

Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds

Sushmita Ruj, *Member, IEEE*, Milos Stojmenovic, *Member, IEEE*, and
Amiya Nayak, *Senior Member, IEEE*

Abstract—We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

Index Terms—Access control, authentication, attribute-based signatures, attribute-based encryption, cloud storage

1 INTRODUCTION

RESEARCH in cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. This frees users from the hassles of maintaining resources on-site. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).

Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement.

Recently, Wang et al. [2] addressed secure and dependable cloud storage. Cloud servers prone to Byzantine failure, where a storage server can fail in arbitrary ways [2]. The cloud is also prone to data modification and server colluding attacks. In server colluding attack, the adversary can compromise storage servers, so that it can modify data files as long as they are internally consistent. To provide secure data storage, the data needs to be encrypted. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption [3], [4]. The keywords are sent to the cloud encrypted, and the cloud returns the result without knowing the actual keyword for the search. The problem here is that the data records should have keywords associated with them to enable the search. The correct records are returned only when searched with the exact keywords.

Security and privacy protection in clouds are being explored by many researchers. Wang et al. [2] addressed storage security using Reed-Solomon erasure-correcting codes. Authentication of users using public key cryptographic techniques has been studied in [5]. Many homomorphic encryption techniques have been suggested [6], [7] to ensure that the cloud is not able to read the data while performing computations on them. Using homomorphic encryption, the cloud receives ciphertext of the data and performs computations on the ciphertext and returns the encoded value of the result. The user is able to decode the result, but the cloud does not know what data it has operated on. In such circumstances, it must be possible for the user to verify that the cloud returns correct results.

Accountability of clouds is a very challenging task and involves technical issues and law enforcement. Neither clouds nor users should deny any operations performed or requested. It is important to have log of the transactions performed; however, it is an important concern to decide

- S. Ruj is with Indian Statistical Institute, 203 B.T. Road, Kolkata 700108, India. E-mail: sush@isical.ac.in.
- M. Stojmenovic is with the Univerzitet Singidunum, Danijelova 32, Belgrade 11000, Serbia. E-mail: mstojmenovic@singidunum.ac.rs.
- A. Nayak is with the School of Electrical Engineering and Computer Science, University of Ottawa, 800 King Edward, Ottawa K1N6N5, ON, Canada. E-mail: anayak@site.uottawa.ca.

Manuscript received 30 Sept. 2012; revised 28 Dec. 2012; accepted 11 Jan. 2013; published online 14 Feb. 2013.

Recommended for acceptance by X. Li, P. McDaniel, R. Poovendran, and G. Wang.

For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDSSI-2012-09-1006.

Digital Object Identifier no. 10.1109/TPDS.2013.38.

how much information to keep in the log. Accountability has been addressed in TrustCloud [8]. Secure provenance has been studied in [9].

Considering the following situation: A law student, Alice, wants to send a series of reports about some malpractices by authorities of University *X* to all the professors of University *X*, research chairs of universities in the country, and students belonging to Law department in all universities in the province. She wants to remain anonymous while publishing all evidence of malpractice. She stores the information in the cloud. Access control is important in such case, so that only authorized users can access the data. It is also important to verify that the information comes from a reliable source. The problems of access control, authentication, and privacy protection should be solved simultaneously. We address this problem in its entirety in this paper.

Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking). There are broadly three types of access control: *user-based access control* (UBAC), *role-based access control* (RBAC), and *attribute-based access control* (ABAC). In UBAC, the access control list contains the list of users who are authorized to access data. This is not feasible in clouds where there are many users. In RBAC (introduced by Ferraiolo and Kuhn [10]), users are classified based on their individual roles. Data can be accessed by users who have matching roles. The roles are defined by the system. For example, only faculty members and senior secretaries might have access to data but not the junior secretaries. ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data. For instance, in the above example certain records might be accessible by faculty members with more than 10 years of research experience or by senior secretaries with more than 8 years experience. The pros and cons of RBAC and ABAC are discussed in [11]. There has been some work on ABAC in clouds (for example, [12], [13], [14], [15], [16]). All these work use a cryptographic primitive known as attribute-based encryption (ABE). The eXtensible access control markup language [17] has been proposed for ABAC in clouds [18].

An area where access control is widely being used is health care. Clouds are being used to store sensitive information about patients to enable access to medical professionals, hospital staff, researchers, and policy makers. It is important to control the access of data so that only authorized users can access the data. Using ABE, the records are encrypted under some access policy and stored in the cloud. Users are given sets of attributes and corresponding keys. Only when the users have matching set of attributes, can they decrypt the information stored in the cloud. Access control in health care has been studied in [12] and [13].

Access control is also gaining importance in online social networking where users (members) store their personal information, pictures, videos and share them with selected groups of users or communities they belong to. Access control in online social networking has been studied in [19]. Such data are being stored in clouds. It is very important that only the authorized users are given access to those information. A similar situation arises when data is stored in clouds, for example, in Dropbox, and shared with certain groups of people.

It is just not enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user. For example, a user would like to store some sensitive information but does not want to be recognized. The user might want to post a comment on an article, but does not want his/her identity to be disclosed. However, the user should be able to prove to the other users that he/she is a valid user who stored the information without revealing the identity. There are cryptographic protocols like ring signatures [20], mesh signatures [21], group signatures [22], which can be used in these situations. Ring signature is not a feasible option for clouds where there are a large number of users. Group signatures assume the pre-existence of a group which might not be possible in clouds. Mesh signatures do not ensure if the message is from a single user or many users colluding together. For these reasons, a new protocol known as attribute-based signature (ABS) has been applied. ABS was proposed by Maji et al. [23]. In ABS, users have a claim predicate associated with a message. The claim predicate helps to identify the user as an authorized one, without revealing its identity. Other users or the cloud can verify the user and the validity of the message stored. ABS can be combined with ABE to achieve authenticated access control without disclosing the identity of the user to the cloud.

