Enforcing Corporate Governance’s Internal Controls and Audit in the Cloud

Sabrina De Capitani di Vimercati*, Sara Foresti*, Stefano Paraboschi†, Pierangela Samarati*

* Università degli Studi di Milano, Italy – Email: name.surname@unimi.it
† Università degli Studi di Bergamo, Italy – Email: parabosc@unibg.it

Abstract—More and more organizations are today using the cloud for their business as a quite convenient alternative to in-house solutions for storing, processing, and managing data. Cloud-based solutions are then permeating almost all aspects of business organizations, resulting appealing also for functions that, already in-house, may result sensitive or security critical, and whose enforcement in the cloud requires then particular care. In this paper, we provide an approach for securely relying on cloud-based services for the enforcement of Internal Controls and Audit (ICA) functions for corporate governance. Our approach is based on the use of selective encryption and of tags to provide a level of self-protection to data and for enabling only authorized parties to access data and perform operations on them, providing privacy and integrity guarantees, as well as accountability and non-repudiation.

Keywords—Cloud-based services; outsourcing; internal controls and audit process; selective encryption

I. INTRODUCTION

Corporate Governance is a collection of rules, best practices, and processes needed to achieve an organization’s objectives and strategies. The benefits and the importance of having a good corporate governance are continuously increasing, due to the growth in business regulation and capital mobility. Indeed, countries see corporate governance as a key factor for their global competitiveness. There are therefore several attempts to promote the adoption of national Corporate Governance Codes by organizations. As an example, the European Corporate Governance Codes Networks (www.ecgcn.org) has the goal to share experience on issues related to corporate governance. These national Corporate Governance Codes contain many principles focusing on different aspects, such as the model of corporate governance, and relations with shareholders; an important role is played by the internal control and risk management system, which has, as central mechanisms, the internal controls and audit (ICA) functions.

ICA functions aim mainly at verifying the effectiveness and efficiency of operations and their successful realization can contribute to the improvement of the quality of corporate governance and management. ICA functions can be performed in different ways, depending on how the general principles described in the Corporate Governance Code are implemented in the context of a specific organization. This paper focuses on the case of an organization structured in multiple units and where all the operations performed in the units must be checked according to a three-level ICA process. A structure with three levels is the most common in companies that have to comply with market regulations, like banks and financial institutions. The first level of control is executed by an employee of the unit where the operation has been performed. The second level of control is performed by the director of the unit, and the third level of control is performed by an independent auditor. Each level of control aims at verifying different aspects related to, for example, the operational and business area, and produces a report summarizing the results of the control.

The adoption of cloud-based solutions for supporting ICA functions requires to ensure confidentiality and integrity of data and of controls on them, involving different challenges. First, data records subject to internal controls and audit may need to remain confidential to the cloud provider itself. Second, access to data and execution of internal controls and audit should be possible only for authorized parties. Third, parties should be accountable for their actions. Fourth, parties involved in the control should be able to assess integrity of information (data and results of control) on which they operate. Although several proposals have been designed for the protection of data in the cloud (e.g., [1]), none of them can be directly applied to correctly enforce the ICA of corporate governance.

In this paper, we consider the problem of securely relying on the cloud for supporting ICA functions and address all the challenges above. The remainder of this paper is organized as follows. Section II presents the scenario, introducing the parties involved in the ICA functions and their execution. Section III illustrates our solution for providing protection to data in the cloud and enforcing access control on them so that only authorized parties can access them. Section IV enriches such solution with capability of secure support of all ICA functions ensuring their execution only to authorized parties, with confidentiality and integrity guarantees. Section V provides the algorithm implementing the proposed solutions. Section VI discusses related work. Finally, Section VII concludes the paper.

