Security in Internet of Things: A Survey

Conference Paper · May 2017
DOI: 10.1109/ISNCC.2017.8072001

0 CITATIONS
527 READS

3 authors:

Alma Oracevic
Georgia Institute of Technology
6 PUBLICATIONS  14 CITATIONS

Selma Dilek
Hacettepe University
5 PUBLICATIONS  9 CITATIONS

Suat Ozdemir
Gazi University
60 PUBLICATIONS  1,050 CITATIONS

Some of the authors of this publication are also working on these related projects:

- Reliability-Oriented Design Methods for Application Specific Integrated Circuits View project
- virtual machine placement with multiobjective optimization algorithm View project

All content following this page was uploaded by Suat Ozdemir on 02 June 2017.
The user has requested enhancement of the downloaded file.
Abstract—Internet of Things (IoT) can be seen as a pervasive network of networks: numerous heterogeneous entities both physical and virtual interconnected with any other entity or entities through unique addressing schemes, interacting with each other to provide/request all kinds of services. IoT technology is expected to pave the way for groundbreaking applications in a diversity of areas such as healthcare, security and surveillance, transportation, and industry, and integrate advanced technologies of communication, networking, cloud computing, sensing and actuation. Given the enormous number of connected devices that are potentially vulnerable, highly significant risks emerge around the issues of security, privacy, and governance; calling into question the whole future of IoT. IoT applications are expected to affect many aspects of people’s lives, bringing about many conveniences; however, if security and privacy cannot be ensured, this can lead to a number of undesired consequences. This survey focuses on the security aspects of IoT, and discusses up-to-date IoT security solutions.

Keywords—Internet of Things (IoT); survey; security

I. INTRODUCTION

In recent years, concepts such as smart devices, smart cars, smart cities, and smart homes have received great interest from many different research communities. The combination of these concepts is considered as the future of Internet and it is called the Internet of Things (IoT) [1, 2, 3]. Recent technological advances in electronics have enabled the development of all kinds of small-size devices with various degrees of sensing, computing, storage, and power capabilities, which has led to the opportunity of utilizing almost any object as a smart and communicating thing rather than an isolated entity, for the purpose of unlimited number of applications, but at the same time providing that security and confidentiality requirements are met [4, 5].

IoT can be seen as a pervasive network of networks: numerous heterogeneous entities both physical and virtual (people, sensors, software, all kinds of devices) interconnected with any other entity or entities through unique addressing schemes at virtually any scale, interacting with each other to provide/request all kinds of services (See Fig. 1) [1, 2, 6].

In the Y.2060 Recommendation of the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T), the concept of IoT was defined as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies” [5].

Fig. 1. Internet of Things

It is expected that IoT technology will pave the way for groundbreaking applications in a diversity of areas such as healthcare, security and surveillance, transportation, and industry, and that it will be able to integrate technologies such as advanced machine-to-machine communication, autonomic networking, decision-making, confidentiality protection and security, and cloud computing with advanced detection and actuation technologies [5, 7, 8].

Technically speaking, IoT encompasses both static and dynamic objects of the physical world (physical things) and the information world (virtual world), which can be identified and integrated into communication networks (See Fig. 2). The essential features of IoT include: (i) interconnectivity, (ii) things-related services such as privacy protection and semantic consistency, (iii) heterogeneity, (iv) support of dynamic changes in the state and the number of devices, and (v) enormous scale [5].

Fig. 2. Technical perspective of the Internet of Things
The importance of the context of scale is evident from the fact that, by the year of 2010, there were already 1.84 connected devices per person; and it has been estimated that the number of connected devices will accomplish approximately 50 billion by 2020 [9]. Given the enormous number of connected devices that are potentially vulnerable, highly significant risks emerge around the issues of security, privacy, and governance; calling into question the whole future of IoT. IoT applications will affect many aspects of people’s lives, bringing about many conveniences; however, if security and privacy cannot be ensured, this can lead to a number of undesired consequences such as violation of private information and other opportunities for foul play [10].