Existing work [12], [13], [14], [15], [16], [18], [38] on access control in cloud are centralized in nature. Except [38] and [18], all other schemes use ABE. The scheme in [38] uses a symmetric key approach and does not support authentication. The schemes [12], [13], [16] do not support authentication as well. Earlier work by Zhao et al. [15] provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. We, therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. Although Yang et al. [34] proposed a decentralized approach, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, Ruj et al. [16] proposed a distributed access control mechanism in clouds. However, the scheme did not provide user authentication. The other drawback was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. In the preliminary version of this paper [1], we

extend our previous work with added features that enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. In this version we also address user revocation, that was not addressed in [1]. We use ABS scheme [24] to achieve authenticity and privacy. Unlike [24], our scheme is resistant to replay attacks, in which a user can replace fresh data with stale data from a previous write, even if it no longer has valid claim policy. This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud. We, therefore, add this extra feature in our scheme and modify [24] appropriately. Our scheme also allows writing multiple times which was not permitted in our earlier work [16].

1.1 Our Contributions

The main contributions of this paper are the following:

1. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.
2. Authentication of users who store and modify their data on the cloud.
3. The identity of the user is protected from the cloud during authentication.
4. The architecture is decentralized, meaning that there can be several KDCs for key management.
5. The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized.
6. Revoked users cannot access data after they have been revoked.
7. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information.
8. The protocol supports multiple read and write on the data stored in the cloud.
9. The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.

1.2 Organization

The paper is organized as follows: Related work is presented in Section 2. The mathematical background and assumptions are detailed in Section 3. We present our privacy preserving access control scheme in Section 4 followed by a real life example in Section 5. The security is analyzed in Section 6. Computation complexity is discussed in Section 7, and comparison with other work is presented in Section 8. We conclude in Section 9.

2 RELATED WORK

ABE was proposed by Sahai and Waters [26]. In ABE, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs. In key-policy ABE or KP-ABE (Goyal et al. [27]), the sender has an access policy to encrypt data. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to

decrypt information if it has matching attributes. In Ciphertext-policy, CP-ABE ([28], [29]), the receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates.

All the approaches take a centralized approach and allow only one KDC, which is a single point of failure. Chase [30] proposed a multiauthority ABE, in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Multiauthority ABE protocol was studied in [31] and [32], which required no trusted authority which requires every user to have attributes from at all the KDCs. Recently, Lewko and Waters [35] proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices. To get over this problem, Green et al. [33] proposed to outsource the decryption task to a proxy server, so that the user can compute with minimum resources (for example, hand held devices). However, the presence of one proxy and one KDC makes it less robust than decentralized approaches. Both these approaches had no way to authenticate users, anonymously. Yang et al. [34] presented a modification of [33], authenticate users, who want to remain anonymous while accessing the cloud.

To ensure anonymous user authentication ABSs were introduced by Maji et al. [23]. This was also a centralized approach. A recent scheme by Maji et al. [24] takes a decentralized approach and provides authentication without disclosing the identity of the users. However, as mentioned earlier in the previous section it is prone to replay attack.

3 BACKGROUND

In this section, we present our cloud storage model, adversary model and the assumptions we have made in the paper. Table 1 presents the notations used throughout the paper. We also describe mathematical background used in our proposed solution.

3.1 Assumptions

We make the following assumptions in our work:

1. The cloud is honest-but-curious, which means that the cloud administrators can be interested in viewing user's content, but cannot modify it. This is a valid assumption that has been made in [12] and [13]. Honest-but-curious model of adversaries do not tamper with data so that they can keep the system functioning normally and remain undetected.
2. Users can have either read or write or both accesses to a file stored in the cloud.
3. All communications between users/clouds are secured by secure shell protocol, SSH.

3.2 Formats of Access Policies

Access policies can be in any of the following formats: 1) Boolean functions of attributes, 2) linear secret sharing scheme (LSSS) matrix, or 3) monotone span programs. Any access structure can be converted into a Boolean function

TABLE 1
Notations

Symbols	Meanings
U_u	u -th User/Owner
\mathcal{A}_j	j -th KDC
\mathcal{A}	Set of KDCs
L_j	Set of attributes that KDC \mathcal{A}_j possesses
$l_j = L_j $	Number of attributes that KDC \mathcal{A}_j possesses
$I[j, u]$	Set of attributes that \mathcal{A}_j gives to user U_u for encryption/decryption
I_u	Set of attributes that user U_u possesses
$J[j, u]$	Set of attributes that \mathcal{A}_j gives to user U_u for claim attributes
J_u	Set of attributes that user U_u possesses as claim attributes
$AT[j]$	KDC which has attribute j
$PK[j]/SK[j]$	Public key/secret key of KDC \mathcal{A}_j for encryption/decryption
$sk_{i,u}$	Secret key given by \mathcal{A}_j corresponding to attribute i given to user U_u
TPK/PSK	Trustee public key/secret key
$APK[j]/ASK[j]$	Public key/secret key of KDC \mathcal{A}_j for verifying claim
\mathcal{X}	Boolean access structure
\mathcal{Y}	Claim policy
τ	Time instant
R	Access matrix of dimension $m \times h$
M	Matrix of dimension $l \times t$ corresponding to the claim predicate
MSG	Message
$ MSG $	Size of message MSG
C	Ciphertext
H, \mathcal{H}	Hash functions, example SHA-1

[35]. An example of a Boolean function is $((a_1 \wedge a_2 \wedge a_3) \vee (a_4 \wedge a_5)) \wedge (a_6 \vee a_7)$, where a_1, a_2, \dots, a_7 are attributes.

