Formal Analyze of a Private Access Control Protocol to a Cloud Storage

Mouhebeddine Berrima[1], Pascal Lafourcade[2], Matthieu Giraud[2] and Narjes Ben Rajeb[3]
[1]LIP2, *Université de Monastir, Monastir, Tunisia*
[2]LIMOS, *Université Clermont Auvergne, Aubière, France*
[3]LIP2, *Université Tunis El-Manar, Tunis, Tunisia*
[1]*berrima.mouheb@gmail.com*,[2]{*first.last*}*@uca.fr*, [3]*narjes.benrajeb@gmail.com*

Keywords: Cloud storage, formal methods, attribute based signature, attribute based encryption, data and user privacy.

Abstract: Storing data in the Cloud makes challenging data's security and users' privacy. To address these problems cryptographic protocols are usually designed. Cryptographic primitives have to guarantee some security properties such that data and user privacy or authentication. *Attribute-Based Signature* (ABS) and *Attribute-Based Encryption* (ABE) are very suitable for storing data on an untrusted remote entity. In this work, we formally analyze the Ruj *et al.* protocol of cloud storage based on ABS and ABE schemes. We model the protocol and its security properties with ProVerif an automatic tool for the verification of cryptographic protocols. We discover an unknown attack against user privacy. We propose a correction, and automatically prove the security of the corrected protocol with ProVerif.

1 INTRODUCTION

Cloud storage refers data storage services hosted over the Internet. The cloud users store data online, so that they or any other authorized users can access them from any location via the Internet. However, the share of the sensitive data on a third party through a public network brings some security challenges. In particular, there are concerns with the privacy of users and data. Protecting privacy in cloud is more difficult than in traditional environments, because sensitive data may be disseminated and stored over many external location, managed by external service providers (Wang et al., 2010a), and both cloud and user can be malicious (Mulazzani et al., 2011; Zhang et al., 2012). User privacy is required in many applications when users store sensitive information like financial or health data (Tang et al., 2012). There are two important privacy requirements when a user stores data on the cloud: *anonymity* and *unlinkability*. The ISO/IEC standard (governmental organisations, 2009) define anonymity as the property ensuring that a user may use a service or a ressource without disclosing his (or her) identity. However, preserving the anonymity property may still release information about a user by allowing an adversary to track several uses of a resource by the same user. Such information might allow an adversary to deduce or at least restrict the possible identities of a user. Therefore, the unlinkability property is required, ensuring that the different uses of a service or a ressource for the same user should not be linked by an adversary. On the other hand, the Cloud Service Provider (CSP) must authenticate the user to be sure that he has the right to store data on the cloud, moreover this authentication must be done without reveal any information about his identity. Attribute-Based Signature (ABS) is a cryptographic scheme privacy-preserving authentication. Indeed, in ABS the verifier of a signature can only check if the message is signed by authorized one without knowing any information about its identity.

Data Privacy has been also gained research interest because only authorized users have access to sensitive data on the cloud. Data must be protected when transmitted to CSP and during the storage. The protection is against the unauthorized users as well as the CSP since the cloud is often assumed to be honest but curious (Li et al., 2010; Yu et al., 2010). To ensure data privacy, several works propose the storage of data in encrypted form. Thus, if the storage is compromised, then the leaked information should be protected. Identity based cryptography is not feasible in this situation because the inability of users to share their encrypted data at a fine-grained level. *Attribute-Based Encryption* (ABE), introduced by Sahai and Waters (Sahai and Waters, 2005), solves the problem of fine grained access control. There are two complementary forms of ABE (Goyal et al.,

2006): *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) and *Key-Policy Attribute-Based Encryption* (KP-ABE). In CP-ABE, the users have given a set of attributes and the data are encrypted under an access policy described as Boolean formula. Only users having the attributes satisfying the access policy can decrypt the ciphertext. In KP-ABE, the situation is reversed: users are associated with access policies and ciphertexts are encrypted with sets of attributes.

