Future Generation Computer Systems 76 (2017) 540–549

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation

Prem Prakash Jayaraman [a,*], Xuechao Yang [b], Ali Yavari [b], Dimitrios Georgakopoulos [a], Xun Yi [b]

[a] Swinburne University of Technology, Melbourne, Victoria, 3122, Australia

[b] RMIT University, Melbourne, Victoria, 3000, Australia

ARTICLE INFO

Article history:
Received 16 March 2016
Received in revised form
16 January 2017
Accepted 1 March 2017
Available online 18 March 2017

Keywords:
Internet of Things
IoT privacy and security
Secure IoT platform

ABSTRACT

The Internet of Things (IoT) is the latest web evolution that incorporates billions of devices that are owned by different organisations and people who are deploying and using them for their own purposes. IoT-enabled harnessing of the information that is provided by federations of such IoT devices (which are often referred to as IoT things) provides unprecedented opportunities to solve internet-scale problems that have been too big and too difficult to tackle before. Just like other web-based information systems, IoT must also deal with the plethora of Cyber Security and privacy threats that currently disrupt organisations and can potentially hold the data of entire industries and even countries for ransom. To realise its full potential, IoT must deal effectively with such threats and ensure the security and privacy of the information collected and distilled from IoT devices. However, IoT presents several unique challenges that make the application of existing security and privacy techniques difficult. This is because IoT solutions encompass a variety of security and privacy solutions for protecting such IoT data on the move and in store at the device layer, the IoT infrastructure/platform layer, and the IoT application layer. Therefore, ensuring end-to-end privacy across these three IoT layers is a grand challenge in IoT. In this paper, we tackle the IoT privacy preservation problem. In particular, we propose innovative techniques for privacy preservation of IoT data, introduce a privacy preserving IoT Architecture, and also describe the implementation of an efficient proof of concept system that utilises all these to ensure that IoT data remains private. The proposed privacy preservation techniques utilise multiple IoT cloud data stores to protect the privacy of data collected from IoT. The proposed privacy preserving IoT Architecture and proof of concept implementation are based on extensions of OpenIoT - a widely used open source platform for IoT application development. Experimental evaluations are also provided to validate the efficiency and performance outcomes of the proposed privacy preserving techniques and architecture.

1. Introduction

"Internet of Things" (IoT) is the latest Internet evolution that involves (i) incorporating billions of internet-connected sensors, cameras, displays, smart phones, wearable, and other smart devices that communicate via the internet (which are collectively referred to as IoT things), and (ii) harnessing their data and functionality to provide novel smart services and products that benefit our society. A recent forecast made by the Gartner projects Internet of Things and the associated ecosystem to be a $1.7 trillion market by 2020 and include 28.1 billion connected things [1]. IoT is fuelling a paradigm shift of a truly connected world in which everyday objects become interconnected, able to communicate directly with each another, and capable of collectively providing smart services [2]. However, in many such applications [3] the data collected by IoT is sensitive and must be kept private and secure. Examples of sensitive IoT data include physiological data collected by (in some cases wearable) biomedical sensors, energy consumption data collected by smart meters, and location data collected by mobile phones to name just a few. The disclosure of such data may create opportunities for criminal activity, or result in serious harm or even death. Therefore from such a perspective, IoT presents a significant challenge for security, privacy and trust, which are considered to be among the remaining main barriers in IoT application development.

* Corresponding author.
E-mail address: prem.jayaraman@gmail.com (P.P. Jayaraman).

http://dx.doi.org/10.1016/j.future.2017.03.001
0167-739X/

Most of existing solutions for protection of privacy-sensitive data in IoT focus on communication channels security and authorisation. Little work has been done to protect sensitive sensor data after they are collected, integrated and stored. This creates opportunities for both hackers and malicious administrators to steal and disclose privacy-sensitive data collected and distilled from IoT devices. To protect such privacy-sensitive data against hacking, we need to develop an IoT platform/infrastructure that ensure end-to-end privacy and security (i.e., starting from the point of data collection from IoT devices thought the point of data harnessing for delivering IoT applications and/or related services).

