Chapter 4
Access Control Challenges in Enterprise Ecosystems:
Blockchain-Based Technologies as an Opportunity for Enhanced Access Control

Hugo Santos Martins
University of Lisbon, Portugal

Sérgio Guerreiro
University of Lisbon, Portugal

ABSTRACT

There is an increasing gap between the needs of modern, complex, and distributed environments in regards to control of access to data and the level to which classical access control solutions can fulfill those needs. The purpose of this chapter is to highlight the current state of art of existing research over access control in increasingly decentralized environments and to argue how the subject of access control is more relevant than ever before, with increasing research opportunities emerging. In this chapter, the authors analyze the current state of the art of access control mechanisms and systems over decentralized applications with a focus on enterprise ecosystems, analyze the current challenges and opportunities that the new technological landscape offers, specifically over the application of blockchain-based technologies in access control, and propose new research directions for the future.

INTRODUCTION

Access control has been a subject of research since the early inceptions of the digital era, from time-sharing systems such as the ADEPT-50 (Weissman, 1969) research conducted in the 1970s (Graham & Denning, 1972; Bell & LaPadula, 1973; Lampson, 1974), cloud computing (Yu, Wang, Ren, & Lou, 2010; Wang, Liu, & Wu, 2010; Wan, Liu, & Deng, 2012; Ruj, Nayak, & Stojmenovic, 2011) and, more recently, over the Internet of Things (IoT) ecosystem (Ouaddah, Mousannif, Abou Elkalam, & Ait Ouahman, 2017;

DOI: 10.4018/978-1-5225-5927-6.ch004

Dorri, Kanhere, & Jurdak, 2016). Nonetheless, it is a subject with endless research opportunities due to the continuous advances offered in the industry.

Although it has been deeply researched, there is an increased perception of its importance due to, among other things, recent and recurring data breaches (Burgess, 2017; Lieber, 2017; The Guardian, n.d.), and the rise of IoT devices' usage and cloud services. Increasingly complex and distributed technological ecosystems, with increasing numbers of users, demand different approaches to the subject of access control and its management. With information and resources increasingly scattered around the globe, in high-functioning distributed clusters of computational capacity, new challenges to the current access control methodologies are emerging. In an increasingly digital world, in which huge quantities of data are created each day, it is becoming a necessity to strengthen and adapt the mechanisms of access control.

A survey over existing decentralized access control solutions (Miltchev, Smith, Prevelakis, Keromytis, & Ioannidis, 2008) for distributed file systems has found issues with ease of use, scalability, and management difficulties, especially over permission revocation. Existing access control solutions for cloud services are either centralized (Calero, Edwards, Kirschnick, Wilcock, & Wray, 2010; Ruj, Nayak, & Stojmenovic, 2011; Yu, Wang, Ren, & Lou, 2010) or rely heavily on complex Public Key Infrastructure and Key Distribution Centers (Ruj, Stojmenovic, & Nayak, 2012; Ruj, Stojmenovic, & Nayak, 2014; Bauer, Garriss, & Reiter, 2005). A review of the state of art over access control in IoT (Ouaddah, Mousannif, Abou Elkalam, & Ait Ouahman, 2017) has suggested a modern approach to access control should be concerned with providing "many and diverse approaches" (p. 242) rather than a "one-size-fits-all approach" (p. 242).

Ouaddah, Mousannif, Elkalam, and Ouahman (2017) suggest that current IoT access control solutions face two main challenges: developing improved access control mechanisms over the classical ones, and developing decentralized approaches to access control in IoT in an effort to improve security and ensure privacy. Access control for the Internet has also been researched by using smart certificates over a centralized architecture (Park & Sandhu, 1999).

Other efforts in researching decentralized access control are either outdated for modern applications (Satyanarayanan, 1989; Karger, 1977) or are purely theoretical (Thomas & Sandhu, 1993). Much of the existing research has been found to be centralized, lacking in implementations, for current systems, lacking in scalability capacities and traceability, focused on IoT or cloud services.

The previous two paragraphs are meant to expose how, even though access control has previously been researched extensively, the industry has continuously posed new challenges to the very concept and mechanisms of access control, as well as its implementations. This chapter aims to analyze and expose the current state of art in access control, over complex and highly distributed, and increasingly decentralized, technological ecosystems, the challenges posed by these new environments and the new research opportunities that are emerging. It is important that a boundary be set between decentralized and distributed applications. This will allow a deeper understanding of the concepts brought forth by this chapter.

In that sense, a distributed system is one that is distributed, geographically, physically or virtually, but may still maintain centralized authority elements, whereas a decentralized system is one that does not possess a centralized authority element, and in which each element is an authority in itself, coordinating the status of the entire system by communicating with other elements, through consensus protocols (Castro & Liskov, 1999). In this context, a decentralized systems is inherently distributed but a distributed system is not necessarily decentralized.