International Journal of Computer & Information Technologies (IJOCIT)
Corresponding Author: *Sara Musavi Fakhr*
September, 2016

A Survey on Security Issues in Internet of Thing

Sara Mousavi Fakhr[1], Faranak Fotouhi [2]
[1]*MCS, Department of Computer Engineering and IT, Qom University*
[2] *Assistant Professor in Pervasive Computing, Department of Computer Engineering and IT, Faculty of Engineering, University of Qom, Alghadir Boulevard, The Old Isfahan Road*
Qom, Iran Postal Code: 3716146611
[12,] *Qom, Iran*
saramousavi1368@gmail.com[1]
f-fotouhi@qom.ac.ir[2]

Abstract: With the recent advances in radio-frequency identification (RFID), low-cost wireless sensor devices, and Web technologies, the Internet of Things (IoT) approach has gained momentum in connecting everyday objects to the Internet and facilitating machine-to-human and machine-to-machine communication with the physical world. So, it is one of the newest applications in the field of communication networks and expected to penetrate all aspects of life in near future. In general, new application to development and use in large-scale may be faced with many challenges. Since the IoT brings together a large variety of devices of different platforms, computational capacities and functionalities, so the network heterogeneity and the ubiquity of IoT devices introduce increased demands on security protection. In order that, in this paper we investigate security of internet of things include three main aspects: *authentication, confidentiality and access control*. These aspects are important to ensure secure communication and safe sharing environment. We point out the main challenges on security aspects of IoT and provide presented solutions in the literature.

Keywords: Internet of thing, security, authentication, confidentiality, access control.

1. Introduction

Nowadays, the Internet of Things (IoT) is a widely-discussed topic among researchers, engineers and technicians. IoT links the objects of the real world with the virtual world, thus enabling anytime, anyplace connectivity for anything and not only for anyone. It refers to a world where physical objects and beings, as well as virtual data and environments, all interact with each other in the same space and time. These things should be able to exchange

information and provide services through different means and from different place [1].

IoT tends to be the next wave of innovation and there are many definitions of the IoT paradigm. For example, IoT can be defined as a highly interconnected network of heterogeneous entities such as tags, sensors, embedded devices, hand-held devices and back-end servers. IoT provides new services and applications that can be deployed in smart homes, transport applications (e.g. Vehicular Ad hoc Networks - VANETs), smart metering, smart grid, etc [2].

The machine-to-machine and machine-to-human communications are usually based on IP protocol which can cause that billions of IoT objects become part of the Internet. Therefore, the security in IoT has to be addressed due to the high possibility of security risks such as eavesdropping, unauthorized access, data modification, data forgery and unauthorized remote tampering with devices. For example, attackers can turn on smart devices and heating systems to trigger a collapse of the power grid. Furthermore, attacks against routing protocols can be performed in IoT infrastructure and applications, e.g., Sybil attacks, the sinkhole attack [2].

Security solutions designed for IoT environments have to deal with heterogeneous IoT entities with various hardware specifications. So in this paper, we try to investigate the main challenges on security aspects of IoT and provide presented solutions in the literature.

The paper is organized as follows. The following section gives a explanation of the main challenges of IoT security and reviews solutions about this challenges. Finally, some conclusions are given in section 3.

2. IoT Security Challenges

This section analyzes in depth three key security requirements: *authentication*, *confidentiality*, and *access control*, with a special focus on IoT systems. IoT, in fact, enables a constant transfer and sharing of data among things and users in order to achieve particular goals. In such a sharing environment, authentication, authorization, access control and non-repudiation are important to ensure secure communication. In the following subsections, we explain depth

three key security requirements and review solutions of them.

2.1. Authentication

Information privacy is defined as "the right to select what personal information about me is known to what people". This stresses the idea of information self-determination by people who can evaluate their privacy risks and protect their privacy by taking appropriate actions. The greater the perceived control, the lower the risk. In previous non-electronic environments, individual privacy was easier to protect because of the relative inefficiency of communication channels. Over the past decade, however, the proliferation of Internet and mobile technologies has made information privacy an urgent issue for emerging technologies like electronic commerce, mobile applications, location-base services and cloud services [4].

Authentication concept tries to prevent of revealing information privacy by control the access of illegal users. In order to deal this problem, some approaches have been investigated in the literature as following.