Let $\mathcal{Y} : \{0, 1\}^n \rightarrow \{0, 1\}$ be a monotone Boolean function [24]. A monotone span program for \mathcal{Y} over a field \mathbb{F} is an $l \times t$ matrix M with entries in \mathbb{F} , along with a labeling function $a : [l] \rightarrow [n]$ that associates each row of M with an input variable of \mathcal{Y} , such that, for every $(x_1, x_2, \dots, x_n) \in \{0, 1\}^n$, the following condition is satisfied:

$$\begin{aligned} \mathcal{Y}(x_1, x_2, \dots, x_n) = 1 &\Leftrightarrow \exists v \in \mathbb{F}^{1 \times l} : vM \\ &= [1, 0, 0, \dots, 0] \text{ and } (\forall i : x_{a(i)} \\ &= 0 \Rightarrow v_i = 0). \end{aligned}$$

In other words, $\mathcal{Y}(x_1, x_2, \dots, x_n) = 1$ if and only if the rows of M indexed by $\{i | x_{a(i)} = 1\}$ span the vector $[1, 0, 0, \dots, 0]$. Span programs can be constructed from Boolean functions in a similar way as shown later in Section 5.

3.3 Mathematical Background

We will use bilinear pairings on elliptic curves. Let G be a cyclic group of prime order q generated by g . Let G_T be a group of order q . We can define the map $e : G \times G \rightarrow G_T$. The map satisfies the following properties:

1. $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G$ and $a, b \in \mathbb{Z}_q$, $\mathbb{Z}_q = \{0, 1, 2, \dots, q-1\}$.
2. Nondegenerate: $e(g, g) \neq 1$.

Bilinear pairing on elliptic curves groups is used. We do not discuss the pairing functions which mainly use Weil and Tate pairings [36] and computed using Miller's algorithm. The choice of curve is an important consideration because it determines the complexity of pairing operations.

3.4 Attribute-Based Encryption

ABE with multiple authorities as proposed by Lewko and Waters [35] proceeds as follows [16]:

3.4.1 System Initialization

Select a prime q , generator g of G_0 , groups G_0 and G_T of order q , a map $e : G_0 \times G_0 \rightarrow G_T$, and a hash function $H : \{0, 1\}^* \rightarrow G_0$ that maps the identities of users to G_0 . The hash function used here is SHA-1. Each KDC $\mathcal{A}_j \in \mathcal{A}$ has a set of attributes L_j . The attributes disjoint ($L_i \cap L_j = \emptyset$ for $i \neq j$). Each KDC also chooses two random exponents $\alpha_i, y_i \in \mathbb{Z}_q$. The secret key of KDC \mathcal{A}_j is

$$SK[j] = \{\alpha_i, y_i, i \in L_j\}. \quad (1)$$

The public key of KDC \mathcal{A}_j is published

$$PK[j] = \{e(g, g)^{\alpha_i}, g^{y_i}, i \in L_j\}. \quad (2)$$

3.4.2 Key Generation and Distribution by KDCs

User U_u receives a set of attributes $I[j, u]$ from KDC \mathcal{A}_j , and corresponding secret key $sk_{i,u}$ for each $i \in I[j, u]$

$$sk_{i,u} = g^{\alpha_i} H(u)^{y_i}, \quad (3)$$

where $\alpha_i, y_i \in SK[j]$. Note that all keys are delivered to the user securely using the user's public key, such that only that user can decrypt it using its secret key.

3.4.3 Encryption by Sender

The encryption function is $ABE.Encrypt(MSG, \mathcal{X})$. Sender decides about the access tree \mathcal{X} . LSSS matrix R can be derived as described in Section 3.2. Sender encrypts message MSG as follows:

1. Choose a random seed $s \in \mathbb{Z}_q$ and a random vector $v \in \mathbb{Z}_q^h$, with s as its first entry; h is the number of leaves in the access tree (equal to the number of rows in the corresponding matrix R).
2. Calculate $\lambda_x = R_x \cdot v$, where R_x is a row of R .
3. Choose a random vector $w \in \mathbb{Z}_q^h$ with 0 as the first entry.
4. Calculate $\omega_x = R_x \cdot w$.
5. For each row R_x of R , choose a random $\rho_x \in \mathbb{Z}_q$.
6. The following parameters are calculated:

$$\begin{aligned} C_0 &= MSG e(g, g)^s, \\ C_{1,x} &= e(g, g)^{\lambda_x} e(g, g)^{\alpha_{\pi(x)} \rho_x}, \forall x, \\ C_{2,x} &= g^{\rho_x} \forall x, \\ C_{3,x} &= g^{y_{\pi(x)} \rho_x} g^{\omega_x} \forall x, \end{aligned} \quad (4)$$

where $\pi(x)$ is mapping from R_x to the attribute i that is located at the corresponding leaf of the access tree.

7. The ciphertext C is sent by the sender (it also includes the access tree via R matrix):

$$C = \langle R, \pi, C_0, \{C_{1,x}, C_{2,x}, C_{3,x}, \forall x\} \rangle. \quad (5)$$

3.4.4 Decryption by Receiver

The decryption function is $ABE.Decrypt(C, \{sk_{i,u}\})$, where C is given by (5). Receiver U_u takes as input ciphertext C , secret keys $\{sk_{i,u}\}$, group G_0 , and outputs message msg . It

obtains the access matrix R and mapping π from C . It then executes the following steps:

1. U_u calculates the set of attributes $\{\pi(x) : x \in X\} \cap I_u$ that are common to itself and the access matrix. X is the set of rows of R .
2. For each of these attributes, it checks if there is a subset X' of rows of R , such that the vector $(1, 0, \dots, 0)$ is their linear combination. If not, decryption is impossible. If yes, it calculates constants $c_x \in \mathbb{Z}_q$, such that $\sum_{x \in X'} c_x R_x = (1, 0, \dots, 0)$.
3. Decryption proceeds as follows:
 - a. For each $x \in X'$, $dec(x) = \frac{C_{1,x} e(H(u), C_{3,x})}{e(sk_{\pi(x),u}, C_{2,x})}$.
 - b. U_u computes $MSG = C_0 / \prod_{x \in X'} dec(x)$.

3.5 Attribute-Based Signature Scheme

ABS scheme [24] has the following steps.

