International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 7 Issue7 , July-2017, pp. 1~9
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196

INTERNET OF THINGS (IOT): NEW ERA IN TECHNOLOGY

Surbhi Singh

Research Scholar, Department of Computer Science & Engineering

Deenbandhu Chhotu Ram University of Science & Technology, Sonipat

ABSTRACT- The term 'Internet-of-Things' is used as an umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing and/or actuation capabilities. Internet-of-Things envisions a future in which digital and physical entities can be linked, by means of appropriate information and communication technologies, to enable a whole new class of applications and services. In order to understand the applicability and viability of this distributed approach, it is necessary to know its advantages and disadvantages, not only in terms of features but also in terms of security and privacy challenges. The purpose of this paper is to show that this technology has various challenges that need to be solved, but also various interesting properties and strengths.

Keywords- IoT, Sensors, Authentication, Security, Actuators.

1. INTRODUCTION

Nowadays, around two billion people around the world use the Internet for browsing the Web, sending and receiving emails, accessing multimedia content and services, playing games, using social networking applications and many other tasks. While more and more people will gain access to such a global information and communication infrastructure, another big leap forward is coming, related to the use of the Internet as a global platform for letting machines and smart objects communicate, dialogue, compute and coordinate.

The conventional concept of the Internet as an infrastructure network reaching out to end-users' terminals will fade, leaving space to a notion of interconnected 'smart' objects forming pervasive computing environments This innovation will be enabled by the embedding of electronics into everyday physical objects, making them 'smart' and letting them seamlessly integrate within the global resulting cyber physical infrastructure.

Within such perspective, the term 'Internet-of-Thing' (IoT) is broadly used to refer to both: (i) the resulting global network interconnecting smart objects by means of extended Internet technologies,

(ii) the set of supporting technologies necessary to realize such a vision (including, e.g., RFIDs,

sensor/actuators, machine-to-machine communication devices, etc.) and (iii) the ensemble of applications and services leveraging such technologies to open new business and market opportunities.

2. IoT- AN OVERVIEW

Internet of Things (IoT) is an increasingly popular concept that has been widely adopted in a wide range of applications, partly due to decreasing costs of digital devices (e.g. mobile and portable devices such as sensors) and Internet services. In a typical IoT deployment, one could obtain information sent by sensors installed in rural and remote areas as long as there is Internet connection, for example via WiFi or a wireless sensor network (WSN).

IoT is an emerging IT technology. A main function of IoT is to collect data measured by sensors integrated with short range wireless networks such as Bluetooth, ZigBee, or Wi-Fi, which again transmit data to larger networks such as Internet network gateways. IoT sensors provide low cost, scalable, efficient, low power, and integrated data through all sub-networks. As more sensors are incorporated and data collection period increases, the data becomes significantly large and hence the name "Big Data". Big data was introduced by Gartner Report in 2001 and had athreefold definition encompassing 3Vs: Volume, Velocity, and Variety.

One of the major challenges that must be overcome in order to push the Internet of Things into the real world is security. IoT architectures are supposed to deal with an estimated population of billions of objects, which will interact with each other and with other entities, such as human beings or virtual entities. And all these interactions must be secured somehow, protecting the information and service provisioning of all relevant actors and limiting the number of incidents that will affect the entire IoT.

Various threats, are introduced in the following paragraph.

1. Denial of service (DoS). There are a wide number of DoS attacks that can be launched against the IoT. Beyond traditional Internet DoS attacks that exhaust service provider resources and network bandwidth, the actual wireless communication infrastructure of most data acquisition networks can also be targeted (e.g. jamming the channels). Malicious internal attackers that take control of part of the infrastructure can create even more mayhem.
2. Physical damage. This threat can be seen as a subset of the DoS threat. In this attacker model, active attackers usually lack technical knowledge, and can only hinder the provisioning of IoT services by destroying the actual 'things'. This is a realistic attack in the IoT context, because things might be easily accessible to anyone (e.g. a street light). If that is not possible, the attacker can simply target the hardware module in charge of creating the 'virtual persona' of the thing.

