Chapter 10
Policy Management in Cloud: Challenges and Approaches

Hassan Takabi
University of Pittsburgh, USA

James B. D. Joshi
University of Pittsburgh, USA

ABSTRACT

Cloud computing paradigm is still an evolving paradigm but has recently gained tremendous momentum due to its potential for significant cost reduction and increased operating efficiencies in computing. However, its unique aspects exacerbate security and privacy challenges that pose as the key roadblock to its fast adoption. Cloud computing has already become very popular, and practitioners need to provide security mechanisms to ensure its secure adoption. In this chapter, the authors discuss access control systems and policy management in cloud computing environments. The cloud computing environments may not allow use of a single access control system, single policy language, or single management tool for the various cloud services that it offers. Currently, users must use diverse access control solutions available for each cloud service provider to secure data. Access control policies may be composed in incompatible ways because of diverse policy languages that are maintained separately at every cloud provider. Heterogeneity and distribution of these policies pose problems in managing access policy rules for a cloud environment. In this chapter, the authors discuss challenges of policy management and introduce a cloud based policy management framework that is designed to give users a unified control point for managing access policies to control access to their resources no matter where they are stored.

INTRODUCTION

Cloud computing has recently generated intensive interest within computing research communities. It essentially tries to consolidate the economic utility model with the evolutionary development of many existing computing approaches and technologies such as distributed services, applications, information and infrastructure consisting of pools of computers, networks, information and storage resources (Cloud Security Alliance, 2011), Catteddu & Hogben, 2009). Cloud computing has shown tremendous potential to enhance collaboration, agility, scale, and availability (Takabi,
Policy Management in Cloud

Joshi, & Ahn, 2010). Its definitions, attributes, characteristics, issues, underlying technologies, risks, and values have been evolving and change over time. Confusion still exists about how a cloud is different from existing models and how these differences might affect its adoption. Some see a cloud as a novel technical revolution while others consider it a natural evolution of technology, economy and culture (Takabi, Joshi, & Ahn, 2010).

So far, no single, agreed upon definition of cloud computing exists. The US National Institute of Standards and Technology (NIST) defines cloud as follows: “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.” (Mell & Grance, 2011). The five key characteristics of cloud computing include on demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service, all of which are geared toward using clouds seamlessly and transparently (Mell & Grance, 2011). The three key cloud delivery models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) (Mell & Grance, 2011).

In IaaS, the cloud provider provides a set of virtualized infrastructural components such as virtual machines and storage on which the customers can build and run applications. The most basic component is a virtual machine (VM) and the virtual operating system (OS) where the application will eventually reside. Issues such as trusting the virtual machine image, hardening hosts, and securing inter-host communication are critical areas in IaaS. PaaS enables the programming environments to access and utilize the additional application building blocks. Such programming environments have a visible impact on the application architecture. One such impact would be that of the constraints on what services the application can request from an OS. For example, a PaaS environment may limit access to well-defined parts of the file system, thus requiring a fine-grained authorization service. In SaaS, the cloud providers enable and provide application software enabled as on-demand-services. As clients acquire and use software components from different providers, securely composing them and ensuring that information handled by these composed services are well protected become crucial issues.

Various cloud deployment models include public cloud, private cloud, community cloud, and hybrid cloud composed of multiple clouds (Mell & Grance, 2011). A public cloud refers to an external or publicly available cloud environment that is accessible to multiple tenants, while a private cloud is typically a tailored environment for a particular organization. Similarly, community cloud is tailored for a particular group of customers.

As more and more consumers start using cloud services, Service Level Agreement (SLA) is becoming a key aspect of immigrating to the cloud. The SLA is used to describe the relationship between cloud providers and consumers and is fundamental of consumers’ trust in cloud service providers. An SLA should clearly address several factors like a list of services the provider delivers along with a specific definition of these services, the responsibilities of both parties, a set of metrics to ensure the provider is delivering the services as stated, an auditing mechanism to monitor the quality of services, business continuity and disaster recovery plan, location of data, seizure of data, how to address failures of the provider and disputes between the provider and consumer, the available options when the terms of the SLA are not met, system redundancy and maintenance, jurisdiction, and how the SLA term can be modi-
Policy Management in Cloud

fied over time. Some of the other requirements that need to be taken into account in SLAs are security, privacy, data encryption, transparency, data retention and deletion, hardware erasure and destruction, monitoring, auditing, metrics used for monitoring and auditing, regulatory compliance, and machine-readable SLAs.

