THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Authenticated Dynamic Group Key Mechanism for Data Sharing in the Cloud

J. Subha
M.E., Computer Science and Engineering, Jay Shriram Group of Institutions, India
T. Seenivasan
Assistant Professor, Jay Shriram Group of Institutions, India

Abstract:
Authenticated dynamic group key mechanism for data sharing designs a secure data sharing data in an untrusted cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally it supports efficient user revocation and a new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

Key words: *Identity privacy, Public revocation, Encryption computation*

1. Introduction

Nowadays, various wireless networks such as telecommunication systems, roadside-to-vehicle communication systems and WLANs have become widely available and interconnected. To provide seamless access services for mobile users (e.g., PDA, laptop computer, smart phone and vehicle) without being limited by the geographical coverage of each access point, handover authentication modules have been deployed. Privacy is a serious concern for the above handover authentication services whereas mobile privacy protection is a complicated issue. Users are deeply concerned about their privacy-related information such as the identity, position, and roaming route. Unfortunately, in current handover authentication techniques it is commonly assumed that the APs are trustworthy and would keep users' privacy-related information confidential. However, since such information is extremely sensitive and coveted by many companies, which may use it to improve their business, such an assumption may not be valid. Therefore, a user should be protected from the prying eyes of APs. Without appropriate security and privacy guarantees, users are reluctant to accept such mobile services. To satisfy the security and privacy requirements, it is prerequisite to elaborately design an efficient handover authentication mechanism to achieve security and privacy preservation for practical wireless networks.

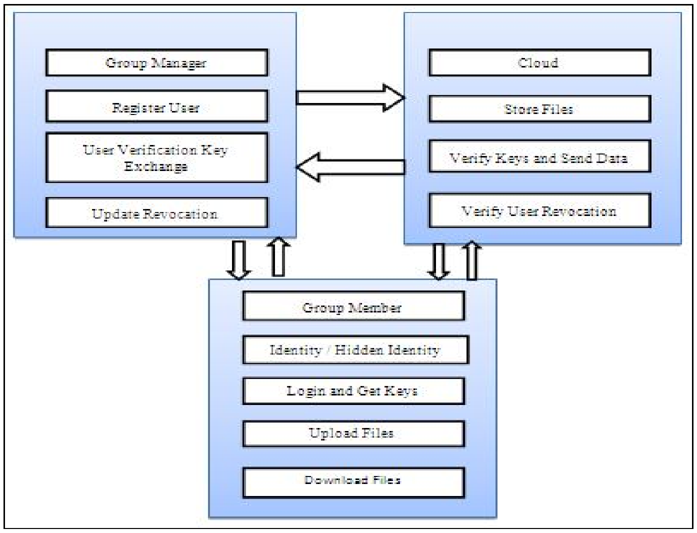

Figure 1: Architecture diagram of Authenticated dynamic data sharing

A secure and efficient handover authentication protocol should satisfy the following requirements. (1) User authentication. (2) Session key establishment. (3) Low communication cost and computation complexity: in general, an MU does not have sufficient resources in comparison with fixed nodes such as APs. Therefore, a handover authentication process should minimize energy consumption of MUs. Additionally; such a process should be fast enough to maintain persistent connectivity. (4) Strong user anonymity and untraced ability: it allows an MU not to expose his private information to eavesdroppers or APs. (5) Provision of user revocation mechanism with forward secrecy: due to some reasons (e.g., the subscription period of a user has expired or a user's secret key has been compromised), handover authentication should allow an AP to find out whether an MU is revoked.

At the same time, however, it should also guarantee the anonymity of the revoked user's protocol runs before the revocation, which means forward secure user revocation. (6) Conditional privacy preservation: although it is desirable to provide strong user anonymity and untraced ability, it is the liability for the AAA server to reveal the related private information (e.g., identity, position) of a user in case of emergency (e.g., enhanced 911 location service mandated by U.S. Federal Communications Commission). (7) AAA server anonymity: besides the identity of the MU, the identity of its AAA server should also be hidden from eavesdroppers and the legitimate network entities except the visited AP.