An approach makes use of a custom encapsulation mechanism, namely smart business security IoT application Protocol intelligent Service Security Application Protocol. It combines cross-platform communications with encryption, signature, and authentication, in order to improve IoT applications development capabilities by establishing a secure communication system among different things. Other approach 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) [5]. The extensive evaluation, based on real IoT systems, shows that such an architecture provides message integrity, confidentiality, and authenticity with

enough affordable energy, end-to-end latency, and memory overhead [5].

Another study [4] differs from previous studies in at least two aspects. First, it proposes a research model including network externalities and its determinants in examining IoT service usage. Though prior studies have examined the network externalities that affect IT adoption few, if any, empirical studies have examined such effects in the context of IoT service adoption. Therefore, it decomposes network externalities and tests their effect on users' perceived benefits. Second, this study empirically examines the impact of CFIP on IoT service adoption, which has received less attention in the literature. Moreover, it also decomposes CFIP to better understand its relative importance within existing models of IoT usage [4].

2.2. Confidentiality

Since IoT includes the high level of heterogeneity, coupled to the wide scale of IoT systems, is expected to magnify security threats of the current Internet, which is being increasingly used to let interact humans, machines, and robots, in any combination. The high level of heterogeneity in IoT systems may make conflict and affect on integrity of this systems. With reference to security, data anonymity, confidentiality and integrity need to be guaranteed, as well as authentication and authorization mechanisms in order to prevent unauthorized users (i.e., humans and devices) to access the system. Whereas, concerning privacy requirement, both data protection and users personal information confidentiality have to be ensured, since devices may manage sensitive information [2].

An approach shows that confidentiality and integrity are 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. In [6] the authors argue that most of the KMS protocols are

not suitable for IoT. In fact, key pool ones suffer insufficient connectivity; mathematical ones make use of the deployment knowledge to optimize the construction of their data structures, but such an approach cannot be used in IoT since client and server nodes are usually located in different physical locations; combination-based KMS protocols suffer both connectivity and scalability/ authentication; negotiation ones make use of the wireless channel and its inherent features to negotiate a common key, however they cannot be suitable for IoT because client and server nodes usually belong to different networks and they should route the information through the Internet in order to be able to talk with each other. Hence, the KMS protocols which might be suitable for some IoT scenarios are the Blom and the polynomial schema [2], whose computational overhead is quite low in comparison to a Public Key Cryptography (PKC) operations (i.e., public key framework). However for such schemes, several countermeasures are required in order to manage device authentication and face man-in-the-middle attacks. For example a framework is presented for IoT based on Public Key Infrastructure (PKI)[7].

A more practical approach, as [8], 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), and the TAS gives a temporary certificate to validated LONS, which can apply for inquiry services many times with the certificate in the validated time. A security ONS query service with anonymous authentication provides credentials only to authorized and trusted LONS, preventing the illegal ONS to enquire information from things. In the transmission process, Remote Information Server of Things (R-TIS) wraps the information of things into multiple encryption

layers with the routing node's public key. The encrypted data are decrypted at each routing node, until the Local Information Server of Things (L-TIS) receives the plain text. Meanwhile, the nodes can check the integrity of received data and the creditability of routing path in the transmitting procedure. Such a transmission model results very weak in terms of attack-resistance due to the adoption of hop-by-hop encryption/decryption behavior.

2.3. Access Control

Access control refers to the permissions in the usage of resources, assigned to different actors of a wide IoT network. Two subjects are identified: the data holders and the data collectors. Users and things, as data holders, must be able to feed data collectors only with the data regarding a specific target. At the same time, data collectors must be able to identify or authenticate users and things as legitimate data holders, from which the information are collected. In IoT we have also to deal with processing of streaming data and not, as in traditional database systems, with discrete data. The main critical issues in this context refer to performance and temporal constraints, since access control for a data stream is more computational intensive than in traditional DBMS (Data-Base Management System). In fact, queries have to be directly executed on incoming streams, which can be made of large volumes of data that might arrive at unpredictable rates. Several works deal with these aspects [2].

