user credentials. Credentials are presented unique characteristics (RFID, Near Field Communication (NFC) tag, face or voice recognition) or information (password) by the user to the authentication parties are, and they are fundamental. Authentication credentials can be one or more and they are part of one of the following groups:

"Something you know" or "something a user knows", type of authentication is based on a shared secret between the involved parties. The typical example is a password authentication scheme. Other various ways for identification already exist such as drawing patterns on smart devices screens, graphical images which have to be recognized. Those methods are unable to replace the usage of traditional password identification because of their usage and insufficient security advantage. "Something you are" or "something a user is" - here, the main role is played by the provided biometric information such as fingerprints, retina or facial scan, voice etc. The weakness is that there is a risk of unintended usage of the digital biometric information and potential threat of theft or it might be copy and use to falsify certain body part because the biometrical information is unique and distinctive in corporation to the user and cannot be changed as password for instance. "Something you have" or "something a user has" - in that case, the authentication requires to be provided an actual item (tokens) where the user's secret is stored such as smart card, a Universal Serial Bus (USB) stick, a serial tap etc .The user does not need to remember secret as it is in the password authentication. It emphasizes a question about whether it can provide real user identification since the sharing of the items between users. In addition, those items can be stolen or lost.

Analyzing the user's behavior regarding browsing, mouse click or other patterns is an alternative method for identification. However, the behavior method is imitable, non-resistible to attacks and its usage is limited in secure systems. Behavioral biometrics is harder to imitate because the capture may depend on a different time of the day, but it is also harder to produce correct results.

The validation of user identity is the main aim for the both identification and authentication processes.

B. Device authentication - Device authentication is also an important aspect in IoT because of the devices' role and broad usage everywhere around us. "Something that is characteristic to a device" are required behavioral credentials or physical context (such as geographic features or transmitted signal frequency) in order to authenticate and determine the device's identity. The mentioned credentials are more often considered as context-based as identity-based. "Something a device has" - here, the secret key is stored in device and has to be provided in order to prove user identification (mentioned above as "something a user has"). Device authentication is often used in an automatic sense/way without requiring presence of user at the certain moment. Therefore, the secret stored in devices is meaningful for device authentication also, not only for the user's.

III. CONCLUSION

The number of devices has been only and rapidly increased and it is predictable that this trend will continue in the next years. This means only one - billion of connected devices, requiring automatic and secured processing will be deployed and operating. The evolution of the ICT industry will trigger new disruptive technologies that will be fundamental and will indicate the need of new business services and applications models, massive "thing" communication capacity, next generation infrastructure, integration of mass-scale cloud architecture and easiest way of action performing ensuring full control from user's perspective.

IV. REFERENCES

[1]. '"The internet of things" [Online]. Available: http://www.ioti.eu/iot/public/news/resources/TheThingsintheInternetofThings_SH.pdf. [Accessed: 31-Mar2015].

[2]. K. Ashton "That 'Internet of Things' Thing - RFID Journal." [Online].Available:http://www.rfidjournal.com/articles/view?4986. [Accessed: 31-Mar-2015].

[3]. Jeroen van den Hoven, "Fact sheet- Ethics Subgroup IoT - Version4.0."[Online].Available:http://www.ethicsinside.eu/contact. [Accessed: 31-Mar-2015].

[4]. M. V. Moreno, J. L. H. Ramos, and A. F. Skarmeta, "User role in IoT-based systems," 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 141–146.

[5]. "Internet of People: Technology 2015-2025: IDTechEx." [Online].Available:http://www.idtechex.com/research/reports/internet-of-people-technology-2015-2025-000388.asp. [Accessed: 31-Mar-2015].

[6]. Ingo Friese, "Concepts of Identity within the Internet of Things - DG - Identities of Things - Kantara Initiative." [Online]. Available:http://kantarainitiative.org/confluence/display/IDoT/Concepts+of+Identity+within+the+Internet+of+Things. [Accessed: Apr-2015].

[7]. Finjan Software Inc, "User Identification and Authentication." 2008.[Online].Availablehttps://www3.trustwave.com/software/secure_web_gateway/manuals/9.2.0/User_Identification_and_Authentica tion.pdf

[8]. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Netw., vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[9]. P.. Mahalle, N. R. Prasad, and R. Prasad, "Identity Management Framework towards Internet of Things. CTIF Aalborg, November 2013

[10]. "Liberty Alliance." [Online]. Available: http://www.projectliberty.org/. [Accessed: 03-Apr-2015].

[11]. "Final: OpenID Authentication 2.0 - Final." [Online]. Available: http://openid.net/specs/openid-authentication2_0.html. [Accessed: 03-Mar-2015].

[12]. M. Weiser, "The computer for the 21 st century," ACM SIGMOBILE Mob. Comput. Commun. Rev., vol. 3, no. 3, pp. 3–11, Jul. 1999.

[13]. B. Ndibanje, H.-J. Lee, and S.-G. Lee, "Security Analysis and Improvements of Authentication and Access Control in the Internet of Things," Sensors, vol. 14, no. 8, pp. 14786–14805, Aug. 2014.

[14]. Dave Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything." Apr2011. [Online]. Availablewww.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Accessed: November-2014].

[15]. D. Rotondi and S. Piccione, "Managing Access Control for Things: A Capability Based Approach," in Proceedings of the 7th International Conference on Body Area Networks, ICST, Brussels, Belgium, Belgium, 2012, pp. 263–268.

[16]. J. Song, A. Kunz, M. Schmidt, and P. Szczytowski, "Connecting and Managing M2M Devices in the Future Internet," Mob. Netw. Appl., vol. 19, no. 1, pp. 4–17, Feb. 2014.

[17]. EU Project eWALL http://ewallproject.eu/

[18]. EU FP7 eWALL project, Deliverable D2.1, Preliminary User and System Requirements v1.0, February 2014

[19]. "New Business Models Required for Internet of Things"[Online].Available:http://www.iottechworld.com/business/new-business-models-required-for-internet-of-things.html [Accessed: May-2015].

[20]. "Internet of Things (IOT): Seven enterprise risks to consider". [Online].Available:http://searchsecurity.techtarget.com/tip/Internet-of-Things-IOT-Seven-enterprise-risks-to-consider [Accessed: May-2015].