3. Eavesdropping. Passive attackers can target various communication channels (e.g. wireless networks, local wired networks, Internet) in order to extract data from the information flow. Obviously, an internal attacker that gains access to a particular infrastructure will be able to extract the information that circulates within that infrastructure.
4. Node Capture. As aforementioned, things (e.g. household appliances, street lights) are physically located in a certain environment. Instead of destroying them, an active attacker can try to extract the information they contain. Note also that, instead of things, active attackers can also target other infrastructures that store information, such as data processing or data storage entities.
5. Controlling. As long as there is an attack path, active attackers can try to gain partial or full control over an IoT entity. The scope of the damage caused by these attackers depends mainly on (a) the importance of the data managed by that particular entity, (b) the services that are provided by that particular entity.

3. SECURITY CHALLENGES IN IoT

Security represents a critical component for enabling the widespread adoption of IoT technologies and applications. Without guarantees in terms of system-level confidentiality, authenticity and privacy the relevant stakeholders are unlikely to adopt IoT solutions on a large scale. In early-stage IoT deployments (e.g., based on RFIDs only), security solutions have mostly been devised in an ad hoc way. This comes from the fact that such deployments were usually vertically integrated, with all components under the control of a single administrative entity. In the perspective of an open IoT eco-system, whereby different actors may be involved in a given application scenario (e.g., one stakeholder owing the physical sensors/actuators, one stakeholder handling the data and processing them, various stakeholders providing different services based on such data to the end-users, etc.), a number of security challenges do arise. In this section, we aim at revising and discussing the major security challenges to be addressed to turn Internet-of-Things technology into a mainstream, widely deployed one. In particular, we identified three key issues requiring innovative approaches: data confidentiality, privacy and trust.