Related Work: (Bertino et al., 2009; Angin et al., 2010; Chow et al., 2012) proposed approaches to deal with security and privacy. In (Bertino et al., 2009), the privacy of users is preserved with zero-knowledge proof protocols while it is based on anonymous identification in (Angin et al., 2010). Recently, taking advantages of ABS and ABE has emerged as a widely accepted approach by the cloud security community (Ruj et al., 2012; Li et al., 2010; Zhao et al., 2011). The ABS is used to ensure the authentication while hiding anonymity, and the ABE allows a fine-grained access control to data. The protocol proposed by (Ruj et al., 2012) is among the pioneering works to use ABS and ABE. The protocol uses the SSH protocol to secure the communication between the users and the cloud, and supports reading and writing data stored in the cloud.

Contributions: We analyze the Ruj *et al.* protocol (Ruj et al., 2012) which we abbreviate *RSN'12* protocol. We model it in the applied π-calculus (Abadi and Fournet, 2001).We use ProVerif tool (Blanchet et al., 2001) to analyze cryptographic protocols (Puys and Lafourcade, 2015; Cremers et al., 2009). For sake of simplicity, we consider one attribute in our modeling of the ABE and ABS schemes. We formalize and verify the fundamental security properties of the protocol. In writing mode, we verify the writer authentication and writer privacy which is expressed by the anonymity of writer's identity and unlinkability, that is a user who stores data on the cloud. While in reading mode, we check the required property that is data privacy. We show that the unlinkability of a writer is not satisfied against an attack in which the adversary delays the messages of some writers. Then, we propose a fix, which prevents this attack.

Outline: We give a description of RSN'12 protocol in Section 2. We model RSN'12 protocol in Section 3 and analyze the security properties in Section 4. Finally, we conclude in Section 5.

2 RSN'12 PROTOCOL DESCRIPTION

In (Ruj et al., 2012) the authors propose a protocol for reading and writing data stored in the cloud which is based on the decentralized approach of CP-ABE (Lewko and Waters, 2011) and ABS (Maji et al., 2008) where many authorities distribute secret keys associated to attribute. Using ABS the cloud verifies the authenticity of a user without knowing his identity before storing data. Using ABE only valid users are able to decrypt the stored data. The protocol makes the following assumptions:

1. The CSP is honest-but-curious, i.e. it tries to derive some information from the messages he learned during the execution of the protocol, but cannot modify the user's content.
2. Users can have a read or/and write access to a file stored in the CSP.
3. All the communications between participants are secured by SSH (Secure Shell) protocol.

The RSN'12 protocol involves a user who may be a writer or/and a reader, a Trusty Authority (TA) registering users, one or more Key Distribution Center (KDC) issuing the secret keys associated to users' attributes, and a CSP. The TA and the KDC are trusted entities while the CSP is semi-trusted. Some users can be malicious and thus are considered as untrusted entities. The protocol is composed of three sub-protocols.

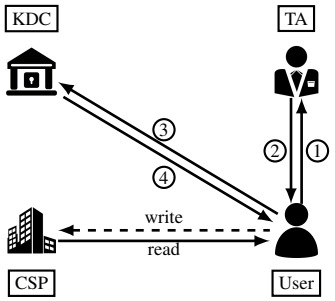

Figure 1: RSN'12 protocol.

Registering and getting attribute secret keys. In a first phase, a user gets attribute secret keys from the KDCs by presenting his token obtained from TA:

- The user presents his identity to the TA, for instance a federal government (① in Fig. 1).
- TA registers the user if he is eligible and gives him a token as described in ABS scheme (② in Fig. 1). TA embeds a random value in the token which will be incorporate in the attribute secret keys for signing to prevents collusion of the users.
- The user on presenting the token to the KDC receives secret attribute keys for signing and de-

cryption (③ in Fig. 1). The KDC checks the validity of the token using TA's public key, and sends the corresponding keys for signing and decryption (④ in Fig. 1).