3.5.1 System Initialization

Select a prime q , and groups G_1 and G_2 , which are of order q . We define the mapping $\hat{e} : G_1 \times G_1 \rightarrow G_2$. Let g_1, g_2 be generators of G_1 and h_j be generators of G_2 , for $j \in [t_{max}]$, for arbitrary t_{max} . Let \mathcal{H} be a hash function. Let $A_0 = h_0^{a_0}$, where $a_0 \in \mathbb{Z}_q^*$ is chosen at random. $(TSig, TVer)$ mean $TSig$ is the private key with which a message is signed and $TVer$ is the public key used for verification. The secret key for the trustee is $TSK = (a_0, TSig)$ and public key is $TPK = (G_1, G_2, \mathcal{H}, g_1, A_0, h_0, h_1, \dots, h_{t_{max}}, g_2, TVer)$.

3.5.2 User Registration

For a user with identity U_u the KDC draws at random $K_{base} \in G$. Let $K_0 = K_{base}^{1/a_0}$. The following token γ is output

$$\gamma = (u, K_{base}, K_0, \rho), \quad (6)$$

where ρ is signature on $u \| K_{base}$ using the signing key $TSig$.

3.5.3 KDC Setup

Choose $a, b \in \mathbb{Z}_q^*$ randomly and compute: $A_{ij} = h_j^a, B_{ij} = h_j^b$, for $A_i \in \mathbb{A}, j \in [t_{max}]$. The private key of i th KDC is $ASK[i] = (a, b)$ and public key $APK[i] = (A_{ij}, B_{ij} | j \in [t_{max}])$.

3.5.4 Attribute Generation

The token verification algorithm verifies the signature contained in γ using the signature verification key $TVer$ in TPK . This algorithm extracts K_{base} from γ using (a, b) from $ASK[i]$ and computes $K_x = K_{base}^{1/(a+bx)}$, $x \in J[i, u]$. The key K_x can be checked for consistency using algorithm $ABS.KeyCheck(TPK, APK[i], \gamma, K_x)$, which checks

$$\hat{e}(K_x, A_{ij} B_{ij}^x) = \hat{e}(K_{base}, h_j),$$

for all $x \in J[i, u]$ and $j \in [t_{max}]$.

3.5.5 Sign

The algorithm

$$ABS.Sign(TPK, \{APK[i] : i \in AT[u]\}, \\ \gamma, \{K_x : x \in J_u\}, MSG, \mathcal{Y}),$$

has input the public key of the trustee, the secret key of the signer, the message to be signed and the policy claim \mathcal{Y} . The

policy claim is first converted into the span program $M \in \mathbb{Z}_q^{l \times t}$, with rows labeled with attributes. M_x denotes row x of M . Let π' denote the mapping from rows to the attributes. So, $\pi'(x)$ is the mapping from M_x to attribute x . A vector v is computed that satisfies the assignment $\{x : x \in J[i, u]\}$. Compute $\mu = \mathcal{H}(MSG \| \mathcal{Y})$. Choose $r_0 \in \mathbb{Z}_q^*$ and $r_i \in \mathbb{Z}_q, i \in J_u$ and compute:

$$Y = K_{base}^{r_0}, S_i = (K_i^{r_{v_i}})^{r_0} \cdot (g_2 g_1^\mu)^{r_i} (\forall i \in J_u), \quad (7)$$

$$W = K_0^{r_0}, P_j = \prod_{i \in AT[u]} (A_{ij} B_{ij}^{\pi'(i)})^{M_{ij} r_i} (\forall j \in [t]). \quad (8)$$

The signature is calculated as

$$\sigma = (Y, W, S_1, S_2, \dots, S_t, P_1, P_2, \dots, P_t). \quad (9)$$

3.5.6 Verify

Algorithm

$$ABS.Verify(TPK, \sigma = (Y, W, S_1, S_2, \dots, S_t, \\ P_1, P_2, \dots, P_t), MSG, \mathcal{Y}),$$

converts \mathcal{Y} to the corresponding monotone program $M \in \mathbb{Z}_q^{l \times t}$, with rows labeled with attributes. Compute $\mu = \mathcal{H}(MSG \| \mathcal{Y})$. If $Y = 1$, $ABS.Verify = 0$ meaning false. Otherwise, the following constraints are checked

$$\hat{e}(W, A_0) \stackrel{?}{=} \hat{e}(Y, h_0), \quad (10)$$

$$\prod_{i \in I} \hat{e}(S_i, A_{ij} B_{ij}^{\pi'(i)})^{M_{ij}} \stackrel{?}{=} \begin{cases} \hat{e}(Y, h_1) \hat{e}(g_2 g_1^\mu, P_1), j = 1, \\ \hat{e}(g_2 g_1^\mu, P_j), j > 1, \end{cases} \quad (11)$$

where $i' = AT[i]$.

4 PROPOSED PRIVACY PRESERVING AUTHENTICATED ACCESS CONTROL SCHEME

In this section, we propose our privacy preserving authenticated access control scheme. According to our scheme a user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS, as discussed in Sections 3.4 and 3.5, respectively. We will first discuss our scheme in details and then provide a concrete example to demonstrate how it works. We refer to the Fig. 1. There are three users, a creator, a reader, and writer. Creator Alice receives a token γ from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token γ . There are multiple KDCs (here 2), which can be scattered. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 1, SK s are secret keys given for decryption, K_x are keys for signing. The message MSG is encrypted under the access policy \mathcal{X} . The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy \mathcal{Y} , to prove her authenticity and signs the message under this claim. The ciphertext C with signature is c , and is sent to the cloud. The cloud verifies the signature and stores

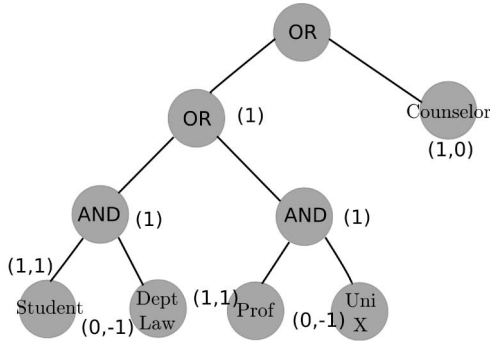


Fig. 2. Example of claim policy.

malpractices by authorities of University X to all the professors of University X , Research chairs of universities X, Y, Z and students belonging to Law department in university X . She wants to remain anonymous, while publishing all evidence. All information is stored in the cloud. It is important that users should not be able to know her identity, but must trust that the information is from a valid source. For this reason she also sends a claim message which states that she “Is a law student” or “Is a student counselor” or “Professor at university X .” The tree corresponding to the claim policy is shown in Fig. 2.