The goal of this paper is to examine the security issues and challenges of IoT, and present an overview of up-to-date security solutions. This paper also provides a scope for future research areas by stating IoT security issues that have not been addressed yet. The rest of this paper is organized as follows. Section II describes security in the IoT. In section III, related work in the field of IoT security is presented. Section IV shows the comparison of presented solutions for IoT security, and finally, conclusion marks are given in section V.

II. SECURITY IN THE INTERNET OF THINGS

IoT growth offers a lot of opportunities; however, it is still not completely developed or protected. Adding new devices, hardware endpoints, large number of lines of code, together with more infrastructure to endure with the load, creates a large number of challenges, unmatched by anything similar experienced over the past two decades [11,12]. Information insecurity will directly endanger the entire IoT system.

The IoT devices have brought IoT security further up the bunch of issues that need to be addressed quickly because of vulnerabilities found on it. For example, researchers found critical vulnerabilities in a wide range of IoT baby monitors, which could be leveraged by hackers to carry out a number of nefarious activities, including monitoring live feeds, changing camera settings and authorizing other users to remotely view and control the monitor [13]. Another example is a group of hackers that write off a power grid in a part of Ukraine to cause the first blackout from a cyber attack. Hackers are looking for more ways to strike critical infrastructures, such as power grids, hydroelectric dams, chemical plants, and more every day, and these sorts of attacks are probably just the beginning [14].

Since poorly secured IoT devices could serve as entry points for cyber attacks by allowing malicious individuals to re-program a device or cause it to malfunction, the security in IoT cannot be ignored. If the signal of IoT is snapped or somehow disrupted, it will have huge effect on the security of the entire information of IoT. Hackers, software that is malicious and all sorts of viruses in the communication process could alter data and information integrity.

When defining what a secure IoT is, it is important to understand the characteristics that define security. The security requirements that have to be considered in a typical IoT application are divided into three main categories: (i) confidentiality, (ii) integrity, and (iii) authentication.

- Confidentiality implies discretion in keeping information secret from the third parties. For example, sensitive sensor data, such as the strategic military information, require confidentiality. It is one of the most requested properties in wireless sensor network (WSN) applications. If it were possible to manipulate the reports of a WSN, forces may be misguided, which could give the enemy an advantage. Confidentiality is also important for critical social and industrial applications.

- To preserve the integrity of data in IoT, the communication recipient has to verify that the received messages have not been modified during transmission or delivery. Data integrity certifies that a data being transferred is never altered or corrupted. It is very important, because even if intruders cannot obtain the data, if compromised nodes corrupt the transmitted data, the network may not function properly. In fact, if the communication channel is unreliable, data may be altered without the presence of an intruder. Integrity check ensures detection of accidental and intentional message changes.

- Authentication is the process of determining whether a message is, in fact, from where it claims it is, or what it is declared to be. The sensor nodes must determine the identity of the peer node they are communicating with and authentication enables that. Authenticity guarantees that a message is authentic. Message authentication code (MAC) is a short piece of information used to authenticate a message and provide integrity and authenticity assurances on the message.

IoT has the same security issues as all components that make particular multiple heterogeneous networks. Simply put, IoT has security issues as all sensor networks, mobile communications networks and the Internet. However, it has its own security considerations such as privacy issues, different authentication and access control network configuration issues [12].

A. Security issues

The biggest challenge of IoT is ensuring data and privacy protection. The key technologies of IoT are RFID technology, sensor technology, embedded system technology and nanotechnology; therefore, one of the main risks comes from the technology of construction. Since IoT is the integration of multiple heterogeneous networks it is difficult to achieve a reliable connection between the individual nodes in IoT due to the nodes constantly changing. In furtherance of analyze the security issues of the IoT in more detail, IoT architecture can be divided into three layers: sensing layer, transportation layer and application layer (Table I).