In this paper we introduce a novel privacy-preserving technique and a related IoT architecture that are designed to protect sensitive IoT sensor data from disclosure and hacking [4,5]. The basic idea in this technique involves two steps. First, each data item x that is collected from an IoT device is randomly transformed to a sum of n numbers, i.e., $x = x_1 + x_2 + x_n (n \geq 2)$, and each addend $x_1, \ldots, x_n$ is stored in a different data store. Therefore, our solution requires the use of n data stores (in a server or/and the cloud) and each data store D_i keeps only the addend x_i of $x (n \geq i \geq 1)$. Second, we also propose the introduction of a homomorphic encryption scheme that allows access to the data collected from IoT devices via the aggregation of their addends, and hence without the risk of exposing sensitive data to hackers or to data store administrators. Even in cases where all but one of the n data stores are compromised, the IoT data remains private. Specifically, this paper makes the following contributions:

- Introduces a privacy-preserving technique for controlling access to sensitive IoT data via decomposing sensitive data to addends that are stored in multiple data stores and then (re)aggregating the IoT data when is requested by a user without exposing any anything beyond meaningless addends.
- Proposes a blueprint for a privacy preserving IoT architecture that provides end-to-end privacy based on the proposed privacy-preserving data access scheme.
- Describes a proof-of-concept system prototype implementation and evaluates its efficiency.

The rest of the paper is organised as follows. In Section 2, we present a survey of the current state-of-the-art in IoT security. In Section 3, we propose and formulate the proposed security technique. In Section 4, we present the blueprint architecture the IoT system that implements the proposed security technique implementation. In Section 5, we present experimental evaluations of the developed system. Section 6 concludes the paper.

2. Related work

IoT is an important new internet technology with great potential for developing smart buildings and cities, assisted living and healthcare, precision agriculture and environmental monitoring, manufacturing, as well as for security and defence [6]. IoT systems and their applications must deal with malicious information disclosure and provide techniques that protect sensitive data, such as patient data in healthcare, energy consumption data from smart energy meters, and location data. IoT poses the following privacy challenges that define the need for novel privacy and data protection techniques [7,8]:

- Lack of control over IoT devices,
- Inferences derived from collected data,
- Pattern extraction from anonymous data, and
- Privacy loss across IoT layers, e.g., devices, infrastructure storage, applications, and related communications.

The need for security and privacy solutions is also highlighted by IoT forensic researchers [9–11].

Existing techniques for protecting sensitive data in IoT have mainly focused on securing the communication channel, as well as user authentication and authorisation. However, there is a significant gap in developing techniques that can ensure privacy in the collection, storage, and retrieval (providing computed aggregations without exposing the data) of IoT data.

2.1. Communication channel security mechanisms

To secure communication in IoT, it is important to encrypt data communicated between IoT devices, gateways and other IoT infrastructure due to the public nature of the Internet. Keys for encryption must be agreed upon by communicating nodes [12,13]. Due to resource constraints, key agreement in IoT is non-trivial. Many key agreement schemes used in general networks, such as Kerberos [14] and RSA [15], may not be suitable for IoT because there is usually no trusted infrastructure in IoT. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. To overcome this problem, a random key pre-distribution scheme [16] was proposed, where each sensor node receives a random subset of keys from a large key pool before deployment and any two nodes can find one common key within their subsets and use that key to secure the communication. Without requiring any key pre-distribution, data sensed within IoT has been used to establish the common secret key. For example, in [17], two sensors S1 and S2 in a Body Sensor Network (BSN) use the common electrocardiogram (EKG) signals of a patient to establish a secret key.

Roman et al. [18], Du et al. [19] and Camtepe et al. [20] analyse the applicability of several link-layer oriented key management systems (KMS), which establish keys for sensor nodes within the same WSN using techniques such as linear algebra, combinatorics and algebraic geometry. However, the authors mention not all mathematical-based KMS protocols can fulfil the IoT context, according to the analysis result, only [19,21] might be suitable for some IoT scenarios. At the end of the paper, the authors recommend to use a trusted third party to enable other key management mechanisms.

OSCAR [22] is a more recent approach for end-to-end security of IoT. It is based on the concept of object security and focuses on securing the message payload to enable secure M2M communication. The novel aspect of OSCAR is the use of cryptography techniques over CoAP protocol to ensure lightweight and scalable encryption. Similarly in [23], the authors propose a lightweight method using (Internet Protocol Security) IPsec for securing end-to-end communication channel between unconstrained peers and IoT devices (constrained). The proposed method makes it possible for an unconstrained node to set up an IPsec-ESP Transport Mode connection with an IoT device while moving the master session key generation and authentication processes from the IoT device to the trusted gateway. The ESP mode (that provides data encryption and authentication) allows the setup of an end-to-end secure connection between two peers by encrypting the payload, therefore, the proposed method relieves the IoT devices from the computational burden associated with the generation of cryptographic data. Under the proposed method, IoT devices can benefit from higher level of cryptosystem without executing the intensive computation. In [24], the authors propose a novel secure and scaled IoT storage system to tackle the aforementioned issues at both data and system levels, which is based on Shamir's secret sharing scheme. There are mainly four components in the proposed system: client, dispatcher, peer managers and regular peers, and the system is organised into three layers: (1) file saving and restoration, (2) connection setup and data transfer, and (3) share replication.