The leaves of the tree consists of attributes and the intermediary nodes consists of Boolean operators. In this example the attributes are “Student,” “Prof,” “Dept Law,” “Uni X ,” “Counselor.” The above claim policy can be written as a Boolean function of attributes as

((Student AND Dept Law) OR (Prof AND Uni X)) OR (Student Counselor).

Boolean functions can also be represented by access tree, with attributes at the leaves and $AND(\wedge)$ and $OR(\vee)$ as the intermediate nodes and root. Boolean functions can be converted to LSSS matrix as below: Let $v[x]$ be parents vector. If node $x = AND$, then the left child is $(v[x]|1)$, and the right child is $(0, \dots, 1)$. If $x = OR$, then both children also have unchanged vector $v[x]$. Finally, pad with 0s in front, such that all vectors are of equal length. The proof of validity of the algorithm is given in [25]. We do not present it here due to lack of space.

Using this algorithm, the span program for this policy is

$$M = \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & 1 \\ 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

An assignment $v = (v_1, v_2, v_3, v_4, v_5)$ satisfies this span program if $vM = (1, 0)$.

The cloud should verify that Alice indeed satisfies this claim. Since she is a law student, $v = (1, 1, 0, 0, 0)$ and is a valid assignment. As a valid user she can then store all the encrypted records under the set of access policy that she has decided. The access policy in case of Alice is

((Prof AND Uni. X) OR
(Research Chair AND ((Uni X OR Uni Y) OR Uni Z)) OR
((Student AND Dept Law) AND Uni X).

Later when a valid user, say Bob wants to modify any of these reports he also attaches a set of claims which the cloud verifies. For example, Bob is a research chair and might send a claim “Research chair” or “Department head” which is then verified by the cloud. It then sends the encrypted data to the Bob. Since Bob is a valid user and has matching attributes, he can decrypt and get back the information.

If Bob wants to read the contents without modifying them, then there is no need to attach a claim. He will be able to decrypt only if he is a Professor in University X or a Research chair in one of the universities X, Y, Z or a student belonging to Department of Law in university X .

Here it is to be noted that the attributes can belong to several KDCs. For example, the Professors belonging to university X have credentials given by the university X , and the Ph.D. degree from a University P , the student counselor might be a psychologist authorized by the Canadian Psychological Association and assigned an employee number by a university, the research chairs can be jointly appointed by the universities X, Y, Z and the government. The students can have credentials from the university and also a department.

Initially, Alice goes to a trustee, for example, the Canadian health service and presents her a health insurance number or federal agency presents her a social insurance number. Either or both of these trustees can give her token(s) $\gamma = (u, K_{base}, K_0, \rho)$. With the token she approaches the KDCs in the university X and department D and obtains the secret keys for decryption and for keys K_x and K_y for signing the assess policy. She can also access the public keys $APK[i]$ of other KDCs. The entire process is carried on in the following way:

5.1 Data Storage in Clouds

Let the data be denoted by MSG , \mathcal{X} is the access policy

((Prof AND Uni. X) OR
(Research Chair AND ((Uni X OR Uni Y) OR Uni Z)) OR
((Student AND Dept Law) AND Uni X).

Alice encrypts the data and obtains the ciphertext

$$C = Enc(MSG, \mathcal{X}).$$

Alice also decides on a claim policy \mathcal{Y} which is shown in Fig. 2. From the matrix, $v = (1, 1, 0, 0, 0)$ can be calculated. The values of $Y, W, S_1, S_2, S_3, S_4, S_5, P_1, P_2$ can be calculated. $\mu = \mathcal{H}(MSG \parallel \mathcal{Y})$. The current time stamp τ is attached to the ciphertext to prevent replay attacks. The signature σ is calculated as $ABS.Sign$. The ciphertext

$$c = (C, \tau, \sigma, \mathcal{Y}).$$

is then send to the cloud. The cloud verifies the signature using the function $ABS.Verify$ as given in (11). If Alice has valid credentials then the ciphertext (C, τ) is stored, else it is discarded.

5.2 Reading from the Cloud and Modifying Data

Suppose Bob wants to access the records stored by Alice. Bob then decrypts the message MSG using his secret keys using function $ABE.Decrypt$. Writing proceeds like file creation. It is to be noted that the time τ is added to the data so that even if Bob’s credentials are revoked, he cannot write stale data in the cloud.

6 SECURITY OF THE PROTOCOL

In this section, we will prove the security of the protocol. We will show that our scheme authenticates a user who wants to write to the cloud. A user can only write provided the cloud is able to validate its access claim. An invalid user cannot receive attributes from a KDC, if it does not have the credentials from the trustee. If a user's credentials are revoked, then it cannot replace data with previous stale data, thus preventing replay attacks.

Theorem 1. *Our access control scheme is secure (no outsider or cloud can decrypt ciphertexts), collusion resistant and allows access only to authorized users.*

Proof. We first show that no unauthorized user can access data from the cloud. We will first prove the validity of our scheme. A user can decrypt data if and only if it has a matching set of attributes. This follows from the fact that access structure S (and hence matrix R) is constructed if and only if there exists a set of rows X' in R , and linear constants $c_x \in \mathbb{Z}_q$, such that $\sum_{x \in X'} c_x R_x = (1, 0, \dots, 0)$. A proof of this appear in [25, Chapter 4].