II. SCENARIO AND PROBLEM DEFINITION

We consider an organization composed of different operating units whose employees can process and manage different operations. Each unit is under the control of a unit director, who is responsible for the activity of the unit. For simplicity of exposition, but without loss of generality, we assume that
Each director is responsible for one unit only. Formally, we
denote the set of units of the organization as $U$, and, for each
unit $u_i \in U$, we denote its employees as $E_i$ and its director as $d_i$. Each unit $u_i$ stores the information of operations in a
log, modeled as a set $O_i$ of operation records. Each record
stores the information of the corresponding operation, which
includes a unique operation identifier $i.d$ and the identifier of
the unit $u$ where the operation has been processed. We
use the traditional dot notation to refer to a specific attrib-
ute of an operation record (e.g., $o.r.e$ denotes the identifier of
an operation $o$). For simplicity, in the following, we will use
the term operation to refer interchangeably to the operation
and its record. Notation $D$, $E$, and $O$ is used to refer to
the set of directors, employees, and operations of all units,
respectively (i.e., $D = \{d_1, \ldots, d_n\}$, $E = E_1 \cup \ldots \cup E_n$, and $O = O_1 \cup \ldots \cup O_n$). Note that the directors of units are disjoint from the set of employees, that is, $D \cap E = \emptyset$.

Example 2.1: We consider, as a running example, an
organization with two units $U = \{X, Y\}$, where unit $X$ has
three employees $E_x = \{x_1, x_2, x_3\}$ and is directed by $d_x$, and
unit $Y$ has two employees $E_y = \{y_1, y_2\}$ and is directed by
$d_y$. The set of operations processed by units $X$ and $Y$ are $O_x$ and $O_y$, respectively.

The management of operations and of the corresponding
internal controls and audit operate in compliance with a
regulation established by the organization, according to
which:  
1) information related to an operation is accessible to
all employees and the director of the unit where the
operation has been processed; and ii) information related to
all operations of all the units is accessible to all independent
auditors. These two requirements naturally translate into an
access control policy regulating which subject (employee,
director, auditor) should be authorized to access the opera-
tions. Given the set $S = E \cup D \cup A$ of subjects in the system,
the access control policy of the organization can be formally
defined as follows.

Definition 2.1 (Access control policy): Let $S = E \cup D \cup A$
be the set of subjects, $U$ be the set of units, and $O$ be the
set of operations. An access control policy $P$ regulating
access to operations in $O$ is a set of permissions of the
form $(s, o)$, with $s \in S$, $o \in O$, such that only the following
permissions are included:

1) $\forall s \in E \cup D, \forall o \in O : (s, o) \in P$ if $o \in unit(s)$;
2) $\forall a \in A, \forall o \in O : (a, o) \in P$.

Each pair $(s, o)$ in $P$ states that $s$ can access $o$.

Due to the huge number of operations that are processed
on a daily basis, the operation records as well as the
Corresponding reports generated during the internal controls
and audit process are stored and managed in the cloud (see
Figure 1). Our goal is therefore the design of a solution that
supports the external storage of the operation records while
guaranteeing the confidentiality and integrity of their content
as well as the integrity and non repudiation of ICA reports.
Indeed, the cloud provider, which is not under the direct
control of the organization, is assumed to be honest-but-
curious meaning that it is trustworthy to properly manage the
ICA process but it may not be trusted to read the operations
content and reports. Figure 2 summarizes the notation used
in the paper. In the following, we first describe how to
enforce the access control policy of the organization using selective encryption (Section III) and then shows how to enforce the ICA process (Section IV and Section V).

III. STORAGE AND ACCESS CONTROL

Before moving the storage of the operations to the cloud, the record of each operation is encrypted to guarantee its confidentiality with respect to the cloud provider. Our solution enforces the access control policy of the organization over the encrypted operations externally stored leveraging the selective encryption technique (e.g., [2]). Basically, we encrypt different operations with different encryption keys and ensure that each subject can decrypt all and only the operations she is authorized to access. To do so without requiring the distribution of multiple keys to subjects, we organize keys in a hierarchical structure enabling a subject to derive from a single key (the one assigned to the subject) all, and only, the keys used for encrypting the operations that the subject is authorized to access (e.g., [3]). Each subject $s$ with key $k_s$, can then derive another key $k'$ through a public token computed as $t=k\oplus h(k_s,l)$, where $h$ is a deterministic cryptographic function, $\oplus$ is the bitwise xor operator, and $l$ is a publicly available label associated with key $k$. The derivation process can be direct or indirect, through a chain of tokens (i.e., key $k$ can in turn be used to derive another key $k'$). Intuitively, key derivation permits to assign a single key to each subject (employee, director, auditor), from which she can derive the encryption keys used to protect the operations that she is authorized to access. The access control policy $\mathcal{P}$ can then be translated into an equivalent encryption policy dictating the key used to encrypt each operation, the key released to each subject, and key derivation via tokens. Basically, each employee, director, and auditor has her own key. Also, since all operations processed at a specific unit can be accessed by the same set of subjects (i.e., the employees and the director of the unit as well as all auditors), they can be all encrypted with the same key. We can therefore associate a key with each unit and use it for encrypting all the operations processed at the unit. The employees and director of each unit must then be able to derive, from their own key, the key of the unit where they work. The auditors must instead be able to derive, from their own key, the keys of all the units. Formally, an encryption policy equivalent to the access control policy $\mathcal{P}$ of the organization is defined as follows.