Writing on the cloud. To store a message MSG on the cloud, the user proceeds as follows:

- He creates an access policy $\mathcal{X}$ containing all required fields, and encrypts the message MSG under $\mathcal{X}$ as $C = Encrypt(MSG, \mathcal{X})$.
- Then he calculates the message $C_1 = \mathcal{H}(C)\|\tau$ where $\mathcal{H}$ is a hash function, τ is a timestamp and $\|$ is the concatenation operation. The timestamp is used to prevent the user to use stale message back with a valid signature, when his attributes have been revoked. Next, he generates the signature σ of C_1 with a claim policy $\mathcal{Y}$.
- Finally, he sends $c = (C, \tau, \sigma, \mathcal{Y})$ to the CSP. Then CSP verifies, using $Verify$ algorithm, if the message $\mathcal{H}(C)\|\tau$ was signed by a user satisfying the claim policy $\mathcal{Y}$.

Reading from the cloud. A user can access at any time to the data and requests a ciphertext, then the CSP sends the requested ciphertext using SSH. Note that, the authors do not propose any revocation model, but it is still possible to incorporate it. The protocol is clear but contains some ambiguities. We discuss these minor problems and explain how to fix them.

3 MODELING RSN'12 PROTOCOL

In this section we describe the Proverif processes used to model RSN'12 protocol.

The main process. It is specified as the parallel composition of the processes modeling the roles of writers, readers, TA, KDC and CSP. First, the fresh secret keys used respectively by the TA, the KDC, and the CSP for asymmetric encryption and signature, are generated. Their corresponding public keys are then sent on a public channels, i.e. they are made available to the adversary. Moreover, the fresh secret keys used in ABS and ABE schemes, are also generated and their corresponding public keys are published. The secret keys of the writer and the reader are made under replication to model an infinite number of writers and readers. The processes writer and reader are under replication, because one user may establish many sessions with the CSP. In our modeling, we use public keys of asymmetric encryption as identities of participants.

The writer process. The writer process models the role of a writer. After the receipt of a token form the TA, the writer sends a request to the KDC to get attribute secret key for signing, this request is encoded by a pair `(token,write)`. Afterwards, the writer encrypts his message and signs it using the attribute secret key.

The reader process. At first, a reader behaves as a writer by requesting a token from the TA and an attribute secret key for decryption from the KDC. Next, it has access to the CSP, to read a message stored on the cloud. Finally, he decrypts the message read from the CSP using his attribute secret key, and behaves as a sub-process with the received message.

The KDC process. When receiving a request from a user, the KDC checks the correctness of the token using the public key of user used as its identity, which was authenticated during SSH authentication protocol. If the token is valid, it issues an attribute secret key for encryption or signing following the mode access "write" or "read".

The CSP process. The CSP is responsible of the storage of user data.If the signature is valid with respect to the claim policy, the CSP stores the message that becomes immediately accessible by the readers. A reader access directly to the CSP to read a file.

4 SECURITY ANALYSIS

We analyse the security properties of the protocol. All proofs of our propositions are not presented because they are directly implied by our ProVerif codes.

4.1 Confidentiality

It means that a user without valid access policy cannot decrypt the data stored on the cloud. In applied π-calculus this property can be expressed as a secrecy property: it should be impossible for an adversary, interacting with the protocol and without valid attribute secret key, to learn a message which is encrypted and stored on the cloud.

Definition 1. *Given an access policy AP, a cloud storage protocol ensures confidentiality if a secret message stored on the cloud by an honest writer is not deducible by an attacker without attribute secret key satisfying AP.*

Proving secrecy property is expressed by the reachability notion. We request ProVerif to check that a private message, encrypted using a public access policy, cannot be deduced by the attacker. Proverif proves this property in less one minute.

