Chapter 1
Privacy Preserving in the Modern Era:
A Review of the State of the Art

Rihab Boussada
National School of Computer Science (ENSI), Tunisia & Sesame University, Tunisia

Mohamed Elhoucine Elhdhili
National School of Computer Science (ENSI), Tunisia

Balkis Hamdane
Supcom, Tunisia & Iset'Com, Tunisia

Leila Azouz Saidane
National School of Computer Science (ENSI), Tunisia

ABSTRACT

The development of data communication technologies promotes large-scale sensitive data collection and transmission in various application areas. The sensitivity and criticism of the exchanged data raise several privacy issues. A lack of privacy may cause moral and emotional damage and discrimination. It can even create an unequal society. To fill this gap, a better understanding of privacy concept and its requirements is required. This chapter presents a comprehensive survey of privacy-preserving in the modern era. It deals with this concept of privacy-preserving from all perspectives, classifying its requirements into content-oriented and context-oriented ones. Based on the taxonomy, privacy attacks are described, and approaches and mechanisms for privacy protection are reviewed. A future research direction about privacy preserving in various fields is finally exposed.

DOI: 10.4018/978-1-6684-5250-9.ch001

INTRODUCTION

The common denominator of the emergent technologies and applications is col- lection, aggregation and transfer of personal data. While affirming the important role played by these applications to improve daily life, there are limits that could hinder their adoption. These limits are intrinsically linked to the sensitivity of the personal data exchanged and the risks of their disclosure.

Despite the ethical, legal and social vacuum that surrounds this concept, the privacy preserving is essential for promoting the adoption of each new system in a real environment Eckhoff and Wagner (2017). It is considered as a fundamental and individual right. Indeed, the disclosure of personal data, without the consent and the knowledge of its possessor, may have consequences often tragic. It is therefore necessary to protect the content by using, for example, cryptographic primitives. However, despite the protection of data, the extraction of personal information remains possible. Certainly, the meta-data, contained in the exchanges, are essential to ensure routing, but it is easily accessible by attackers. Indeed, based on these collected meta-data, an attacker can deduce information about his target which may make him subject to discrimination and cause him moral, physical and emotional distress. This observation is under- scored by the quote from Michael Hayden, "We kill people based on meta-data" Cole (2014).

However, privacy issue is relatively little covered in the literature. Indeed, most of the existing proposals do not meet all the privacy requirements. This is probably due to the fact that privacy protection is a complex task for a variety of reasons. Indeed, the privacy concept itself is a notion that is neither formalized nor clearly defined. In this context, it is imperative to circumscribe this issue and precisely define its requirements. A second source of complexity is the absence of a compromise between privacy preserving and performance.

In this article, we explore privacy issues in detail and take an in-depth look at existing protocols and mechanisms. We aim to present the privacy-preserving concept in modern era from the communication perspective. Particularly, this paper:

- gives a detailed explanation of privacy-preserving concept and its fundamental requirements from the communication perspective;
- presents the privacy-preserving message transmission approaches;
- reviews and classifies attacks that compromise privacy
- explores mechanisms and approaches and classifies them according to the privacy preserving properties.

The rest of this article is organized as follows. In Section 2, we present the concept of privacy and present the privacy properties. In Section 3, The privacy attacks and models are exposed. The fundamental message transmission approaches ensuring privacy are explored in Section 4, while exiting protocols and mechanisms are presented in Section 5. The open issues are identified in Section 6. Conclusions are presented in Section 7.

PRIVACY CONCEPT

Privacy is a vague notion and difficult to define Solove (2007). In the literature, there are several definitions of this notion Nair and Tyagi (2021).