**Definition 3.1 (Equivalent encryption policy):** Let $\mathcal{P}$ be the access control policy over the set $U$ of units and the set $S=\mathcal{E}\cup D\cup A$ of subjects, and $O$ be the set of operations. An encryption policy $\Pi$ equivalent to $\mathcal{P}$ is a 7-tuple $(S,O,K,\mathcal{L},\phi_\mathcal{S},\phi_\mathcal{O},T)$ where:

1) $(K,\mathcal{L})$ is the set of keys and corresponding labels such that $K=K_S\cup K_U$, with $K_S=\{k_s|s\in S\}$ and $K_U=\{k_u|u\in U\}$;
2) $\phi_\mathcal{S}:S\rightarrow K_S$ is an injective function assigning a key and corresponding label to each subject;
3) $\phi_\mathcal{O}:O\rightarrow K_U$ is a function assigning a key and corresponding label to each operation such that $\forall o',o''\in O$ with $o'=o''\cup u$, $\phi_\mathcal{O}(o')=\phi_\mathcal{O}(o'')$;
4) $T$ is the set of tokens defined over $K$ and $\mathcal{L}$ such that: $\forall (s,o)\in \mathcal{P}$, $\phi_\mathcal{S}(s)\xrightarrow{\mathcal{T}} \phi_\mathcal{O}(o)$; $\forall k_u\in K_U$, $\forall o\in \phi_\mathcal{O}^{-1}(k_u)$, $(\phi_\mathcal{S}^{-1}(k_u),o)\in \mathcal{P}$.

Notation $k'\xrightarrow{\mathcal{T}} k''$ indicates that key $k''$ is derivable from key $k'$ through a (sequence of) token(s) in $T$. The above definition of equivalent encryption policy says that: there is a key for each subject and each unit, and all operations of the same unit $u$ are encrypted with the same key $k_u$ (1-3), and each subject $s$ is associated with a key $\phi_\mathcal{S}(s)$ from which she can derive all and only the keys of the operations that $s$ is authorized to access according to policy $\mathcal{P}$ (4). Note that the definition does not say anything about how to create the tokens to guarantee policy equivalence. We can therefore adopt different strategies. Our solution consists in creating, for each unit $u\in U$, a token enabling the direct derivation of $k_u$ from the key of each employee and director of $u$ and from the key of each auditor. Each operation $o\in O$ is then encrypted with key $k_u$, thus ensuring the correct enforcement of conditions 3 and 4 of Definition 3.1.

**Example 3.1:** Figure 3 graphically illustrates the key derivation structure of our running example, obtained ac-
In this section, we present our solution for the enforcement of these requirements when the operation records are encrypted and stored at an external cloud provider where no trusted monitor can directly enforce them.

A. Report generation

When moving the storage of operation records to the cloud, the enforcement of requirement R1 is complicated by the absence of a trusted party to whom controls can be delegated. Indeed, the cloud provider is not trusted for authentication and policy enforcement. The idea is then to design a solution that, in cooperation with the cloud provider, exploits selective encryption for the enforcement of requirement R1. Intuitively, our solution consists in associating a secret, encrypted using selective encryption, with each report to regulate (write) access to it. The secret is a value generated together with the operation and encrypted with a key known only to the subjects authorized to generate the report and to the cloud provider. The encrypted secret is called tag and the cloud provider will accept a write/create operation on a report related to a given operation when the requesting subject shows ability to decrypt the corresponding tag. Formally, a tag is defined as follows.

