Chapter 107
A Comprehensive Survey on Privacy and Security Issues in Cloud Computing, Internet of Things and Cloud of Things

Syrine Sahmim Ep Guerbouj
National School of Computer Science (ENSI), Manouba University, Tunisia

Hamza Gharsellaoui
https://orcid.org/0000-0002-6171-2621
National Engineering School of Carthage (ENICarthage), Carthage University, Tunisia & National Institute of Applied Sciences and Technology (INSAT), Carthage University, Tunisia & Khurmah University College, Taif University KSA, Saudi Arabia

Sadok Bouamama
https://orcid.org/0000-0002-3840-3978
Higher College of Technology (DMC), Dubai, UAE

ABSTRACT

This journal article deals with the most important existing problems of security and privacy of the Cloud Computing (CC), Internet of Things (IoT) and Cloud of Things (CoT) concepts especially confidentiality issues. With the evolution of ubiquitous computing, everything is connected everywhere, therefore these concepts have been widely studied in the literature. However, due to the systems complexity and the difficulty to control each access attempt, intrusions and vulnerabilities will be more recurrent. To tackle this issue, researchers have been focused on various approaches enforcing security and privacy. In the present article, risk factors and solutions regarding these technologies are reviewed then current and future trends are discussed.

DOI: 10.4018/978-1-7998-5339-8.ch107

1. INTRODUCTION

Today, technology is quickly changing the way we interact with the world around us. Indeed, companies are developing products for the consumer market that would have been unimaginable a decade ago: Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. These are all examples of the Internet of Things (IoT), an interconnected environment where all manner of objects has a digital presence and the ability to communicate with other objects and people. The IoT explosion is already around us, in the form of wearable computers, smart health trackers, smart contracts to developp and facilitate the e-commerce(B2C, B2B and C2C) process and respect the international standard policies as mentionned in (Tripathy et al., 2017), connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn't a mobile phone, tablet, or traditional computer.

It can be noticed that the way we use technologies is changing, a dramatic transformation is shaping the world from isolated systems to ubiquitous Internet-based-enabled 'things'. These things are capable of communicating with each other by sending data which contain valuable information. However, this new world built on the basis of Internet, contains numerous challenges as regard to the security and the privacy perspective.

1.1. Motivation

In recent years, due to the fast development of new and more efficient computing methods, the interest of academics and practitioners has been shifting toward Internet-based Computing. Commonly known applications are Internet of Things (IoT), Cloud Computing (CC) and Cloud of Things (CoT).

After a number of technology variants have appeared over the years, we found a need to classify those that can help secure computing. As a matter of fact, there is no review on which solutions are described as regard to these three points of views (i.e. IoT, CC and CoT). Besides, thousands of users of IoT, CC and CoT are communicating with each other, sharing ressources and exchanging high amount of sensitive data and information impose a great need of additional level of security especially to guaranty confidence in service providers as much as controlling the dissemination of personal data and to detect and eliminate vulnerabilities (Werner et al., 2017) . Thus, in this article, the main challenges for privacy and security purposes are described along with an analyze of various constraints and the main techniques used to face one of them such as how to enable the users control over the dissemination of their attributes and data and wewill expose some works dealing with the same problems and discuss the solutions given and propose an idea to tackle the privacy issues mainly.

1.2. Context

1.2.1. Internet of Things

It is defined as a networked interconnection of devices in everyday use that are often equipped with ubiquitous mechanism. The Internet of Things (IoT) is based on processing of large amount of data in order to provide useful service. Along with physical objects, the IoT is composed of embedded software, electronics and sensors. This allows objects to be controlled remotely via the connected network