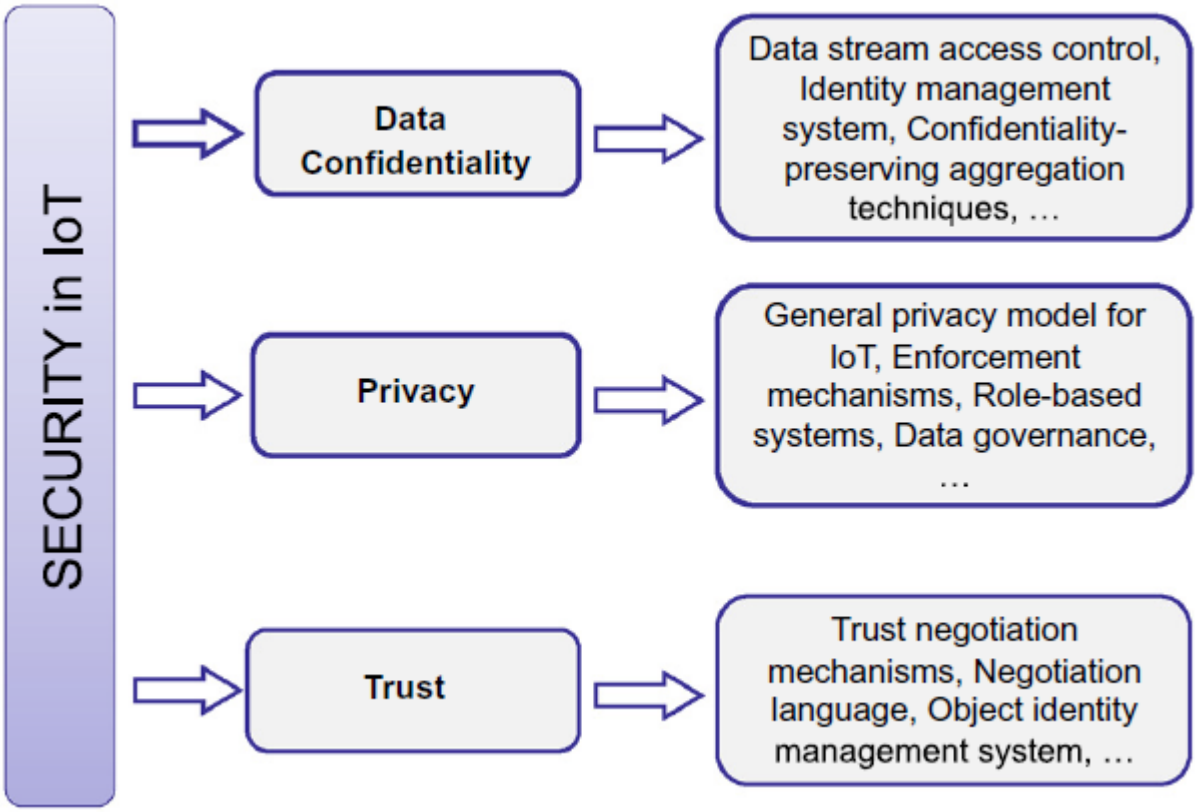

Fig 1. Security Challenges in IoT

4. RELATED WORK

With the incessant progress in the field of ICT and sensor networks, new applications to improve building management systems are constantly emerging. For instance, in office spaces, timers and motion sensors provide a useful tool to detect and respond to occupants, while providing them with feedback information to encourage behavioral changes. The solutions based on these approaches are aimed at providing models based on real sensor data and contextual information. Below is the related work done on IoT in Fig.2

S.No	FEATURE	LITERATURE REVIEW RELATED TO FEATURE
1.	**AUTHENTICATION & CONFIDENTIALITY**	1. The approach presented in [1] makes use of a custom encapsulation mechanism, namely smart business security IoT application Protocol – intelligent Service Security Application Protocol. 2. In [2] it is introduced the first fully implemented two-way authentication security scheme for IoT, based on existing Internet standards, specifically the Datagram Transport Layer Security (DTLS) protocol, which is placed between transport and application layer. This scheme is based on RSA and it is designed for IPv6 over Low power Wireless Personal Area Networks (6LoWPANs). 3. As regards confidentiality and integrity, in [3] it is analyzed how existing key management systems could be applied to the IoT context. It is possible to classify the Key Management System (KMS) protocols in four major categories: key pool framework, mathematical framework, negotiation framework, and public key framework. 4. A more practical approach, as [4], proposes a transmission model with signature-encryption schemes, which addresses IoT security requirements (i.e., anonymity, trustworthy and attack-resistance) by means of Object Naming Service (ONS) queries. Root-ONS can authenticate the identities and platform creditability of Local ONS servers (L-ONS) by a Trusted Authentication Server (TAS). 5. An authentication protocol for IoT is presented in [5], using lightweight encryption method based on XOR manipulation for anti-counterfeiting and privacy protection, in order to cope with constrained IoT devices. 6. The authentication and access control

		method presented in [6] aims at establishing the session key on the basis of Elliptic Curve Cryptography (ECC), another lightweight encryption mechanism.
2.	**ACCESS CONTROL**	1.In [7] the attention is focused on the layer responsible for data acquisition, which is the direct responsible for the information collection. In such a layer, a large amount of nodes are required to sense a wide range of different data types for authorized users in accordance with privacy and security levels. Therefore it presents a hierarchical access control scheme for this layer. 2. Ref. [8] also focuses on the data outsourcing. In particular, due to the large amount of streaming data, companies may not acquire the resources for deploying a Data Stream Management Systems (DSMS). 3. in [9] it is proposed a security framework and an access control model to secure the so called DSMSs, which extends the Borealis data stream engine with security requirements.
1.	**PRIVACY CONTROL**	1.Ref. [10] analyzes the privacy risk that occurs when a static domain name is assigned to a specified IoT node. In this work the authors propose a privacy protection enhanced DNS (Domain Name System) for smart devices, which can authenticate the original users identity and reject illegal access to the smart device. 2. In [11] it is presented a fully decentralized anonymous authentication protocol for privacy-preserving target driven IoT applications.

4.	**TRUST IN IoT**	1. Works [12,13] focus on trust level assessment of IoT entities. The authors assume that most smart objects are human-carried or human-related devices, so they are often exposed to public areas and communicate through wireless, hence vulnerable to malicious attacks. Smart objects have heterogeneous features and need to cooperatively work together.
5.	**ENFORCEMENT IN IoT**	1. In [14] the languages regarding the definition of obligations and policies are classified into two categories. On the one hand, there are policy enforcement languages, which generally simplify the specification and interpretation of policies; however, they lack the formal semantics needed to allow the verification of the policies themselves by means of formal proofs.
6.	**SECURE MIDDLEWARES IN IoT**	1. Both the networking and security issues have driven the design and the development of the VIRTUS Middleware [15], an IoT middleware relying on the open eXtensible Messaging and Presence Protocol (XMPP) to provide secure event-driven communications within an IoT scenario.
7.	**MOBILE SECURITY IN IoT**	1. Ref. [16] analyzes the security challenges for the HIMALIS (Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation) architecture regarding features from IoT and the ID/Locator management messages, vulnerable to attacks. This work proposes a secure and scalable mobility management scheme which considers the IoT constraints, solving the possible security and privacy vulnerabilities of the HIMALIS architecture.

