Privacy-preserving security solution for cloud services

L. Malina*, J. Hajny, P. Dzurenda and V. Zeman

Department od Telecommunications
Brno University of Technology
Brno, Czech Republic
*malina@feec.vutbr.cz

ABSTRACT
We propose a novel privacy-preserving security solution for cloud services. Our solution is based on an efficient non-bilinear group signature scheme providing the anonymous access to cloud services and shared storage servers. The novel solution offers anonymous authenticationfor registered users. Thus, users' personal attributes (age, valid registration, successful payment) can be proven without revealing users' identity, and users can use cloud services without any threat of profiling their behavior. However, if a user breaks provider's rules, his access right is revoked.Our solution provides anonymous access, unlinkability and the confidentiality of transmitted data. We implement our solution as a proof of concept applicationand present the experimental results. Further, we analyzecurrent privacy preserving solutions for cloud services and group signature schemes as basic parts of privacy enhancing solutions in cloud services. We compare the performance of our solution with the related solutionsand schemes.

Keywords: Anonymous authentication, Cloud services, Cryptography, Encryption, Group signatures, Privacy, Security.

1. Introduction

Cloud services are becoming indisputable parts of modern information and communication systems and step into our daily lives. Some cloud services such as Amazon's Simple Storage Service, Box.net, CloudSafe etc. use user identity, personal data and/or the location of clients.Therefore, these cloud computing services open a number of security and privacy concerns. The current research challenge in cloud services is the secure and privacy-preserving authentication of users. Users, who store their sensitive information like financial information, health records, etc., have a fundamental right of privacy. There are few cryptographic tools and schemes like anonymous authentication schemes, group signatures, zero knowledge protocols that can both hide user identity and provide authentication. The providers of cloud services need to control the authentication process to permit the access of only valid clients to their services. Further, they must be able to revoke malicious clients and reveal their identities.

In practice, hundreds of users can access cloud services at the same time. Hence, the verification process of user access must be as efficient as possible and the computational cryptographic overhead must be minimal.

We propose a novel security solution for cloud services that offers anonymous authentication based on group signatures. We aim mainly on the efficiency of the authentication process and user privacy. Our solution also provides the confidentiality and integrity of transmitted data between users and cloud service providers. Moreover, we implement our solution as a proof-of-concept application and compare the performance of our solution with related schemes. Our results show that our solution is more efficient than the related solutions.

The paper is organized as follow: The next section presents the related work. Then, we analyse cryptographic privacy-preserving schemes used in cloud computing. In section 4, we describe group signatures. In section5, wepresent our solution and we introduce our novel privacy-preserving cryptographic scheme for cloud services in section 6. Section 7contains our experimental results and the performance analysis and comparison. Finally, the conclusion of our work is presented.

2. Related work

Privacy-preserving cloud computing solutions have been developed from theoretical recommendations to concrete cryptographic proposals.

There are many works which deal with general security issues in cloud computing but only few works deal also with user privacy.

The authors [1] explore the cost of common cryptographic primitives (AES, MD5, SHA-1,RSA, DSA, and ECDSA) and their viability for cloudsecurity purposes. The authors deal with the encryption of cloud storage but do not mention privacy-preserving access to a cloud storage.

The work [2] employs a pairing based signature scheme BLS to make the privacy-preserving security audit of cloud storage data by the Third Party Auditor (TPA). The solution uses batch verification to reduce communication overhead from cloud server and computation cost on TPA side.Further, the paper [3] introduces the verification protocols that can accommodate dynamic data files. The paper explores the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in Cloud Computing in a privacy-preserving way.These solutions [2] and [3] provide privacy-preserving public audit but do not offer the anonymous access of users to cloud services.

The work [4] establishes requirements for a secure and anonymous communication system that uses a cloud architecture (Tor and Freenet). Nevertheless, the author does not outline any cryptographic solution. Another non-cryptographic solution ensuring user privacy in cloud scenarios is presented in[5]. The authors propose a client-based privacy manager which reduces the risk of the leakage of user private information.In the paper [6], authors use a non-cryptographic approach to obtain the benefits of the public cloud storagewithout exposing the content of files. The approach is based on redundancy techniques including an information dispersal algorithm (IDA).Nevertheless, these solutions do not protect against the linkability of user sessions which can cause unauthorized user profiling.

Jensen et al. [7] propose an anonymous and accountable access method to cloud based on ring and group signatures. Nevertheless, their proposal uses a group signature scheme [8] which is inefficient because the signature size grows with the number of users.

The work [9] presents a security approach which uses zero-knowledge proofs providing user anonymous authentication. The main drawback of the proposal is a large communication overhead between a user and a cloud server due to the Fiat-Shamir identification scheme [10]. In the work [11], the author uses the CLsignature scheme [12] and zero-knowledge proofs of knowledge to achieve user's anonymous access to services like digital newspapers, digital libraries, music collections, etc.

The work [13] presents a cryptographic scheme to ensure anonymous user access to information and the confidentiality of sensitive documents in cloud storages. The work[14]deals with anonymity and unlinkability in cloud services by provided group signature schemes[15]. In the next section, we analyze the solutions [11], [13] and [14].

3. Performance analysis of cryptographic privacy-preserving solutions used in cloud computing

In this section, we investigate the current cryptographic solutions which provide the anonymous or pseudonymous access to cloud services and shared storages.We aim on the authentication phases used in privacy-preserving cloud services. In the following performance analysis, we take into account only expensive operations like bilinear pairings (p), modular exponentiation (e) and multiplication (m). According to the results of works [16], [17], we omit the fast operations like addition, subtraction or hash functions which have a minimal impact on the overall performance. The times of expensive pairing operations have been measured for example in [25].

Table 1shows the performance analysis of the Blantom solution [11], the Lu et al. solution[13], the Chow et al. solution [14]and our scheme described in Section6. Blantom in [11]proposes a solution