In IoT, RFID systems and nodes in WSNs are perceived as one end of the information technology. RFID (Radio Frequency Identification) is automatic identification technology that uses radio-frequency electromagnetic fields to identify objects carrying tags when they come close to a reader [15].
### Security Issues in the IoT Architecture

<table>
<thead>
<tr>
<th>IoT layer</th>
<th>Security issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application layer</td>
<td>Information availability, user authentication, information privacy, data integrity, IoT platform stability, middleware security, management platform</td>
</tr>
<tr>
<td>Transport layer</td>
<td>DOS/DDOS attacks, forgery/middle attack, heterogeneous network attacks, WLAN application conflicts, capacity and connectivity issues etc.</td>
</tr>
<tr>
<td>Sensing layer</td>
<td>Interruption, interception, modification, fabrication, uniform coding for RFID, conflict collision for RFID etc.</td>
</tr>
</tbody>
</table>

At this level (sensing layer), an IoT system aims to acquire, collect and process the data from the physical world. There is a variety of attacks and threats specific for this layer; for example, all threats and attacks that are specific to WSNs [16-22] are also part of the security threats and attacks on IoT, since as soon as a corrupted sensor node connects to IoT the whole system becomes unreliable. Furthermore, IoT security needs also to include the security of a entire system stretch over the sensing layer, transportation layer and application layer. Security architecture of IoT is shown in Fig. 3.

The RFID security, WSNs security, RSN (RFID sensor network) security are included in sensing security. For example, to solve the problem caused by heterogeneous data in IoT, RSN is used. The RSN is the integration of RFID and WSNs [23]. The access network security, core network security and local network security are part of transportation layer security. Furthermore, if we take into consideration different technologies, then 3G access network security, Ad-Hoc network security, and WiFi security are also a part of these sublayers and their security domain. Application layer encompasses application support layer and specific IoT applications. The middleware layer technology security is part of support layer, along with cloud computing platform security, etc. When we consider the security of IoT applications, we will see that their security depends on the application that is truly diverse and comprehensive, hence the safety requirements.

---

**ICMetric** is based on cryptography keys. The idea behind ICMetric is a mathematical and statistical extraction of device features which, when combined, uniquely characterize the performance of a given electronic device. The ICMetric includes two stages of calculations: the calibration stage is applied only once per application domain employing a number of known circuits as a calibration set, while the operation stage is applied each time an encryption key is desired for a given

---

![Security Architecture of IoT](image-url)
circuit. The ICMetric technology adds an additional layer to the existing cryptographic schemes in an attempt to eliminate problems related to key theft and device cloning; therefore, it can be also used for preventing device tampering and unauthorized access. In [25], ICMetric technology is integrated into a healthcare environment, as an approach to debugging and encryption that allows for safe and secure use of electronic devices, which is a crucial requirement of IoT based healthcare applications. ICMetric technology also provides protection of data stored on and transmitted between the devices. It is based on the idea of deriving encryption keys directly from the characteristics of electronic systems' performance that has advantage over the existing security systems by offering an entirely template-free encryption. In [24], a solution for providing security of IoT is presented based on the ICMetric technology coupled with Secure Remote Rabbit Protocol, which secures entities and their intercommunications to provide security for IoT. What distinguishes this paper from the original solution presented in [25] and the solution used in healthcare application presented in [26], is that this solution claims to safeguard against threats at both the device and network level. The authors in [24] claim that their presented solution provides authentication, confidentiality and non-repudiation for continuous data streams for IoT applications.

Liu et al. in [27] proposed a solution for IoT security based on the principles of a biological immune system. A biological immune system has served as a role model for building IoT security. The proposed solution uses a dynamic defense frame for IoT security, since static defense strategies may prove to be inadequate. They propose a circular defense with five links: security threat detection, danger computation, security responses, security defense strategy formulation, and security defense. The links in the frame are correlated with relative data of IoT security. The behavior of a biological immune system is applied to establish links in the proposed scheme solution to make the proposed approach adaptive to the IoT environment. The authors simulated the real IoT environment using immunity-based antigen, self and detector in the real IoT. They are used to imitate the mechanisms which are applied to recognize pathogens in biological immune systems. The simulation results of [27] show that the proposed approach may provide a novel effective method to ensure IoT security.