In [9] an end-to-end security scheme for mobility enabled healthcare Internet of Things (IoT) is proposed. The proposed scheme consists of i) a secure and efficient end-user authentication and authorization architecture based on the certificate based DTLS handshake, ii) secure end-to-end communication based on session resumption, and iii) robust mobility based on interconnected smart gateways. The smart gateways act as an intermediate processing layer (called fog layer) between IoT devices and sensors (device layer) and cloud services (cloud layer). In this scheme, the fog layer facilitates ubiquitous mobility

without requiring any reconfiguration at the device layer. The scheme is demonstrated by simulation and a full hardware/software prototype. Based on analysis, this scheme has the most extensive set of security features in comparison to related approaches found in literature [9].

In [10] 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, this work presents a hierarchical access control scheme for this layer. The scheme considers the limited computational and storage capacity of the nodes, in fact only a single key is given to each user and node; the other necessary keys are derived by using a deterministic key derivation algorithm, therefore increasing the security (since the keys exchange is limited) and reducing lots of the nodes storage costs. Starting from the consideration that in emergency situations (e.g., an accident occurs, and a doctor is needed), the location of the user can be made available, while under normal circumstances, the user's location information is confidential, [11] presents an identity based system for personal location in emergency situations. It consists of: registration, users authentication, policy, and client subsystems. The system confirms the identity of the user through the user authentication subsystem and gets the level of the emergency through the policy subsystem. Then it can make sure that user's location information can be accessed only by some authorized user and only when it is needed. Also a security architecture is developed, which aims at ensuring data integrity and confidentiality, starting from a prototype query processing engine for data streams, called Nile. Such a mechanism is based on FT-RC4, an extension of the RC4 algorithm, which represents a stream cipher encryption scheme, to overcome possible decryption fails due to de synchronization problems. [11] is focalized on

shared processing of window joins over data streams, in order to enhance the performance and the scalability of the DBMS.

In [12] a Model-based Security Toolkit named SecKit in order to address the challenges described above is proposed. The SecKit supports integrated modeling of the IoT system design and runtime viewpoints to allow an integrated specification of security requirements, threat scenarios, trust relationships, and usage control policies. The SecKit integrates previously published approaches for policy refinement, policy enforcement technology at different levels of abstraction with strong guarantees, context-based policy specification, and trust management. In contrast to existing general purpose and IoT focused security approaches, which address some punctual security issues such as access control, risk, or trust without considering details and interrelations between these issues, the SecKit proposes an Enterprise Architecture approach for security engineering. Moreover, SecKit has been conceived with the ultimate scope to give to the end-user the possibility to design and enforce a set of security and privacy policies completely customized; in other words, it is the enduser that decides the desirable trade-off between information disclosure, privacy and security. SecKit has been integrated with the iCore Framework, which is a generic framework for IoT management. It demonstrates the feasibility of the SecKit components embedded in the iCore Framework and provides results of simulations to support its theoretical foundation. In contrast to its previous publication that already introduces the iCore Framework including the SecKit approach and prototype implementation, this paper shows the formalization of some of the SecKit metamodels and also provides extensions to its policy rule language allowing the management of trust relationships. As a consequence, it builds up on SecKit solution towards a more complete coverage of the main challenges in the existing IoT frameworks with a

special focus on data protection, trust, and privacy issues [12].

In [13] UPECSI is presented, its solution for **U**ser-driven **P**rivacy **E**nforcement for **C**loud-based **S**ervices in the **I**oT. UPECSI takes a comprehensive approach to privacy for the cloud-based IoT by providing an integrated solution for privacy enforcements that focuses on individual end-users and developers of cloud services at the same time. UPECSI consists of several technical components and organizational processes. More specifically, with UPECSI, it presents the following core contributions: i) individual, user-driven enforcement of privacy requirements already before any potentially sensitive data is handed over to the cloud, ii) a novel technique for designing and implementing cloud-based services that integrates privacy functionality into the development process, and iii) an easy to understand, flexible, and transparent approach for users of different privacy expertise to configure their individual privacy settings. These contributions of our comprehensive approach to privacy in the cloud-based IoT allow us to lay the foundation for bringing the IoT and cloud computing together in a user-accepted fashion [13].

3. Comparison of Reviewed Approaches

After discuss about main challenges in security of IoT, let us compare the advantage and disadvantage of reviewed approach and how deal this approach with main challenges. Table 1 demonstrates that these approaches how address the challenges.