We note that

$$dec(x) = \frac{C_{1,x} e(H(u), C_{3,x})}{e(sk_{\pi(x),u}, C_{2,x})} = e(g, g)^{\lambda_x} e(H(u), g)^{\omega_x}. \quad (14)$$

Thus,

$$\begin{aligned} \prod_{x \in X'} dec(x) &= \prod_{x \in X'} (e(g, g)^{\lambda_x} e(H(u), g)^{\omega_x})^{c_x} \\ &= e(g, g)^s. \end{aligned} \quad (15)$$

Equation (15) above holds because $\lambda_x = R_x \cdot v$ and $\omega_x = R_x \cdot w$, where $v \cdot (1, 0, \dots, 0) = r$ and $w \cdot (1, 0, \dots, 0) = 0$. $C_0 / \prod_{x \in X'} dec(x) = C_0 / e(g, g)^s = M$.

For an invalid user, there does not exist attributes corresponding to rows x , such that $\sum_{x \in X'} c_x R_x = (1, 0, \dots, 0)$. Thus, $e(g, g)^s$ cannot be calculated.

We next show that two or more users cannot collude and gain access to data that they are not individually supposed to access. Suppose that there exist attributes $\pi(x)$ from the colluders, such that $\sum_{x \in X} c_x R_x = (1, 0, \dots, 0)$. However, $e(H(u), g)^{\omega_x}$ needs to be calculated according to (15). Since different users have different values of $e(H(u), g)$, even if they combine their attributes, they cannot decrypt the message.

We next observe that the cloud cannot decode stored data. This is because it does not possess the secret keys $sk_{i,u}$ (by (3)). Even if it colludes with other users, it cannot decrypt data which the users cannot themselves decrypt, because of the above reason (same as collusion of users). The KDCs are located in different servers and are not owned by the cloud. For this reason, even if some (but not all) KDCs are compromised, the cloud cannot decode data. \square

Theorem 2. *Our authentication scheme is correct, collusion secure, resistant to replay attacks, and protects privacy of the user.*

Proof. We first note that only valid users registered with the trustee(s) receive attributes and keys from the KDCs. A

TABLE 2
Notations

Symbols	Computation
E_x	Exponentiation in group G_x
τ_H	Time to hash using function H
$\tau_{\mathcal{H}}$	Time to hash using function \mathcal{H}
$\tau_P / \tau_{\hat{P}}$	Time taken to perform 1 pairing operation in e/\hat{e}
$ G $	Size of group G
a	Number of KDCs which contribute keys to user

user's token is $\gamma = (u, K_{base}, K_0, \rho)$, where ρ is signature on $u \| K_{base}$ with $TSig$ belonging to the trustee. An invalid user with a different user-id cannot create the same signature because it does not know $TSig$.

We next show that only a valid user with valid access claim is only able to store the message in the cloud. This follows from the functions $ABS.Sign$ and $ABS.Verify$ given in Section 3.5. A user who wants to create a file and tries to make a false access claim, cannot do so, because it will not have attribute keys K_x from the related KDCs. At the same time since the message is encrypted, a user without valid access policy cannot decrypt and change the information.

Two users cannot collude and create an access policy consisting of attributes shared between them. Suppose, there are two users A and B who have attributes x_A and x_B , respectively. They have the following information K_{baseA}, K_{x_A} and K_{baseB}, K_{x_B} , respectively. A new value of $K_{x_B} = K_{baseA}^{1/(a+bx')}$ cannot be calculated by B, because it does not know the values of (a, b) . Thus, the authentication is collusion secure.

Our scheme is resistant to replay attacks. If a writer's access claims are revoked, it cannot replace a data with stale information from previous writes. This is because it has to attach a new time stamp τ and sign the message $\mathcal{H}(C) \| \tau$ again. Since it does not have attributes, it cannot have a valid signature. \square

The mathematical proofs of security of our scheme follows from the security proofs of [23], [35] and has been omitted for the lack of space.

7 COMPUTATION COMPLEXITY

In this section, we present the computation complexity of the privacy preserving access control protocol. We will calculate the computations required by users (creator, reader, writer) and that by the cloud. Table 2 presents notations used for different operations.

The creator needs to encrypt the message and sign it. Creator needs to calculate one pairing $e(g, g)$. Encryption takes two exponentiations to calculate each of $C_{1,x}$. So this requires $2mE_T$ time, where m is the number of attributes. User needs to calculate three exponentiation to calculate $C_{2,x}$ and $C_{3,x}$. So time taken for encryption is $(3m+1)E_0 + 2mE_T + \tau_P$. To sign the message, Y, W, S'_j s and P_j s have to be calculated as well as $\mathcal{H}(C)$. So, time taken to sign is $(2l+2)E_1 + 2tE_2 + \tau_{\mathcal{H}}$.

The cloud needs to verify the signature. This requires checking for (11). Time taken to verify is $(l+2t)\tau_{\hat{P}} + l(E_1 + E_2) + \tau_{\mathcal{H}}$. To read, a user needs only to decrypt the

TABLE 3
Comparison of Our Scheme with Existing Access Control Schemes

Schemes	Fine-grained access control	Centralized/Decentralized	Write/read access	Type of access control	Privacy preserving authentication	User revocation?
[38]	Yes	Centralized	1-W-M-R	Symmetric key cryptography	No authentication	No
[12]	Yes	Centralized	1-W-M-R	ABE	No authentication	No
[13]	Yes	Centralized	1-W-M-R	ABE	No authentication	No
[16]	Yes	Decentralized	1-W-M-R	ABE	No authentication	Yes
[33]	Yes	Centralized	1-W-M-R	ABE	No authentication	No
[34]	Yes	Decentralized	1-W-M-R	ABE	Not privacy preserving	Yes
[15]	Yes	Centralized	M-W-M-R	ABE	Authentication	No
Ours	Yes	Decentralized	M-W-M-R	ABE	Authentication	Yes