In [28], Zhou and Chao developed a novel architecture for media-aware traffic security and designed and evaluated the proposed security-critical traffic management scheme. The novel media-aware traffic security architecture (MTSA) meets the information security requirements for multimedia communication, computation, and service in the IoT environment. The authors embedded the proposed solution into the existing architecture for multimedia security [29]. In [29], the author described challenges and proposed solutions for multimedia security in wired networks. Same analogy is used in [28], but the solution is adapted to respond to the challenges and requirements of the multimedia system security in the IoT environment. It is stated that distributed privacy paradigm for MTSA, in which the authority, cost, and encryption are obtained in a decentralized manner, is a novel solution. The media-aware traffic security architecture is presented based on the proposed traffic classification to enable diverse multimedia services provided to users anywhere at any time.

Rose described the crossbar memristive physical unclonable functions (PUFs) as an example of the implementation of security primitives and protocols for the emerging IoT devices [30]. The main idea is that nanoelectronic technologies can be leveraged as a way of implementing small, energy-efficient security mechanisms for resource-limited IoT devices. In [30], it is described that in the IoT environment, the PUF has the potential to provide security enhancements in the form of robust authentication or secret key generation. Although PUF has some limitations and restrictions, such as unreliable responses, with utilizing error correction PUFs are a viable option as emerging hardware security primitives.

Lessa dos Santos et al. in [31] introduced an architecture to enable constrained devices to use Datagram Transport Layer Security (DTLS) with mutual authentication to communicate with Internet devices. This security architecture for IoT is based on a third party device called Internet of Things Security Support Provider (IoTSSP) and two main mechanisms for 6LoWPAN Border Router (6LBR) to redirect the DTLS handshaking to the IoTSSP: (i) the Optional Handshaking Delegation, and (ii) the Transfer of Session. The handshaking between the IoTSSP and the constrained device executes the control to prevent Denial of Service (DoS) attacks. The IoTSSP is responsible for: (i) managing certificates and cryptographic keys of constrained devices, (ii) analyzing the Internet device certificate, (iii) authenticating the constrained device and the Internet device, (iv) establishing a secure session between them, and (v) transferring this session to the constrained device.

Kothmayr et al. in [32] described a similar IoT security solution to [31]. They proposed the use of a dedicated hardware to enable security in constrained devices. The main idea is to use the trusted-platform modules (TPM) added to each constrained device. Although this hardware supports RSA, the most widely used public key cryptography, and works on top of the standard low power communication stacks, it does not endorse CoAP recommendation of using ECC cryptography. Furthermore, the proposed architecture provides message integrity, confidentiality and authenticity with affordable energy, end-to-end latency and memory overhead, which make it a feasible security solution for the emerging IoT, as stated in [32].

Xin described a mixed encryption algorithm used in IoT security transmission [33]. The proposed algorithm provides information integrity, confidentiality, non-repudiation on the data transmission for IoT using the hybrid key technology, which takes into account the characteristics of a symmetric key and asymmetric key. Encryption is a required step for the security of the Internet of things. The Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) are broadly used for information security. The proposed algorithm uses AES algorithm encryption for its simplicity, velocity and reliability. The author of the proposed approach in [33] claims
that the hybrid encryption enables achieving a better and more effective information security while the information is transmitted over a number of networking components.

Leo et al., in [34], proposed an architecture model mainly devoted to deploying and managing of a federated environment for authority delegation mechanism, identity based capability and dynamic context information. The main element of the proposed solution is the Secure Mediation GateWay (SMGW) that is dedicated to manage the secure communication for both intraSMGW and interSMGW nodes, under the assumption that the IoT space can be divided into the intraSMGW and interSMGW categories. In [34], the SMGW is in charge of the management of all security features, from the simple accounts management up to the availability of a crypto engine, to support the secure remote access to things within the SMGW domain.

