Computer Networks 000 (2018) 1–24

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Review article

Internet of things security: A top-down survey

Djamel Eddine Kouicem[a,*], Abdelmadjid Bouabdallah[a], Hicham Lakhlef[a]

Sorbonne Universités, Université de Technologie de Compiègne CNRS, HEUDIASYC UMR 7253, CS 60319, Compiègne Cedex 60203, France

ARTICLE INFO

Article history:
Received 1 June 2017
Revised 14 February 2018
Accepted 14 March 2018
Available online xxx

Keywords:
Internet of Things
Security
Privacy
Cryptography
Blockchain
Software defined networking

ABSTRACT

Internet of Things (IoT) is one of the promising technologies that has attracted a lot of attention in both industrial and academic fields these years. It aims to integrate seamlessly both physical and digital worlds in one single ecosystem that makes up a new intelligent era of Internet. This technology offers a huge business value for organizations and provides opportunities for many existing applications such as energy, healthcare and other sectors. However, as new emergent technology, IoT suffers from several security issues which are most challenging than those from other fields regarding its complex environment and resources-constrained IoT devices. A lot of researches have been initiated in order to provide efficient security solutions in IoT, particularly to address resources constraints and scalability issues. Furthermore, some technologies related to networking and cryptocurrency fields such as Software Defined Networking (SDN) and Blockchain are revolutionizing the world of the Internet of Things thanks to their efficiency and scalability. In this paper, we provide a comprehensive top down survey of the most recent proposed security and privacy solutions in IoT. We discuss particularly the benefits that new approaches such as blockchain and Software Defined Networking can bring to the security and the privacy in IoT in terms of flexibility and scalability. Finally, we give a general classification of existing solutions and comparison based on important parameters.

1. Introduction

Nowadays, Internet of Things (IoT) is changing much about the world we live in, the way we drive, how we make decisions, and even how we get energy. Internet of things consists of sophisticated sensors, actuators and chips embedded in the physical things that around us by making them smarter than ever. These things are connected together and exchange huge data between them and with other digital components without any human intervention [3]. IoT contributes significantly to enhance our daily life throughout many applications come from different sectors such as smart cities, smart building, healthcare, smart grids, industrial manufacturing among others.

Currently, one of the issues that potentially threats Internet of Things' devices is the security and the privacy of exchanged/collected data that are often deeply linked to the life of users. Gartner[1] envisioned that, by 2017, more than 20% of organizations and businesses will deploy security solutions to protect their IoT devices. These considerations lead us to underline the importance of enforcing security mechanisms in IoT applications which play a pioneer role in mitigating IoT risks. Security problems in IoT are most challenging than the existing security problems in Internet of nowadays. Indeed, it is instructive to note that the things are highly resources-constrained in terms of computing capacity, memory and energy which make the existing security solutions absolutely not applicable. Moreover, the high number of connected objects, estimated by Cisco [46] to be about 50 billions of objects by 2020, arises scalability issues.

These last years, a lot of researches are leading to address the various security challenges closely related to IoT such as key management issues [114], confidentiality, integrity, privacy, policy enforcements [110,113] among many other challenges. The main works in the literature tried to adapt the security solutions proposed for wireless sensor networks (WSNs) and Internet in the context of IoT. However, we must point out that IoT's challenges take a new dimension which is far from being easy to overcome with traditional solutions. In addition, we must emphasize that most security approaches rely to centralized architectures, making their applications in IoT much more complicated regarding the large number of objects. So, distributed approaches are required to deal with security issues in IoT. In this paper, we survey the different solutions according to two perspectives, namely the security approaches based on traditional cryptographic approaches and the other approaches based on new emerging technologies as SDN and Blockchain.

* Corresponding author.
E-mail address: djamel-eddine.kouicem@hds.utc.fr (D.E. Kouicem).

[1] https://www.intrinsic-id.com/intrinsic-id-guardtime-announce-alliance-iotblockchain/.

https://doi.org/10.1016/j.comnet.2018.03.012
1389-1286/

Table 1
Recent surveys in IoT security.

	[105]	[89]	[111]	[94]	[5]	[14]
Smart grids	Yes	No	No	No	Yes	No
Smart cities	No	Yes	No	No	Yes	No
Healthcare	No	No	No	No	Yes	No
Manufacturing	No	Yes	No	No	Yes	No
Transport	Yes	No	No	Yes	Yes	
Confidentiality	Yes	No	Yes	Yes	Yes	Yes
Privacy	No	Yes	Yes	Yes	No	Yes
Availability	Yes	No	No	No	Yes	Yes
Blockchain	No	No	No	No	No	No
SDN	No	No	No	No	Yes	No
Context-awareness	Yes	Yes	Yes	No	No	No
Safety-Security	Yes	Yes	No	No	No	No

In the literature, there are some published surveys that cover different aspects of security in IoT. In [14,66,74,108,127,137], authors underlined the security challenges and issues in IoT without discussing the various solutions proposed for these challenges. Moreover, Roman et al. [104] discussed the main benefits and also the important issues to be addressed in terms of security and privacy in decentralized architectures.

