Chapter 6
A Cognitive Access Framework for Security and Privacy Protection in Mobile Cloud Computing

Gianmarco Baldini
Joint Research Centre – European Commission, Italy

Pasquale Stirparo
Joint Research Centre – European Commission, Italy

ABSTRACT

Information systems and wireless communications are becoming increasingly present in the everyday life of citizens both from a personal and business point of view. A recent development in this context is Mobile Cloud Computing (MCC), which is the combination of Cloud Computing and pervasive mobile networks. Ensuring the preservation of privacy can be difficult in MCC. Therefore, this chapter provides an overview of the main challenges in ensuring privacy in MCC and surveys the most significant contributions from the research community. The second objective of the chapter is to introduce and describe a new framework for privacy protection based on the concepts of Virtual Object (VO) and Composite Virtual Object (CVO), where data are encapsulated and protected using a sticky policy approach and a role-based access model. The proposed iCore framework is compared to the privacy challenges described in the first objective.

INTRODUCTION

Information systems and wireless communications are becoming increasingly present in the everyday life of citizens both from a personal and business point of view. This trend is supported by various drivers, which include greater business efficiency, improved quality of life, improved access to information and support for mobility. The recent emergence of cases of identity theft described by Ghosh (2010) has shown that the development and deployment of these technologies is still far from perfect and many challenges remain. A key challenge is to ensure that the same citizen's data,

DOI: 10.4018/978-1-4666-4781-7.ch006

which is used in business and personal transactions, is also not used by unauthorized parties or "reused" in contexts or applications that can bring harmful consequences to citizen and businesses.

There are various reasons for the "shortcomings" of the current pervasive information and communication technologies. Regulation and laws for these new issues have not been formulated yet, technologies to protect identity of citizens are still at the premature stage, and applications are often not designed considering privacy and security to be essential.. The Internet paradigm calls for "openness" but this should not mean that personal data is open to the world. In synthesis, there are various gaps and issues in the current regulatory and technology frameworks, which must be addressed.

Some issues are not easy to be resolved because they are part of a trade-off. Regulators, service providers and businesses do not want that the effort to ensure security and privacy is an obstacle to the development of new markets or integration of the old ones. There is a "tussle" between the need for openness to ensure efficient transactions among various applications and the need to restrict the access to data.

Another key element in this context is the evolution of wireless communications and support for mobility. Until a few years ago, wireless communication technology was used by the common citizen mostly for voice. Recent technological evolutions both from network and mobile devices has fostered the provision of data connectivity, which can be used to support new applications in a virtuous cycle: new applications and "hunger" for data support the deployment of networks, which can provide wireless broadband connectivity. At the same time, mobile devices have become increasingly powerful and reconfigurable. The gap between personal computers and mobile devices is now "blurred" in the sense that similar applications and services can be provided on both platforms.

A recent development in this context is MCC, which is the combination of Cloud Computing and mobile networks.

As described in Ghosh (2010) and Han, & Gani (2012), MCC can benefit mobile computing with increased capabilities and improved power efficiency. Mobile devices can rely on cloud computing to perform computationally intensive operations for various purposes such as multimedia or data processing. By offloading the execution of specific operations to the Cloud, mobile devices and networks can also improve power efficiency. The advantages of MCC for extending battery lifetime, improving data storage capacity and processing power are also described in Dinh, Lee, Niyato, and Wang (2011), where are also identified the outstanding issues for the integration of cloud computing and mobile networks. These issues include availability of the systems and their heterogeneity and that mobile networks may not provide the same bandwidth in all areas or time of the day due to different factors like traffic capacity, wireless coverage and propagation errors. The problems related to low bandwidth and high latency of cellular mobile networks are also mentioned in Bahl, Han, Li, and Satyanarayanan (2012), which proposes the seamless integration of cloudlet and public cloud, and infrastructure specialization for mobile applications. The cloudlet concept is described as a trusted cluster of computers mutually connected through a low latency, high bandwidth wireless network, which is well connected to the Internet and is available for use by nearby mobile devices.

From a security and privacy point of view, MCC may also create new issues. Mobile devices may provide users-related data to the Cloud applications to perform the computational intensive operations described above or just for outsourcing storage. Some Cloud applications such as remote healthcare may even process and store sensitive data related to the current health conditions of