Table 1: Comparison of Reviewed Approaches

	authentication	Confidentiality	Access control
6LoWPANs	*	*	
decomposed CFIP	*	*	
KMS		*	
PKC	*	*	
ONS	*	*	
end-to-end security scheme	*	*	*
hierarchical access		*	*

control			
identity-based personal location	*		*
SecKit	*		*
comprehensive approach	*	*	*

As shown in the table, all approach can't solve all challenge completely and each of them concentrates on certain aspects of challenges in IoT.

According to signification growth of communication between things in the real word, it's necessary to notice on solve the all challenges and provide safe and secure platforms and protocols to connect things and agents.

4. Conclusion

The real spreading of IoT services requires customized security and privacy levels to be guaranteed. The broad overview provided with this survey arises 1195 many open issues, and shed some light on research directions in the IoT security field. More in details, a unified vision regarding the insurance of security and privacy requirements in such a heterogeneous environment, involving different technologies and communication standards is still missing. Suitable solutions need to be designed and deployed, which are independent from the exploited platform and able to guarantee: confidentiality, access control, and privacy for users and things, trustworthiness among devices and users, compliance with defined security and privacy policies. In this study we tried to investigate main challenges in security aspect of IoT and we reviewed some solutions in literary. We denoted that all approach can't solve all challenge completely and each of them concentrates on certain aspects of challenges in IoT but due to unbelievable growth of IoT, it's necessary to notice on solve the all challenges and provide safe and secure

platforms and protocols to connect things and agents.

5. References

[1] Sundmaeker H, Guillemin P, Friess P, Woelffl S. "Visions and challenges for realising the internet of things". Cluster of European Research Projects on the Internet-of-Things (CERPIoT); 2010.

[2] Lukas Malina, Jan Hajny, Radek Fujdiak, Jiri Hosek. "On Perspective of Security and Privacy-Preserving Solutions in the Internet of Things". *Computer Networks*, 2016, doi: 10.1016/j.comnet.2016.03.011

[3] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen Porisini. "Security, privacy & trust in internet of things: The road ahead". Computer Networks, 2014, doi: http://dx.doi.org/10.1016/j.comnet.2014.11.008

[4] Chin-Lung Hsu a, Judy Chuan-Chuan Lin. "An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives". Computers in Human Behavior, vol.62, 2016, pp: 516-527.

[5] Y. Zhao. (2013). "Research on data security technology in internet of things". 2nd International Conference on Mechatronics and Control Engineering, 1260 ICMCE 2013, Dalian, China, pp. 1752–1755.

[6] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos. "Key management systems for sensor networks in the context of the internet of things". Computers & Electrical Engineering. vol.37 (2), (2011), pp:147–159.

[7] H. Ning. "A security framework for the internet of things based on public key infrastructure". Advanced Materials Research,vol.674, 2013, pp: 3223–3226.

[8] Z.-Q. Wu, Y.-W. Zhou, J.-F. Ma. (2011). "A security transmission model for internet of things". Jisuanji Xuebao/Chinese Journal of Computers 34 (8), 2011, pp:1351–1364.

[9] S.R. Moosavi, T.N. Gia, E. Nigussie, A.-M. Rahmani, S. Virtanen, H. Tenhunen, J. Isoaho. "End-to-end security scheme for mobility enabled healthcare Internet of Things". *Future Generation Computer Systems*, 2016, http://dx.doi.org/10.1016/j.future.2016.02.020.

[10] J. Ma, Y. Guo, J. Ma, J. Xiong, T. Zhang. (2013) . "A hierarchical access control scheme for perceptual layer of iot". Jisuanji Yanjiu yu Fazhan/ComputerResearch and Development 50 (6), 2013, pp:1267–1275.

[11] C. Hu, J. Zhang, Q. Wen.(2011)."An identity-based personal location system with protected privacy in IoT", Proceedings - 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, 1320 IC-BNMT 2011, Shenzhen, China, pp. 192–195.

[12] Ricardo Neisse, Gary Steri, Igor Nai Fovino, Gianmarco Baldini. "SecKit: A Model-based Security Toolkit for the Internet of Things". Computer & Security vol.54, 2015, pp:60-76.

[13] M. Henze, L. Hermerschmidt, D. Kerpen, R. Haußling, B. Rumpe, K. Wehrle. "A comprehensive approach to privacy in the cloud-based Internet of Things". *Future Generation Computer Systems*, 2015, http://dx.doi.org/10.1016/j.future.2015.09.016