Proposition 1. *RSN'12 protocol ensures the confidentiality property.*

4.2 Writer Authentication

A user can only write in the cloud if he has the attribute validating the claim policy. Moreover, an invalid user can not receive attribute from a KDC, if does not have the token from TA. Authentication property can be captured as a correspondence assertion. To define the authentication of a writer, we annotate the protocol by the following events:

- AcceptSign: This event is placed inside the CSP's process and emitted if the signature is valid, i.e. `absCheckSign` returns true.
- DelivKeySign(IdUser): This event is placed inside the KDC's process and emitted when the KDC issues an attribute secret key for signing to a user with identity IdUser.
- DelivToken(IdUser): This event is placed inside the TA's process and emitted when the TA delivers a token to a user with identity IdUser.

Definition 2. *A cloud storage protocol ensures the authentication of a writer with identity Id if for every execution trace of the protocol each occurrence of the event AcceptSign is preceded by an occurrence of DelivKeySign(Id) which is preceded by an occurrence of DelivToken(Id).*

This property can be expressed in ProVerif in terms of nested correspondence (Blanchet, 2009) which allows us to order events. ProVerif can automatically prove the corresponding nested correspondence in less one second:

$$event(acceptSign) \Rightarrow (event(DelivKeySign(pkwriter)) \Rightarrow event(DelivToken(pkwriter)))$$

Proposition 2. *RSN'12 protocol satisfies the authentication of a writer.*

4.3 Writer Privacy

In the context of cloud storage, writer privacy is expressed by two properties; anonymity and unlinkability. Anonymity of a writer's identity is ensured if it is not possible for anyone, even the CSP, to learn the writer's identity of a stored message. Unlinkability means that no one can link the messages stored on the cloud, more precisely no one is able to decide if two messages were stored by the same writer, or not.

Anonymity: A cloud storage system ensures anonymity if it keeps the writer's identity secret from everyone. Hence, anonymity can be formalized as a secrecy property: no one can deduce the identity of a writer who store a message on the cloud. Since the identities of the writers are known values, anonymity is captured by the concept of *strong secrecy*. Strong secrecy means that the adversary cannot distinguish two instances of the same protocol with two different values of the secret. For the precise definition, we refer the reader to (Blanchet, 2004). In ProVerif, strong secrecy is expressed by diff-equivalence defined between processes that share the same structure and differ only in the choice of terms representing the secret values (Blanchet et al., 2008).

Definition 3. *A cloud storage protocol ensures anonymity of a writer's identity if for any two writers with identities IdW_1, IdW_2 and for any message msg, an adversary cannot distinguish whether msg comes from IdW_1 or IdW_2.*

We request to ProVerif to check if

$$C[Writer(IdW_1, msg)] \approx C[Writer(IdW_2, msg)].$$

with $C[\_]$ is an evaluation context modeling the whole cloud storage protocol as described in main process with a hole for a writer process, and the process $Writer(IdW, msg)$ models a writer with identity IdW storing a message msg on the cloud. ProVerif succeeds to prove this request in 3 seconds.

Proposition 3. *RSN'12 protocol preserves anonymity of writer's identity.*

Unlinkability: Informally, in cloud storage context, unlinkability holds when the differents stored messages of the same writer can not be linked by an attacker even a dishonest user (writer or reader). Thus, unlinkability can be viewed as the secrecy of link between writer and its messages stored on the cloud. The definition of unlikability is similar to the definition of voter privacy in e-voting protocol (Kremer and Ryan, 2005) in the sense that we must consider at least two honest writers. To understand this assumption, consider the case where all the writers are dishonest except one, as the stored messages on the cloud are published by the CSP, the dishonest writers can collude and determine the message of the honest writer.

