Mobile client security architecture: a practical approach

1. About the protection of cloud.
2. Mobile environment problems.
3. Offline mode problem.
4. Other works.
5. Our proposed methods: SSS, ABE, MOS
6. Our architecture.
7. Detailed workflow description.
8. Analytics in detail.
9. Common dangerous scenarios.
10. Analysis of security and complexity.
11. Implementation.

Cloud computing is a new paradigm in the world of distributed networking and computation. The basic feature of the cloud environment is providing the elastic, on-demand and secure service for the end-users. While the first two requirements are rather well supported by the cloud platforms in use, the security is the major concern of the cloud providers and governmental organizations as well as academia and research community [1], [2], [3]. For the small and medium-sized enterprises (SME) the cloud environment is often the most cost-effective and easily scalable solution. However, the security and privacy of the sensitive data in the cloud is a major issue.

A common practice to provide a stable security cloud solution is to use the specific type of cloud service: CASB – Cloud Access Security Broker or CAC - Cloud Access Control. These services are specifically designed to bring the security at a single access point and provide the coordination of the most important security measures. It is measured by Gartner report [4] that such systems will be used by 85% of companies by 2020. The reason is that the organization of the security measures at a single control point allows to control and monitor the level of cloud protection much more effectively. The basic features of the CASM are discovery of cloud services, encryption (along with tokenization for better search properties), access control, DLP services, authentication and auditing/alerting services [5]. The protection of the confidential data, according to the standards of CASB deployment should be provided at rest, in transit and in use [6].

The additional security problems and requirements need to be considered when the mobile devices are actively used in the cloud environment [7]. Today we live in the BYOD (Bring-Your-Own-Device) world and the mobile devices pose a serious risk to the SME cloud platforms as the bottleneck of the information security system (ISS). While the enterprise web interface and the cloud environment can be protected by the powerful third-party services such as CASB and CAC, the mobile client is usually light-weighted and generally less protected. The protection scheme used on a mobile device should be both computationally secure as well as resource-constrained due to the battery power limitations [8]. Therefore, the encryption on a mobile device is not a good solution: the proposed schemes are computationally good but lack the security analysis in many cases [9]. The common practice is the shadow user activities monitoring [7]. However, one area of the mobile device usage stays unprotected in all the proposed scenarios.

Suppose, SME uses CASB in order to protect data at rest (server protection), in transit (communication with server), in use (while the client is connected to the network). But what happens when the mobile client goes offline? And even worse - with some sensitive data on board? All powerful cloud-based tools cannot help and the mobile app has to secure itself with its own limited resources. Moreover, the critical point is the difference in strategy of online and offline protection. Due to the resource constraint, we cannot perform the extensive computation and encryption on a device.

In this paper, we consider the concept of the offline mobile client security. We propose a novel approach based on the powerful cryptographic preventive methods such as secret sharing [10] and ABE encryption [11]. Also, we propose to use the analysis of user behavior in order to reduce the risks and harm of the most common threats: the expired user misusing password or the intruder attack. We use the key expiration period and incorporate it safely into our system. Our main target is providing a maximum defence at the minimal resource cost.

The paper is structured as follows. In section 2, we analyze the most common security problems in the mobile cloud environment and the solutions proposed. We mainly concentrate on the offline protection in the BYOD world. In section 3, we give the basic definitions and explanations of the methods used: SSS, ABE, MOS. In section 4 we present our complete solution to the problem of offline mobile client security. In section 5 we trace the workflow of the client activity and analyze the common security breaches. We discuss security proofs for our system in section 5. Section 6 is the practical implementation and analysis of complexity.

[1] <https://cloudsecurityalliance.org/>

[2] <http://www.ciphercloud.com/blog/cloud-data-security-and-eu-data-privacy-rules-compliance-with-encryption-and-tokenization/>

[3] <http://www.gartner.com/technology/topics/cloud-computing.jsp>

[4] <https://www.skyhighnetworks.com/cloud-university/what-is-cloud-access-security-broker/>

[5] <http://www.gartner.com/technology/reprints.do?id=1-2RUEH70&ct=151110&st=sb>

[6] <http://www.ciphercloud.com/blog/cloud-data-encryption-easy/>

[7] <https://securityintelligence.com/how-to-protect-mobile-apps-essentials/>

[8] Abdul Nasir Khan, M. L. Mat Kiah, Mazhar Ali, Shahaboddin Shamshirband, Atta ur Rehman Khan. A Cloud-Manager-Based Re-Encryption Scheme for Mobile Users in Cloud Environment: a Hybrid Approach

[9] Abdul Nasir Khan, M. L. Mat Kiah, Mazhar Ali, Sajjad A. Madani, Atta ur Rehman Khan, Shahaboddin Shamshirband. BSS: block-based sharing scheme for secure data storage services in mobile cloud environment

[10] TODO: reference to SSS papers

[11] TODO reference to ABE papers