TABLE 4
Comparison of Computation and Size of Ciphertext While Creating a File

Schemes	Computation by creator	Computation by cloud	Size of ciphertext
[12]	$(m+2)E_0$	0	$m \log G_0 + G_T + m \log m + MSG $
[13]	$(m+2)E_0$	0	$m \log G_0 + G_1 + MSG $
[16]	$(3m+1)E_0 + 2mE_T + \tau_P$ (encrypt)	0	$2m G_0 + m G_T + m^2 + MSG $
[33]	$(2m+1)E_0 + E_T + \tau_P$ (encrypt)	$mE_0 + mE_T + (m+1)T_p$	$(2m+1) G_0 + G_T + m^2 + MSG $
[34]	$(4m+1)E_0 + 2aE_T + \tau_P$ (encrypt)	$3maE_T + (3ma+1)\tau_P$	$(3m+1) G_0 + G_T + m^2 + MSG $
[15]	$E_1 + (2m+1)E_0 + m\tau_H$ (encrypt) $(2l+2)E_1 + 2tE_2 + \tau_H$ (sign)	$(l+2t)\tau_P + l(E_1 + E_2) + \tau_H$ (verify)	$ G_2 + (2m+1) G_1 + MSG $ $+ (l+t+2) G_1 + m^2$
Our approach	$(3m+1)E_0 + 2mE_T + \tau_P$ (encrypt) $(2l+2)E_1 + 2tE_2 + \tau_H$ (sign)	$(l+2t)\tau_P + l(E_1 + E_2) + \tau_H$ (verify)	$2m G_0 + m G_T + m^2 + MSG $ $+ (l+t+2) G_1 $

TABLE 5
Comparison of Computation during Read and Write by User and Cloud

Schemes	Computation by user while write	Computation by user while read	Computation by cloud while write
[12]	No write access	$m\tau_P$	No write access
[13]	No write access	$m\tau_P$	No write access
[16]	No write access	$2m\tau_P + \tau_H + O(mh)$	No write access
[33]	No write access	$E_0 + \tau_H + O(mh)$	No write access
[34]	No write access	$E_0 + \tau_H + O(mh)$	No write access
[15]	$E_1 + (2m+1)E_0 + m\tau_H$ (encrypt) $(2l+2)E_1 + 2tE_2 + \tau_H$ (sign)	$(2m+1)\tau_P$ (decrypt)	$(l+2t)\tau_P + l(E_1 + E_2) + \tau_H$ (verify)
Our approach	$(3m+1)E_0 + 2mE_T + \tau_P$ (encrypt) $(2l+2)E_1 + 2tE_2 + \tau_H$ (sign)	$2m\tau_P + \tau_H + O(mh)$ (decrypt)	$(l+2t)\tau_P + l(E_1 + E_2) + \tau_H$ (verify)

ciphertext. This requires $2m$ pairings to calculate $e(H(u), C_{3,x})$ and $e(sk_{\pi(x),u}, C_{2,x})$ and $O(mh)$ to find the vector c . Decryption takes $2m\tau_P + \tau_H + O(mh)$. Writing is similar to creating a record. The size of ciphertext with signature is $2m|G_0| + m|G_T| + m^2 + |MSG| + (l+t+2)|G_1|$.

When revocation is required, C_0 needs to be recalculated. $e(g, g)$ is previously calculated. So, only one scalar multiplication is needed. If the user revoked is U_u , then for each x , $C_{1,x}$ has to be recomputed. $e(g, g)$ is already computed. Thus, only two scalar multiplication needs to be done, for each x . So a total of $2m' + 1$ scalar multiplications are done by the cloud, where m' is the number of attributes belonging to all revoked users. Users need not compute any scalar multiplication or pairing operations. Additional communication overhead is $O((m' + 1)|G_T|)$.

The curves chosen are either MNT curves (proposed by Miyaji, Nakabayashi, and Takano) or supersingular curves. Considering the requirements, elliptic curve group of size 159, with an embedding degree 6 (type d curves of pairing-based cryptography (PBC) [36]) can be used. Pairing takes 14 ms on Intel Pentium D, 3.0-GHz CPU [16]. Such operations are very suitable for a cloud computing environment. A new library for ABE is also available at [37].

PBC library [36] is a C library which is built above GNU GMP (GNU Math Precision) library and contains functions to implement elliptic curves and pairing operations. Each element of G needs 512 bits at an 80-bit security level and 1,536 bits when 128-bit of security are chosen [39]. Each cryptographic operation was implemented using the PBC library ver. 0.4.18 on a 3.0-GHz processor PC. The public key parameters were selected to provide 80-bit security level. According to [39], implementation uses 160-bit elliptic curve group on the supersingular curve $y^2 = x^3 + x$ over a 512-bit finite field. The computational cost for a pairing operation is 2.9 ms and that of exponentiation on G (and G_0) and G_T (and G_2) are 1 and 0.2 ms, respectively.

We will compare our computation costs with existing schemes like [12], [13], [15] in Section 8.

8 COMPARISON WITH OTHER ACCESS CONTROL SCHEMES IN CLOUD

We compare our scheme with other access control schemes (in Table 3) and show that our scheme supports many

features that the other schemes did not support. 1-W-M-R means that only one user can write while many users can read. M-W-M-R means that many users can write and read. We see that most schemes do not support many writes which is supported by our scheme. Our scheme is robust and decentralized, most of the others are centralized. Our scheme also supports privacy preserving authentication, which is not supported by others. Most of the schemes do not support user revocation, which our scheme does. In Tables 4 and 5, we compare the computation and communication costs incurred by the users and clouds and show that our distributed approach has comparable costs to centralized approaches. The most expensive operations involving pairings and is done by the cloud. If we compare the computation load of user during read we see that our scheme has comparable costs. Our scheme also compares well with the other authenticated scheme of [15].

9 CONCLUSION

We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

ACKNOWLEDGMENTS

This work is partially supported by NSERC Grant CRDPJ386874-09 and the grant: "Digital signal processing, and the synthesis of an information security system," TR32054, Serbian Ministry of Science and Education.