Definition 4. *A cloud storage protocol ensures unlinkability if for any two writers with identities IdW_1, IdW_2 and for any two messages $msg1$ and $msg2$, an adversary cannot distinguish the situation in which IdW_1 stores $msg1$ and IdW_2 stores $msg2$ from the situation in which IdW_1 stores $msg2$ and IdW_2 stores $msg1$.*

In applied π-calculus this definition can be formalized as the following equivalence:

$$C[Writer(IdW_1, msg1)|Writer(IdW_2, msg2)] \approx C[Writer(IdW_1, msg2)|Writer(IdW_2, msg1)],$$

where $C[\_]$ is an evaluation context modeling the whole protocol with a hole for two writers. In ProVerif, the above pair of process can be expressed as single biprocess as follows:

$$C[Writer(IdW_1, choice[msg_1, msg_2])] \mid C[Writer(IdW_2, choice[msg_2, msg_1])] .$$

ProVerif finds an attack, in which a man-in-the-middle attacker selectively delays or delete some messages sent to the CSP by one writer until he can link a message to somebody.

Proposition 4. *RSN'12 protocol does not ensure unlinkability property.*

For this attack we consider an attacker that is a semi-honest reader with valid attribute secret keys, who wants link the messages to a writer. In a real cloud storage environment, to achieve the attack, an attacker performs the following steps:

- Access to CSP and memorize all the files stored in the cloud.
- Listen to the network, and wait for a message send to the CSP.
- When a new message *MSG* is sent, he identifies its sender *IdW* and blocks all the messages sent to CSP after the message *MSG*. He now has just to wait until *MSG* becomes available on the CSP, i.e. CSP appends *MSG* to the previous files.
- Then, he can access to the files and then learn *MSG* by comparing the current contents of files with the previous contents. Thus, he concludes that *MSG* was sent by a writer with identity *IdW* and can link a file to somebody.

Fixed protocol: To fix this problem, a solution is that the CSP simultaneously publishes at least two incoming messages from different persons. However, the messages are accessible from a file, so if the messages are written on the file in a deterministic order, for instance following arriving time of the messages, the adversary can link a message with its writer by inspecting the order of the sent messages to the CSP on the network. Then, the CSP must write the incoming messages on the files in non-deterministic way.

Proposition 5. *The revisited RSN'12 protocol ensures unlinkability property.*

5 CONCLUSION

In this paper, we revisit the security of the protocol of (Ruj et al., 2012).We use ProVerif to prove automatically claimed security properties by the authors in the original paper. ProVerif helps us to discover a flaw in this protocol for the unlinkability property. We then give a correction and prove the security of the modified version with ProVerif. The next step is to use our framework to model and analyze more protocols using ABE and ABS in order to discover flaws or formally prove the security of these protocols.

ACKNOWLEDGEMENTS

This research was conducted with the support of the FEDER program of 2014-2020, the region council of Auvergne-Rhône-Alpes, the Indo-French Centre for the Promotion of Advanced Research (IFCPAR) and the Center Franco-Indien Pour La Promotion De La Recherche Avancée (CEFIPRA) through the project DST/CNRS 2015-03 under DST-INRIA-CNRS Targeted Programme.

REFERENCES

Abadi, M. and Fournet, C. (2001). Mobile values, new names, and secure communication. In *ACM SIGPLAN Notices*, volume 36, pages 104–115. ACM.

Adams, C., Cain, P., Pinkas, D., and Zuccherato, R. (2001). Internet x.509 public key infrastructure time-stamp protocol (tsp). RFC 3161.

Angin, P., Bhargava, B., Ranchal, R., Singh, N., Linderman, M., Othmane, L. B., and Lilien, L. (2010). An entity-centric approach for privacy and identity management in cloud computing. In *Reliable Distributed Systems, 2010 29th IEEE Symposium on*, pages 177–183.

Bertino, E., Paci, F., Ferrini, R., and Shang, N. (2009). Privacy-preserving digital identity management for cloud computing. *IEEE Data Eng. Bull.*, 32(1):21–27.

Blanchet, B. (2004). Automatic proof of strong secrecy for security protocols. In *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, pages 86–100.

Blanchet, B. (2009). Automatic verification of correspondences for security protocols. *J. Comput. Secur.*, 17(4):363–434.

Blanchet, B., Abadi, M., and Fournet, C. (2008). Automated verification of selected equivalences for security protocols. *The Journal of Logic and Algebraic Programming*, 75(1):3–51.