In [35], the authors propose a basic theoretical framework that will allow achieving IoT security via providing its topological sustainability in order to confront security threats, aimed at disrupting, degrading or destroying IoT components and services. The aim is to maintain IoT security through topological sustainability which allows protection of nodes in IoT from a large class of DoS attacks via maintaining adaptive random d-regular graph topology, taking into consideration specific IoT requirements such as constrained computational resources on the IoT end devices.

Raza et al. in [36] implemented Scalable Security with Symmetric Keys (S3K) - a highly scalable and flexible key management scheme for DTLS security standard for resource-constrained IoT devices. S3K is lightweight; it entails establishing only a single trusted relationship between the resource server and a device, and it enables devices with no previous security relation to use DTLS as it does not require predistribution of trusted keys. The evaluation results showed that S3K is highly effective against battery-drain and DoS attacks.

IV. COMPARISON OF THE PROPOSED SOLUTIONS FOR IoT SECURITY

Many researches investigate and discuss the security aspects of IoT but with an emphasis on just one level of the IoT architecture. This survey paper observes the security of the whole system, instead of observing the security from a single layer point of view.

<table>
<thead>
<tr>
<th>Proposed solution for the IoT security</th>
<th>Methods for achieving security</th>
<th>Security Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Tahir et al. [24]]</td>
<td>ICMetric (cryptographic keys) coupled with SRRP</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>[Hopkins et al. [25]]</td>
<td>ICMetric (cryptographic keys)</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>[Kovalchuk et al. [26]]</td>
<td>ICMetric (cryptographic keys)</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>[Zhou et al. [27]]</td>
<td>Dynamic IoT security based on the principles of immune system</td>
<td>x x x x</td>
</tr>
<tr>
<td>[Rose [30]]</td>
<td>Key management, watermarking</td>
<td>x x ✓ x</td>
</tr>
<tr>
<td>[Lessa dos Santos et al. [31]]</td>
<td>Nano-electronic security primitives</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>[Kothmayr et al. [32]]</td>
<td>ECC cryptography</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>[Xin [33]]</td>
<td>DTLS handshake and RSA keys</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>[Leo et al. [34]]</td>
<td>AES and ECC hybrid encryption algorithm</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>[Zegzhda and Stepanova [35]]</td>
<td>Secure mediation gateway</td>
<td>x x ✓ ✓</td>
</tr>
<tr>
<td>[Raza et al. [36]]</td>
<td>shared keys</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

In Table II, the authors summarize the security requirements of the proposed solutions and compare them to the existing solutions. The table shows, there are only a small number of solutions that address all aspects of fundamental security requirements.

V. OPEN SECURITY CHALLENGES IN IoT

There are many possible directions for further research in the area of IoT security, primarily due to the ever-growing and all-encompassing nature of IoT. As the number and variety of connected things continues to increase rapidly, simply ensuring scalability is not sufficient to guarantee a successful implementation and practical usefulness of IoT. Challenges such as introducing standards, ensuring Quality of Service, confidentiality and reliability, managing huge amounts of data, and providing energy efficiency still pose major issues that need to be addressed. Open or not fully addressed security challenges in IoT can be broadly categorized as follows: (i) standardization for heterogeneous devices; (ii) extensive deployment and scalability; (iii) confidentiality; (iv) software and hardware vulnerability; (v) physical security of devices; and (vi) energy consumption and efficiency.

VI. CONCLUSION

IoT is expected to integrate advanced technologies of communication, networking, cloud computing, sensing and actuation, and pave the way for groundbreaking applications in a variety of areas, which will affect many aspects of
people’s lives and bring about many conveniences. Nevertheless, given the enormous number of connected devices that are potentially vulnerable, highly significant risks emerge around the issues of security, privacy, and governance in IoT. This survey focuses on the security issues and challenges of IoT, presents an overview of up-to-date IoT security solutions, and presents some of the open challenges in this field. Due to page limitations we are not able to present the details of all the details, however the extended version of this paper will cover detailed explanation of each research problem and future research directions.

REFERENCES