Chapter 57
Secure Mobile Multi Cloud Architecture for Authentication and Data Storage

Karim Zkik
University of Mohammed V in Rabat, Morocco

Ghizlane Orhanou
University of Mohammed V in Rabat, Morocco

Said El Hajji
University of Mohammed V in Rabat, Morocco

ABSTRACT

The use of Cloud Computing in the mobile networks offer more advantages and possibilities to the mobile users such as storing, downloading and making calculation on data on demand and its offer more resources to these users such as the storage resources and calculation power. So, Mobile Cloud Computing allows users to fully utilize mobile technologies to store, to download, share and retrieve their personal data anywhere and anytime. As many recent researches show, the main problem of fully expansion and use of mobile cloud computing is security, and it's because the increasing flows and data circulation through internet that many security problems emerged and sparked the interest of the attackers. To face all this security problems, we propose in this paper an authentication and confidentiality scheme based on homomorphic encryption, and also a recovery mechanism to secure access for mobile users to the remote multi cloud servers. We also provide an implementation of our framework to demonstrate its robustness and efficiently, and a security analysis.

INTRODUCTION

The use of mobile technologies grew by a phenomenal way during the recent years. According to the annual report of Ericsson mobile traffic increased by 55% between 2013 and 2014, more than 4 billion smartphones available on the market in 2016, and 90% of the world population will have a smartphone by 2020. The use of cloud computing has contributed directly to increasing use of mobile services,

because it allows users to freely access and use different platforms and applications, and it allows them to store their data in remote servers that they can access anytime and anywhere.

The major concern of the use of Cloud Mobile is security (Fernando, Seng, & Rahayu, 2013) because many attackers constantly try to take advantage of vulnerabilities in mobile networks to access data stored in the remote cloud servers. The use of multi Cloud Computing (Ardagna, 2015) instead of single cloud allowed to offer more possibility in terms of security and data management (Tebaa, & El Hajji, 2014; Aljawarneh, 2011). It allows among others to reduce the risk of data loss, it duplicates the resources and allows dividing the security tasks across multiple servers.

Despite the use of multi cloud services, there are still number of security concerns that are related to the limitation of mobile device resources, the possibility of connection through any network even if it is not secure and lack of authentication and encryption platforms in the majority of the existing mobile applications, in addition to the risk of infection by worms or other malicious codes (Aljawarneh & others, 2016).

The aim of our work is to develop a security platform that allows user authentication and data encryption. We will use for that the properties of homomorphic encryption to generate a robust electronic signature. Then we'll use the features of multi Cloud computing to enhance the authentication mechanism by dividing the verification tasks on different virtual machines so that an attacker will never be able to recover or intercept passwords or some other personal information of the concerned mobile user. We will also use a mechanism that classify the data according to their degree of sensitivity and generates a new password for each new connection to reduce the risk that an attacker can gain access to user's account. As high availability is one of the main aspects of security in Mobile Cloud Computing networks, we developed a recovery mechanism by adding a new backup server, which communicates with the storage server and can take over in case of infection and attacks or when the storage server is down.

The rest of paper is structured as follows. In section 2 we discuss some security notion that will be used in our framework, we enumerate some security issue of mobile networks in Cloud and Multi Cloud Computing and we present some related works. In section 3 we present our proposed framework, and we detail the generation of the homomorphic signature, the authentication and the confidentiality mechanism, and the recovery scheme. We present also a security analysis to prove the robustness of our framework. In section 4 we conclude the paper.

SECURITY CONCERN IN MOBILE CLOUD COMPUTING

Preliminaries

In this part, we will present some concepts that we used in designing our model, including the multi cloud computing, homomorphic encryption and security requirements in MCC, and we will present the main threats and attacks in a MCC environment.

Mobile Multi Cloud Computing

Mobile Cloud Computing is a model where applications and mobile data are downloaded stored and hosted using cloud computing technology. This technology allowed changing our lives because all data,

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/secure-mobile-multi-cloud-architecture-for-authentication-and-data-storage/224624

Related Content

IoT-Fog-Blockchain Framework: Opportunities and Challenges
Tanweer Alam (2020). *International Journal of Fog Computing (pp. 1-20).*
www.irma-international.org/article/iot-fog-blockchain-framework/266473

FogLearn: Leveraging Fog-Based Machine Learning for Smart System Big Data Analytics
Rabindra K. Barik, Rojalina Priyadarshini, Harishchandra Dubey, Vinay Kumarand Kunal Mankodiya (2018). *International Journal of Fog Computing (pp. 15-34).*
www.irma-international.org/article/foglearn/198410

Multi-Layer Token Based Authentication Through Honey Password in Fog Computing
Praveen Kumar Rayani, Bharath Bhushanand Vaishali Ravindra Thakare (2018). *International Journal of Fog Computing (pp. 50-62).*
www.irma-international.org/article/multi-layer-token-based-authentication-through-honey-password-in-fog-computing/198412

Feedback-Based Resource Utilization for Smart Home Automation in Fog Assistance IoT-Based Cloud
Basetty Mallikarjuna (2020). *International Journal of Fog Computing (pp. 41-63).*
www.irma-international.org/article/feedback-based-resource-utilization-for-smart-home-automation-in-fog-assistance-iot-based-cloud/245709

Collaborating Decision Support and Business Intelligence to Enable Government Digital Connectivity
Leu Fang Yie, Heru Susantoand Desi Setiana (2021). *Web 2.0 and Cloud Technologies for Implementing Connected Government (pp. 95-112).*
www.irma-international.org/chapter/collaborating-decision-support-and-business-intelligence-to-enable-government-digital-connectivity/259736