Definition 4.1 (Tag): A tag is the result of the encryption $\text{Enc}(\sigma, k_{SP})$ of a secret $\sigma$ with a key $k_{SP}$ known to the subjects in $S \subseteq \mathcal{E} \cup D \cup A$ and to the cloud provider $P$.

The secret $\sigma$ used to compute a tag can be a randomly generated number. The proper enforcement of requirement R1 requires each operation to be associated with three different tags, one for each report, that must be encrypted with different keys shared by the cloud provider and the subjects authorized to generate the report. Formally, each operation $o$ of unit $u_i$ is associated with three tags computed as follows.

- $\text{tag}_e = \text{Enc}(\sigma, k_{E,P})$, with $k_{E,P}$ a key known only to the employees $E_i$ of unit $u_i$ and to the cloud provider $P$, and $\sigma$ the secret needed to create/write report $re$ (R1.1).
- $\text{tag}_d = \text{Enc}(\sigma', k_{d,P})$, with $k_{d,P}$ a key known only to the director $d_i$ of unit $u_i$ and to the cloud provider $P$, and $\sigma'$ the secret needed to create/write report $rd$ (R1.2).
- $\text{tag}_a = \text{Enc}(\sigma'', k_{A,P})$, with $k_{A,P}$ a key known to the auditors $A$ and to the cloud provider $P$, and $\sigma''$ the secret needed to create/write report $ra$ (R1.3).

Figure 4 shows the structure of the outsourced records. As an example, operation $o_x$ processed at unit $X$ is associated with tags $\text{tag}_e = \text{Enc}(\sigma, k_{E,P})$, $\text{tag}_d = \text{Enc}(\sigma', k_{d,P})$, and $\text{tag}_a = \text{Enc}(\sigma'', k_{A,P})$ enabling the employees of unit $X$, its director $d_x$, and all auditors to create/write report $re$, $rd$, and $ra$, respectively. Indeed, the cloud provider will permit to write report $re$ (and $ra$, resp.) only to subjects demonstrating their ability to correctly decrypt $\text{tag}_e$ ($\text{tag}_d$ and $\text{tag}_a$, resp.). Operatively, a subject (i.e., an employee $e$, director $d$, and auditor $a$, resp.) before performing a check on an operation has to first download the appropriate tag from the cloud provider (i.e., $\text{tag}_e$, $\text{tag}_d$, or $\text{tag}_a$, resp.), decrypt it, and send the retrieved secret to the cloud provider. The cloud provider allows the subject to write the report only if the communicated secret corresponds to the secret that the provider retrieves decrypting the same tag (i.e., $\text{tag}_e$, $\text{tag}_d$, and $\text{tag}_a$, resp.).

The key derivation structure illustrated in Section III is then extended with the keys necessary for the management of tags. In particular, the structure is extended by adding a node for the key $k_P$ of the cloud provider and a node for each key $k_{SP}$ shared by a subset $S \subseteq S$ of subjects and the
cloud provider. The cloud provider, as well as the authorized subjects, can derive these keys through a direct token from their own key. For instance, each employee \( e \in E_i \) working at unit \( u_i \) can derive key \( k_{E.P} \) through a token from key \( k_e \) to key \( k_{E.P} \).

Example 4.1: Consider our running example and the key derivation structure in Figure 3. Figure 5 illustrates the extended key derivation structure, where nodes with a dotted circle represent keys shared with the cloud provider, and dotted edges represent the tokens added to the original key derivation structure for allowing authorized subjects and the cloud provider to derive the keys necessary to decrypt tags.

B. Report update

Requirement R2 regulates who can update a report and until when. As an example, consider our running example and suppose that employee \( x_1 \) checks operation \( o_x \) and then generates report \( o_x.r.e \). According to R2, only \( x_1 \) can modify \( o_x.r.e \) until director \( d_2 \) begins the second level of control. As discussed in Section IV-A, tags represent an effective solution for regulating, in cooperation with the cloud provider, who can write reports. We then leverage tags to enforce also requirement R2 as described in the following.