Blanchet, B. et al. (2001). An efficient cryptographic protocol verifier based on prolog rules. In *CSFW*, volume 1.

Blanchet, B. and Smyth, B. (2016). Automated reasoning for equivalences in the applied pi calculus with barriers. In *CSF'16*, pages 310–324.

Chow, S. S., He, Y.-J., Hui, L. C., and Yiu, S. M. (2012). Spice–simple privacy-preserving identity-management for cloud environment. In *International Conference on Applied Cryptography and Network Security*, pages 526–543. Springer.

Cremers, C. J. F., Lafourcade, P., and Nadeau, P. (2009). Comparing state spaces in automatic security protocol analysis. In *Formal to Practical Security - Papers Issued from the 2005-2008 French-Japanese Collaboration*, pages 70–94. Springer.

governmental organisations (2009). Iso 15408-2: Common criteria for information technology security evaluation - part 2: Security functional components.

Govinda, K. and Sathiyamoorthy, E. (2012). Identity anonymization and secure data storage using group signature in private cloud. *Procedia Technology*, 4:495–499.

Goyal, V., Pandey, O., Sahai, A., and Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In *ACM CCS'06*.

Kremer, S. and Ryan, M. (2005). Analysis of an electronic voting protocol in the applied pi calculus. In *European Symposium on Programming*, pages 186–200.

Lewko, A. and Waters, B. (2011). Decentralizing attribute-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 568–588. Springer.

Li, M., Yu, S., Ren, K., and Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In *International Conference on Security and Privacy in Communication Systems*, pages 89–106. Springer.

Maji, H. K., Prabhakaran, M., and Rosulek, M. (2008). Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. *IACR Cryptology ePrint Archive*, 2008:328.

Mulazzani, M., Schrittwieser, S., Leithner, M., Huber, M., and Weippl, E. (2011). Dark clouds on the horizon: Using cloud storage as attack vector and online slack space. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11.

Puys, M. and Lafourcade, P. (2015). Evaluations of cryptographic protocols: Verification tools dealing with algebraic properties. In *Foundations and Practice of Security - FPS 2015*. Springer.

Ruj, S., Nayak, A., and Stojmenovic, I. (2011). Dacc: Distributed access control in clouds. In *TrustCom'11*, pages 91–98. IEEE.

Ruj, S., Stojmenovic, M., and Nayak, A. (2012). Privacy preserving access control with authentication for securing data in clouds. In *Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on*, pages 556–563. IEEE.

Sahai, A. and Waters, B. (2005). Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 457–473. Springer.

Tang, Z., Wang, X., Jia, L., Zhang, X., and Man, W. (2012). Study on data security of cloud computing. In *Engineering and Technology (S-CET), 2012 Spring Congress on*, pages 1–3. IEEE.

Wang, B. Y., Ming, J., Zhang, S. M., Jiang, H., and Luo, H. (2014). An access control method based on cp-abe and abs algorithm in cloud storage. In *Applied Mechanics and Materials*, volume 644, pages 1919–1922. Trans Tech Publ.

Wang, C., Ren, K., Lou, W., and Li, J. (2010a). Toward publicly auditable secure cloud data storage services. *IEEE Network*, 24(4):19–24.

Wang, G., Liu, Q., and Wu, J. (2010b). Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In *ACM CCS'10*, pages 735–737.

Ylonen, T. and Lonvick, C. (2006). The secure shell (ssh) authentication protocol. RFC 4252, RFC Editor.

Yu, S., Wang, C., Ren, K., and Lou, W. (2010). Attribute based data sharing with attribute revocation. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*.

Zhang, G., Yang, Y., Zhang, X., Liu, C., and Chen, J. (2012). Key research issues for privacy protection and preservation in cloud computing. In *Second International Conference on Cloud and Green Computing, CGC'12*, pages 47–54.

Zhao, F., Nishide, T., and Sakurai, K. (2011). Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems. In *International Conference on Information Security Practice and Experience*, pages 83–97. Springer.