REFERENCES

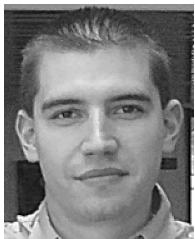
- [1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," *Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing*, pp. 556-563, 2012.
- [2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," *IEEE Trans. Services Computing*, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.
- [3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," *Proc. IEEE INFOCOM*, pp. 441-445, 2010.
- [4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," *Proc. 14th Int'l Conf. Financial Cryptography and Data Security*, pp. 136-149, 2010.
- [5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," *Proc. First Int'l Conf. Cloud Computing (CloudCom)*, pp. 157-166, 2009.
- [6] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., <http://www.crypto.stanford.edu/craig>, 2009.
- [7] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," *Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST)*, pp. 417-429, 2010.
- [8] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, <http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html>, 2013.
- [9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," *Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS)*, pp. 282-292, 2010.
- [10] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," *Proc. 15th Nat'l Computer Security Conf.*, 1992.
- [11] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-Based Access Control," *IEEE Computer*, vol. 43, no. 6, pp. 79-81, June 2010.
- [12] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," *Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm)*, pp. 89-106, 2010.
- [13] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," *Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS)*, pp. 261-270, 2010.
- [14] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," *Proc. 17th ACM Conf. Computer and Comm. Security (CCS)*, pp. 735-737, 2010.
- [15] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," *Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC)*, pp. 83-97, 2011.
- [16] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," *Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2011.
- [17] <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs-01-en.pdf>, 2013.
- [18] <http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud>, 2013.
- [19] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," *Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS)*, 2011.
- [20] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," *Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT)*, pp. 552-565, 2001.
- [21] X. Boyen, "Mesh Signatures," *Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT)*, pp. 210-227, 2007.
- [22] D. Chaum and E.V. Heyst, "Group Signatures," *Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT)*, pp. 257-265, 1991.
- [23] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," *IACR Cryptology ePrint Archive*, 2008.
- [24] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," *Topics in Cryptology - CT-RSA*, vol. 6558, pp. 376-392, 2011.
- [25] A. Beimeil, "Secure Schemes for Secret Sharing and Key Distribution," PhD thesis, Technion, Haifa, 1996.
- [26] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT)*, pp. 457-473, 2005.
- [27] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *Proc. ACM Conf. Computer and Comm. Security*, pp. 89-98, 2006.
- [28] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *Proc. IEEE Symp. Security and Privacy*, pp. 321-334, 2007.
- [29] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," *Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS)*, pp. 343-352, 2009.
- [30] M. Chase, "Multi-Authority Attribute Based Encryption," *Proc. Fourth Conf. Theory of Cryptography (TCC)*, pp. 515-534, 2007.
- [31] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure Threshold Multi-Authority Attribute Based Encryption without a Central Authority," *Proc. Progress in Cryptology Conf. (INDOCRYPT)*, pp. 426-436, 2008.
- [32] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," *Proc. ACM Conf. Computer and Comm. Security*, pp. 121-130, 2009.
- [33] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," *Proc. USENIX Security Symp.*, 2011.

- [34] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," *IACR Cryptology ePrint Archive*, p. 419, 2012.
- [35] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," *Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT)*, pp. 568-588, 2011.
- [36] <http://crypto.stanford.edu/pbc/>, 2013.
- [37] "Libfenc: The Functional Encryption Library," <http://code.google.com/p/libfenc/>, 2013.
- [38] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data," *Proc. ACM Cloud Computing Security Workshop (CCSW)*, 2009.
- [39] J. Hur and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214-1221, July 2011.



Sushmita Ruj received the BE degree in computer science from Bengal Engineering and Science University, Shibpur, India in 2004, and the Masters and PhD degrees in computer science from Indian Statistical Institute, India in 2006 and 2010, respectively. Between 2009 and 2010, she was a Erasmus Mundus Post Doctoral Fellow at Lund University, Sweden and between 2010-2012, she was a Post Doctoral Fellow at University of Ottawa, Canada. She was an

Assistant professor at Indian Institute of Technology, IIT, Indore between 2012-2013 and is currently an Assistant professor at Indian Statistical Institute, Kolkata, India. Her research interests are in security in mobile ad hoc networks, vehicular networks, cloud security, combinatorics and cryptography. She is on the Editorial Board of *Ad Hoc and Sensor Wireless Networks*. Sushmita has served as Program Co-Chair for ICDCS workshop, NFSP'2013, ICC Workshop Secure Networking and Forensic Computing (SNFC) and has served as TPC member for many conferences like Indocrypt, IEEE Globecom, IEEE ICC, IEEE MASS, IEEE PIMRC, ICDCN and many others. She won best paper awards at ISPA 2007 and IEEE PIMRC 2011. She is a member of the IEEE.



Milos Stojmenovic received the bachelor of computer science degree at the School of Information Technology and Engineering, University of Ottawa, ON, Canada, in 2003, the master's degree in computer science at Carleton University in Ottawa, Canada, in 2005, and the PhD degree in the same field at the University of Ottawa, Canada, in 2008. Currently, he is an assistant professor at the Singidunum University, Serbia. He was a visiting researcher at

Japans National Institute of Advanced Industrial Science and Technology in 2009. He published more than 30 articles in the fields of computer vision, image processing, and wireless networks. His work implements machine learning techniques such as AdaBoost and SVM classification which in turn use higher order autocorrelation features to perform image segmentation and classification. He is a member of the IEEE.



Amiya Nayak received the BMath degree in computer science and combinatorics and optimization from the University of Waterloo, ON, Canada, in 1981, and the PhD degree in systems and computer engineering from Carleton University, Ottawa, Canada, in 1991. He has more than 17 years of industrial experience in software engineering, avionics and navigation systems, simulation and system level performance analysis. He is in the Editorial Board of

several journals, including *IEEE Transactions on Parallel and Distributed Systems*, *International Journal of Parallel, Emergent and Distributed Systems*, *International Journal of Computers and Applications*, and *EURASIP Journal of Wireless Communications and Networking*. Currently, he is a full professor at the School of Electrical Engineering and Computer Science at the University of Ottawa. His research interests include the area of fault tolerance, distributed systems/ algorithms, and mobile ad hoc networks with more than 150 publications in refereed journals and conference proceedings. He is a senior member of the IEEE.

► For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.