Restrict updates (R2.1). Since a report can be generated/modified only by the subjects who can prove the knowledge of the corresponding secret (\( \sigma \)) in the tag (i.e., the subjects who can correctly decrypt the tag), updates to the report can be prevented by changing the secret and therefore the tag. In this way, only presenting the new secret a subject can modify the corresponding report. Note that the secret must be changed and encrypted with a key that only the subjects authorized to modify the report (and the cloud provider) know, to avoid that previously authorized subjects can present the old secret and obtain the access. We apply this idea to restrict updates to the employee and auditor reports (the director report can already be updated only by the director). Whenever an authorized subject \( s \in E \cup A \) (i.e., an employee or auditor) starts the analysis of an operation \( o \), the subject has to: 1) generate a new secret \( \sigma' \); 2) create a new tag obtained encrypting the new secret with key \( k_{E.P} \) shared with the cloud provider (\( \text{Enc}(\sigma', k_{E.P}) \)); 3) overwrite the old tag (i.e., \( o_{\text{tag}_e} \) or \( o_{\text{tag}_a} \), depending on whether \( s \) is an employee or an auditor) with the new one. Since the new secret \( \sigma' \) is encrypted with key \( k_{E.P} \), only subject \( s \) can prove to the cloud provider the knowledge of \( \sigma' \), thus blocking the possible attempts by previously authorized subjects (i.e., the employees of the same unit as \( s \) and all the auditors) to modify the report. The new keys needed to encrypt the new secrets (i.e., \( \forall s \in E \cup A \), key \( k_{E.P} \)) are derivable by the authorized subjects (i.e., each subject \( s \in E \cup A \)) and by the cloud provider through tokens added to the key derivation structure and that start from the key of the authorized subjects and from the key of the provider.

Prevent updates (R2.2). A subject who has generated a report can modify it until the subsequent control phase, that is, when a director or auditor starts a control, the subject who has created the report in the previous phase (i.e., an employee or director, resp.) should not be able to update it anymore. To prevent such updates, it is sufficient to substitute the tag of the previous phase with a dummy content that cannot be decrypted. In this way, since the tag cannot be decrypted, the provider as well as any subject cannot retrieve the secret and then nobody is authorized to update the report. Note that also when an auditor terminates her control, the corresponding tag \( \text{tag}_a \) is overwritten with a dummy content. Furthermore, the auditor sets attribute \( fl \) to \( \text{TRUE} \). When attribute \( fl \) is \( \text{TRUE} \) the ICA process on the corresponding operation is considered concluded and the cloud provider does not accept any write operation on any reports.

Example 4.2: Consider operation \( o_x \) of unit \( X \) of our running example. Figure 6 illustrates the evolution of \( \text{tag}_e \), \( \text{tag}_d \), and \( \text{tag}_a \) to satisfy requirement R2, assuming that \( x_1 \), \( d_2 \), and \( a_1 \) perform the first, second, and third level of control, respectively. In the figure, updates to tags are in black, while unchanged tags are in gray. Note that, while any employee in \( E_e \) can start the first level of control, since they can all retrieve \( \sigma_1 \) from \( \text{tag}_e \), when \( x_1 \) starts the first level of control, \( x_2 \) and \( x_3 \) cannot modify \( re \) since they cannot decrypt \( \text{tag}_e \) (they do not know \( k_{E.P} \)) and \( \sigma_1 \) is no more accepted by the provider. Similarly, when \( \text{tag}_e \) is set to dummy by the director, also \( x_1 \) cannot modify \( re \).

Figure 7 illustrates the key derivation structure in Figure 5, extended with the keys necessary to manage tags for the enforcement of requirement R2.
C. Report integrity and accountability

Requirement R3 has the objective to verify that all subjects involved in the ICA process as well as the cloud provider behave properly. In particular, it aims at ensuring that modifications to reports have been produced only by authorized subjects. If all subjects behave as discussed in the previous sections and the cloud provider performs the correct control on tags, the integrity of operations and reports is automatically guaranteed. However, since unauthorized updates to reports cannot be prevented, we adopt a signature-based approach that allows the detection of possible tampering of operations and reports. Each subject has a pair \langle ks, kp \rangle of secret and public keys and uses her secret key to sign the reports she generates. This guarantees that any tampering to an operation or to its reports can be immediately detected by any subject knowing the public key kp of the subject who generated the report. Also, by signing a report, the subject who generated the report cannot repudiate it. Concretely, given a hash function h, each operation record is associated with the following three signatures, one for each subject involved in the three controls of the ICA process.