AHANDOVER authentication protocol enables mobile nodes (e.g., PDA, Laptop PC, smart phone and vehicle) to seamlessly and securely roam over multiple access points. Regardless of the mobile networking technology involved, a typical handover authentication scenario involves three parties: mobile nodes (MNs), access points (APs) and the authentication server (AS). An MN registers to AS, and then connects to any AP for accessing its subscribed services. When the MN moves from the current AP (e.g., AP1) into a new AP (e.g., AP2), handover authentication should be performed at AP2. Through handover authentication, AP2 authenticates the MN to reject any access request by an unauthorized user. Also, a session key should be established between the MN and AP2 to protect the data exchanged over the connection subsequently.

One of the most fundamental services offered by cloud providers is data storage. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans.

2. Existing System

Single owner data access, single-owner manner, where only the group manager can store and modify data in the cloud. However, the single owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others. A cryptographic storage system that enables secure file sharing on entrusted servers. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

A secure provenance scheme, which is built upon group signatures and cipher text-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs encrypted data with her group signature key for privacy preserving and traceability.

3. Proposed System

None of the existing privacy-aware cryptographic primitives such as blind signature, ring signature, and group signature techniques, suits our purpose given the security and efficiency requirements discussed above. Blind signature and ring signature can only provide unconditional privacy, while Pair Hand demands conditional privacy, and hence, revocable anonymity.

The privacy preserving technique based on pseudonyms. Since MNs generally have large storage capacity, rendering the preloading of a large pool of pseudonyms from AS feasible. A recent work quantitatively studied the storage space requirement for preloading anonymous keys (i.e., pseudonyms) and associated certificates for long term use (i.e., one year). Their results are obtained based on quantifying the upper and lower bounds on the pseudonym change interval for maintaining a satisfactory degree of privacy. Since the preloading method in handover authentication protocol involves a pool of shorter-lived pseudonyms, the memory consumption is bounded by the results given by. The preload-and-replenish mechanism has been proposed by many researchers and works efficiently.

4.Results

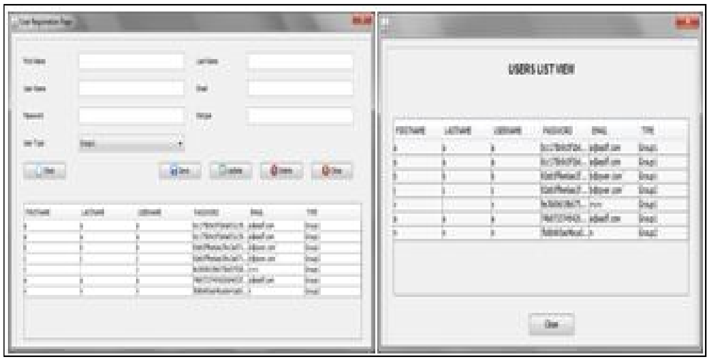

Figure 2: Screenshots for Group Manager

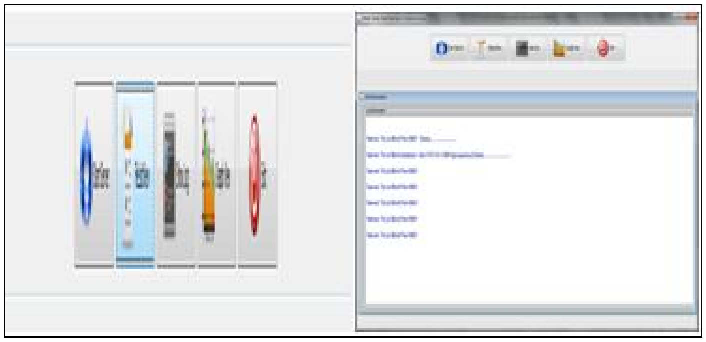

Figure 3: Screenshots for Cloud Server

Figure 4: Screenshots for Group Member

5. Conclusion

Authenticated dynamic group key mechanism for data sharing designs a secure data sharing data in an entrusted cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally it supports efficient user revocation and a new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

6. References

1. A. Fiat and M. Naor, “Broadcast Encryption,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.
2. B. Sheng and Q. Li, “Verifiable Privacy-Preserving Range Query Two-Tiered Sensor Networks,” Proc. IEEE INFOCOM, Proc. IEEE INFOCOM, pp.46-50, 2008.
3. D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.
4. D. Boneh, X. Boyen, and H. Shacham, “Short Group Signature,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004