Fig 2. Literature Review

5. CONCLUSION

The Internet-of-Things may represent the next big leap ahead in the ICT sector. The possibility of seamlessly merging the real and the virtual world, through the massive deployment of embedded devices, opens up new exciting directions for both research and business. In this survey article, we provided an overview of the key issues related to the development of IoT technologies and services. A number of research challenges has been identified, which are expected to become major research trends in the next years. The most relevant application fields have been presented, and a number of use cases identified. We do hope that this survey will be useful for researchers and practitioners in the field, helping them to understand the huge potential of IoT and what are the major issues to be tackled, devising innovative technical solutions able to turn IoT from a research vision into reality.

REFERENCES

[1] Y. Zhao, Research on data security technology in internet of things, in: 2013 2nd International Conference on Mechatronics and Control Engineering, ICMCE 2013, Dalian, China, 2013, pp. 1752–1755.

[2] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, Dtls based security and two-way authentication for the internet of things, Ad Hoc Netw. 11 (8) (2013) 2710–2723.

[3] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Comput. Electrical Eng. 37 (2) (2011) 147–159.

[4] Z.-Q. Wu, Y.-W. Zhou, J.-F. Ma, A security transmission model for internet of things, Jisuanji Xuebao/Chin. J. Comput. 34 (8) (2011) 1351–1364.

[5] J.-Y. Lee, W.-C. Lin, Y.-H.Huang, A lightweight authentication protocol for internet of things, in: 2014 International Symposium on Next- Generation Electronics, ISNE 2014, Kwei-Shan, 2014, pp. 1–2.

[6] N. Ye, Y. Zhu, R.-C. b. Wang, R. Malekian, Q.-M. Lin, An efficient authentication and access control scheme for perception layer of internet of things, Appl. Math. Inf. Sci. 8 (4) (2014) 1617–1624.

[7] J. Ma, Y. Guo, J. Ma, J. Xiong, T. Zhang, A hierarchical access control scheme for perceptual layer of iot, Jisuanji Yanjiu yu Fazhan/ Comput. Res. Dev. 50 (6) (2013) 1267–1275.

[8] Papadopoulos, G. Cormode, A. Deligiannakis, M. Garofalakis, Lightweight authentication of linear algebraic queries on data streams, in: Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data, SIGMOD'13, New York, USA, 2013, pp. 881–892.

[9] W. Lindner, J. Meier, User interactive internet of things privacy preserved access control, in: 10th International Database Engineering and Applications Symposium, 2006, IDEAS'06, Delhi,

2006, pp. 137–147.

[10] Y. Wang, Q. Wen, A privacy enhanced dns scheme for the internet of things, in: IET International Conference on Communication Technology and Application, ICCTA 2011, Beijing, China, 2011, pp. 699–702.

[11] A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda,V Anonymous authentication for privacy-preserving iot target driven applications, Comput. Secur. 37 (2013) 111–123.

[12] F. Bao, I. Chen, Dynamic trust management for internet of things applications, in: Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, Self-IoT 12, USA, San Jose, 2012, pp. 1–6.

[13] F. Bao, I. Chen, Trust management for the internet of things and its application to service composition, in: 13th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, United States, 2012, pp. 1–6.

[14] Y. Elrakaiby, F. Cuppens, N. Cuppens-Boulahia, Formal enforcement and management of obligation policies, Data Knowl. Eng. 71 (1) (2012) 127–147.

[15] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M. Spirito, The virtus middleware: an xmpp based architecture for secure IoT communications, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN 2012, Munich, Germany, 2012, pp. 1–6.

[16] A. Jara, V. Kafle, A. Skarmeta, Secure and scalable mobility management scheme for the internet of things integration in the future internet architecture, Int. J. Ad Hoc Ubiquitous Comput. 13 (3-4) (2013) 228–242.