- se = Sign(h(o.* || re), ks_e), with o.* the set of all attributes in o and e the employee who generated report re.
- sd = Sign(h(se || rd), ks_d), with d the director who generated report rd.
- sa = Sign(h(sd || ra), ks_a), with a the auditor who generated report ra.

Figure 8(a) illustrates the structure of the portion of the outsourced records that includes the three signatures. Each signature guarantees the integrity of the corresponding report and makes the subject who produced the report accountable for its content. Since the public keys used to generate se, sd, and sa are publicly available, all subjects in the system and the cloud provider can verify the signatures and detect tampering of reports and operations. Note that the signature produced at the end of a phase of the ICA process is applied on the digest of the concatenation of the report produced in that phase and the signature computed at the end of the previous phase (with the operation content, for the employee report). By signing the signature computed in the previous phase, the subject implicitly confirms that she has verified such signature before starting her control. Figure 8(b) shows the layered organization of the signatures. Note that this layered structure, which starts with the signature of an employee computed over the operation content together with the employee report, ensures the correct association of each operation with its reports. For instance, if a malicious subject copies the content of o, re into o_j, re, signature o_j, se would signal the inconsistency of the report content.

Example 4.3: With respect to Example 4.2, when employee x_1 has generated report re, she signs o_e with her secret key ks_e. Director d_e can then verify se with key kp_e, generate report rd_e, and sign the concatenation of se and rd_e with her secret key ks_{d_e}. Similarly, auditor a_1 can verify sd_e with kp_{d_e}. When the auditor generates report ra_e, she signs the concatenation of sd_e and ra_e with her secret key ks_{a_1}.

V. Operation generation and control

We describe the functions (Figure 9) implementing the solutions described in the previous sections for the storage of operations and the enforcement of the ICA process.

Generation. Each operation is generated by an employee working at a unit u_i \in U. The operation record is encrypted with the key k_{u_i} of the unit (line 1). The encrypted record is also associated with a unique identifier (line 2) and with the tags regulating the generation of reports (lines 3–6). While tag tag_e can be generated by any employee of the unit, tag_d and tag_a can be generated only by the director of the unit and by auditors, respectively. To avoid requesting continuous online presence of directors and auditors, we assume that the director of the unit and auditors generate a pool of tags in advance (sets DirTags_{u_i} and AuditTags, resp.). When an operation is generated, it is associated with tags extracted from these sets. Reports and signatures for
Operation Management

Generate_Encrypted_Operation(\(o\)) @ \(u_i\)

1. \(o^k_.\text{enc} := \text{Enc}(\sigma_i, k_{u_i})\)
2. \(o^k_.\text{id} := \) generate an identifier
3. randomly generate \(\sigma_1\)
4. \(o^k_.\text{tag}_e := \text{Enc}(\sigma_1, k_{e, p})\)
5. \(o^k_.\text{tag}_a := \text{ExtractTag(DirTags)}\)* tags for director of \(u_i\)
6. \(o^k_.\text{tag}_a := \text{ExtractTag(AuditTags)}\)* tags for auditors
7. \(o^k_.\text{re} := o^k_.\text{rd} := o^k_.\text{ra} := \text{NULL}\)
8. \(o^k_.\text{se} := o^k_.\text{sd} := o^k_.\text{sa} := \text{NULL}\)
9. \(o^k_.\text{f1} := \text{FALSE}\)
10. upload \(o^k\) on the cloud provider

First_Level_Control(id) @ e \(\in E_i\)

1. \(o^k := \) download \(o\) with identifier \(\text{id}\) from the provider
2. \(\sigma_1 := \text{Dec}(o^k_.\text{tag}_a, k_{e, p})\)
3. if Verify(id, 1, \(\sigma_1, E_i\)) \(\text{TRUE}\) then
4. randomly generate \(\sigma_k\)
5. \(o^k_.\text{tag}_e := \text{Enc}(\sigma_k, k_{e, p})\)
6. upload \(o^k\) on the cloud provider
7. \(o := \text{Dec}(o^k_.\text{enc}, k_{u_i})\)
8. report := generate the report for \(o\)
9. \(o^k_.\text{re} := \text{Enc}(\text{report}, k_{u_i})\)
10. \(o^k_.\text{se} := \text{Sign}(h(o^k_.\text{f1})), k_{s_e}\)
11. upload \(o^k\) on the cloud provider