Other surveys are oriented IoT domain applications. In [36,41] provided an overview about security and privacy challenges in smart grids. Other applications are also discussed in other papers. We can cite Healthcare application in [4] and industrial IoT in [105]. Alaba et al. [5] investigated the main security vulnerabilities and attacks in IoT.

Other surveys dealt with IoT security issues and reviewed solutions according to each security service. In contrast, in [111], the authors investigated confidentiality, access control, trust management and privacy solutions in IoT. On the other hand, in [98] Ouaddah et al. reviewed access control solutions. In [94], Kim et al. gave a classification of key management solutions in IoT. In those surveys, the authors focused particularly on classical based cryptographic approaches without discussing the new relevant techniques which could potentially bring huge values in terms of security and privacy.

Intrusion detection in IoT is another important research field which has received a high interest of researchers. Some surveys [25,89] have discussed intrusion detection systems (IDS) in wireless sensor networks and Internet of Things and have provided analysis and comparison of the main existing IDSs.

The main common line between the existing surveys is that most of them focus on cryptographic solutions which belong to centralized approaches. However, recently, many emergent technologies (ex. blockchains, SDN) are being adopted by industrials (ex. IBM's IoT based blockchain solution, named ADEPT) as promising solutions to fix security and privacy issues in IoT that have not been addressed in all existing papers. In this survey, we take a different direction by enumerating the different security approaches, including recent ones and classify them into two main categories: classical approaches and new emerging techniques. Furthermore, we provide a top down review that offers a holistic view of the security in Internet of Things. This review encompasses in three steps the different aspects of security in IoT by starting from generic to specific aspects. We start by enumerating the different challenges related to the various IoT applications. Subsequently, we discuss in more details the several solutions of IoT security recently published in the literature. Finally, we finish our survey with a synthetic comparison and discussion about the most relevant solutions for each IoT application with respect to the several security challenges. By positioning with respect to the aforementioned surveys, the Table 1 shows clearly that the contribution of this paper includes, in a comprehensive way, the most relevant aspects such as lightweight cryptographic approaches, blockchain, the context awareness and the coupling security-safety in IoT. All these aspects constitute the main recent research pieces in the field of Internet of Things security and privacy.

The main contributions of this survey are threefold:

- Present the different security challenges and requirements for the main IoT applications, i.e a top down approach.
- Survey the literature solutions according to two main points of view (classical and new emerging approaches).
- Finally, provide a comparison of the enumerated approaches based to some parameters; and investigate the possibility of applying such approach on a given IoT application.

The rest of the paper is organized as follows. Section 2 gives a background about the main security services and the main known techniques to fulfill each service. We discuss and summarize, in Section 3, the main security challenges and requirements of some well known IoT applications. In Section 4, we provide our classification of security solutions. In Section 5, we describe in details the main classical approaches proposed in literature, we classify those approaches according to security services. New emerging approaches based on blockchain and Software Defined Networking technologies are described in Section 6. We discuss in Section 7, the importance of context awareness to mitigate security in IoT. Section 8 gives details about design approaches of security and safety in Cyber-Physical based IoT systems. Section 9 provides a comparison of the proposed security solutions and their applications in the different IoT sectors. Section 10 concludes the paper.

2. Background on security services

Security consists of all the techniques that aim to preserve, restore and guarantee the protection of information in computer systems from malicious attacks. Daily news puts security at the top of concerns: leakage of personal data and economic espionage, infection of sensitive computer systems, identity theft and fears about card payments are just few examples of threats. The security of computer networks and information systems in general, consists to provide the following services [96]:

- **Confidentiality**: It ensures that information is made unintelligible to unauthorized individuals, entities, and processes.
- **Integrity**: It ensures that data has not been modified by a third party (accidentally or intentionally).
- **Authentication**: It verifies that the data source is the pretended identity.
- **Non-repudiation**: It ensures that the sender of the message can not deny having sent the message in the future.
- **Availability**: It ensures that the services of the system should be available for legitimate users.
- **Privacy**: It ensures that users' identities should not be identifiable nor traceable from their behaviors and their performed actions in the system.

Several cryptographic mechanisms have been put in place to deal with the different security threats and ensure the security services mentioned above. We provide in Table 2 some of those mechanisms.

3. IoT applications: Security requirements and challenges

Internet of Things enables to improve several applications in various fields, such as, healthcare, smarts grids, smart cities, smart homes as well as other industrial applications. However, introducing constrained IoT devices and IoT technologies in such sensitive applications leads to new security and privacy challenges. In this

Please cite this article as: D.E. Kouicem et al., Internet of things security: A top-down survey, Computer Networks (2018), https://doi.org/10.1016/j.comnet.2018.03.012