Second_Level_Control(id) @ \(d_i\)

1. \(o^k := \) download \(o\) with identifier \(\text{id}\) from the provider
2. \(\sigma_2 := \text{Dec}(o^k_.\text{tag}_a, k_{d_i, p})\)
3. if Verify(id, 2, \(\sigma_2, d_i\)) \(\text{TRUE}\) then
4. \(o^k_.\text{tag}_e := \text{dummy}\)
5. upload \(o^k\) on the cloud provider
6. \(o := \text{Dec}(o^k_.\text{enc}, k_{u_i})\)
7. \(o^k_.\text{re} := \text{Dec}(o^k_.\text{re}, k_{u_i})\)
8. if Verify_Signature(o^k_.\text{se}, h(o^k_.\text{f1})), report)) then
9. report := generate the report for \(o\)
10. else report := not passed
11. \(o^k_.\text{rd} := \text{Enc}(\text{report}, k_{u_i})\)
12. \(o^k_.\text{sd} := \text{Sign}(h(o^k_.\text{f1})), k_{s_d}\)
13. upload \(o^k\) on the cloud provider

Third_Level_Control(id) @ \(a\)

1. \(o^k := \) download \(o\) with identifier \(\text{id}\) from the provider
2. \(\sigma_3 := \text{Dec}(o^k_.\text{tag}_a, k_{a, p})\)
3. if Verify(id, 3, \(\sigma_3, A\)) \(\text{TRUE}\) then
4. randomly generate \(\sigma_k\)
5. \(o^k_.\text{tag}_e := \text{Enc}(\sigma_k, k_{e, p})\)
6. \(o^k_.\text{tag}_a := \text{dummy}\)
7. upload \(o^k\) on the cloud provider
8. \(o := \text{Dec}(o^k_.\text{enc}, k_{u_i})\)
9. \(o^k_.\text{re} := \text{Dec}(o^k_.\text{re}, k_{u_i})\)
10. \(o^k_.\text{rd} := \text{Dec}(o^k_.\text{rd}, k_{u_i})\)
11. if Verify_Signature(o^k_.\text{sd}, h(o^k_.\text{f1})), report), k_{p_d}) then
12. report := generate the report for \(o\)
13. else report := not passed
14. \(o^k_.\text{ra} := \text{Enc}(\text{report}, k_{u_i})\)
15. \(o^k_.\text{sa} := \text{Sign}(h(o^k_.\text{f1})), k_{s_a}\)
16. \(o^k_.\text{tag}_a := \text{dummy}\)
17. \(o^k_.\text{f1} := \text{TRUE}\)
18. upload \(o^k\) on the cloud provider

Verify(id, phase, \(\sigma\), \(X\)) @ \(P\)

1. let \(o^k\) be the operation with \(o^k_.\text{id}=\text{id}\)
2. case phase of
3. 1: \(\text{proof} := \text{Dec}(o^k_.\text{tag}_e, k_{e, p})\)
4. 2: \(\text{proof} := \text{Dec}(o^k_.\text{tag}_a, k_{a, p})\)
5. 3: \(\text{proof} := \text{Dec}(o^k_.\text{tag}_a, k_{a, p})\)
6. if \(\text{proof} = \text{TRUE}\) then return(\(\text{TRUE}\))
7. return(\(\text{FALSE}\))

Figure 9. Pseudocode of operation generation and ICA process

The generated operation are set to NULL, while \(f1\) is set to FALSE (lines 7–9). When all information about the operation has been set, the record is uploaded on the cloud provider (line 10).

First level control. When employee \(e\) performs the first control on operation \(o\), she first needs to prove to the cloud provider her ability to decrypt \(\text{tag}_e\) (lines 1–3). The employee then overwrites \(\text{tag}_e\) with a tag that other employees cannot decrypt (lines 4–6). Note that the update to \(\text{tag}_e\) is immediately uploaded on the server. The employee then decrypts the operation record, performs the control, and generates the corresponding report (lines 7–8). She encrypts the report using the key of the unit \(k_u\) and computes signature \(\text{se}\) (lines 9–10). Finally, the operation record is uploaded on the cloud provider (line 11).

Second level control. When the unit director \(d_i\) needs to control operation \(o\), she first decrypts \(\text{tag}_d\) to demonstrate to the cloud provider that she is entitled to generate the report (lines 1–3). The director then nullifies \(\text{tag}_e\) (lines 4–5). She decrypts the operation record and report \(\text{re}\), verifies signature \(\text{se}\), and performs the control (lines 6–10). The director encrypts her report with the key of the unit \(k_u\) and computes signature \(\text{sd}\) (lines 11–12). Finally, the operation record is uploaded on the cloud provider (line 13).

Third level control. When auditor \(a\) controls operation \(o\), she first decrypts \(\text{tag}_a\) to demonstrate that she is authorized to perform the control (lines 1–3). The auditor then overwrites \(\text{tag}_a\) with a tag that other auditors cannot decrypt, and nullifies \(\text{tag}_d\) (lines 4–7). She decryots the operation record and the reports of the first two controls, \(\text{re}\) and \(\text{rd}\), and verifies signature \(\text{sd}\) (lines 8–11). The auditor generates her report, encrypts it with \(k_u\), and computes \(\text{sa}\) (lines 12–15). The auditor finally nullifies \(\text{tag}_a\), sets \(f1\) to TRUE (lines 16–17), and the operation record is uploaded on the cloud provider (line 18).

Note that when one of the controls of an operation fails, the record associated with the operation is not deleted. The unit is alerted and further controls are put in place at the organization level, generating a new report for the operation.

Example 5.1: Figure 10 illustrates the evolution of the record of operation \(o_x\) of our running example. The table has a column for each generation report control and signature attribute, and a row for each ICA phase. We assume that \(o_x\) is verified by employee \(x_1\), director \(d_x\), and auditor \(a_j\).

VI. Related work

The problem of moving data storage and management to the cloud has been widely studied. Since cloud providers are not necessarily trusted, data confidentiality, integrity, and availability are possibly at risk when outsourcing data [1]. Several efforts have been then devoted to the definition of approaches enabling the effective and efficient evaluation of computations and queries directly over encrypted data
and providing integrity of their results (e.g., [7], [8], [9]). For enforcing access control, researchers have investigated approaches that rely on attribute-based encryption based on public keys (e.g., [10], [11], [12], [13], [14]) and selective encryption based on hierarchically organized symmetric keys (e.g., [2], [15], [16]). Attribute-Based Encryption (ABE) regulates access to resources according to access control policies that are defined on attributes associated with every user’s secret key and on an access structure associated with every resource (or vice versa). A user can access a resource when her attributes match the access structure associated with the resource (or vice versa). Selective encryption techniques translate the authorization policy regulating access to resources into an equivalent encryption policy. Each resource is then encrypted with a different key that only authorized users can derive from their own secret key. The management of policy updates is complicated when using both ABE and selective encryption and solutions for both techniques have been proposed (e.g., [17], [18]).

Most of the current solutions for access control enforcement in cloud scenarios mainly focus on the restriction of read operations over sensitive data. A few works have addressed the problem of enforcing restrictions on write operations, which are usually assumed to be an exclusive privilege of the data owner. Similarly to read restrictions, also the proposals aimed at enforcing write restrictions rely on ABE (e.g., [19]) or on selective encryption and key derivation (e.g., [20]). The first class of techniques are based on the combination of ABE with Attribute-Based Signature (ABS), while the second class of techniques rely on digital signatures and/or on HMAC functions.

VII. CONCLUSIONS

We have presented an approach enabling organizations to securely rely on cloud-based solutions for supporting corporate governance’s internal controls and audit functions. By leveraging selective encryption and tags, our approach guarantees confidentiality and integrity of data subjects to audit as well as on controls on them, without requiring trust in the cloud provider. Only authorized parties will be able to access data and perform control functions, also being accountable for them. All parties involved in the ICA process, as well as the organization, will be able to assess integrity of the data and function execution, hence detecting possible misbehavior of the provider itself. Our work leaves space for extensions such as the management of conflict of interests in the enforcement of controls and the support for delegation.

ACKNOWLEDGMENTS

The authors would like to thank Luca Saccagi for discussions on the problem. This work was supported in part by the EC under grant agreement 825333 (MOSAICrOWN) and the Italian MIUR under PRIN project HOPE.

REFERENCES