The complex and dynamic nature of the cloud requires a sophisticated approach to managing SLAs. A continuous monitoring of quality of service (QoS) attributes and measuring the performance of the service is necessary. The service level management gathers the performance information and ensures that terms of the SLA are being met. The current market offers two types of SLAs: Off-the-shelf non-negotiable SLAs and negotiated SLAs for consumer’s specific requirements. A non-negotiable SLA is far less expensive than a negotiated one but is not acceptable for consumers with mission-critical data and applications. However, most public cloud service providers do not offer negotiated SLAs and if the consumers’ needs aren’t met, they can either receive a credit towards next month’s bill or stop using the service.

Moreover, cloud computing increases legal risks and issues like liability, data protection, compliance, data portability, and copyright should be addressed when moving data to the cloud. There has been a lot of debate on the legal landscape of the cloud but many issues are not yet resolved. For example, it is not clear who has control over the data in cloud, what happens to the data when it’s transferred across various jurisdictions, and which laws are applicable to the cloud.

In EU, the Data Protection Directive 95/46 is most relevant regulation to the cloud computing. It can be applied to cloud service providers where they process personal data within the EU jurisdiction. Although the principles of this legal framework can be applied in the cloud computing environment, in practice, things are more complicated and there are a lot of challenges when trying to apply these principles. This is because the data protections laws are outdated and are not able to deal with the legal problems raised by cloud computing environment. In USA, some of the existing regulations are applicable to cloud and perhaps the most controversial one is Patriot Act under which the government can demand access to consumers’ data and the cloud service providers are bound to provide that data without consumers’ consent. In general, EU regulations are more restrictive than regulations of other countries like USA. However, it is not clear how different regulations from various jurisdictions (EU and USA for example) are applied to the data stored and processed in the cloud and whether they are compatible. Perhaps, we need some kind of international legislation to deal with this issue.

Nevertheless cloud computing is being pursued as a very important paradigm and its architectural features allow users to achieve better operating costs and be very agile by facilitating fast acquisition of services and infrastructural resources as and when needed. However, these unique features also give rise to various security and privacy concerns (Takabi, Joshi & Ahn, 2010). Without appropriate security and privacy solutions designed for clouds this potentially revolutionizing computing paradigm could become a huge failure. Several surveys of potential cloud adopters indicate that security and privacy is a number one concern hindering its adoption (Catteddu & Hogben, 2009; Bruening & Treacy, 2009). However, cloud computing is here to stay because of its potential benefits and hence, understanding the security and privacy risks and developing effective solutions are critical to the success of this new computing paradigm (Takabi, Joshi & Ahn, 2010).

In this chapter, we focus on access control and policy management. The cloud environment does not allow use of a single authorization mechanism, single policy language or single management tool for various cloud service providers. Each cloud service provider has its own access control solution. Authorization component is often tightly
Policy Management in Cloud

bound to cloud service provider. This approach is not user-centric and hence, can be a significant bottleneck to its widespread adoption. The definition of access control policies clearly is the business of the organization/users deploying the cloud service. However, not only the cloud service providers themselves are dictating how these policies should be defined but also each of them does it in its own way. An ideal access control scheme must be able to work with all types of content regardless of where they are stored. Users should be able to manage policies to govern access to their information and resources from a central location.

Currently, users must use different access control mechanisms available for each cloud service provider to secure their data and control its dissemination. Access control policies to protect users’ resources may be specified in incompatible policy languages and maintained separately at every cloud service provider (Takabi, Joshi & Ahn, 2010). When such mechanisms are used on a daily basis, they add considerable overhead. This may frustrate users and make them feel that they have given up all control of where their data ends up and how it is used. The challenge here is to design an integrated access control framework that can be used across services from different providers. Security solutions delivered as cloud-based services will have a dramatic impact on the industry. Cloud computing will enable security controls and functions to be delivered in new ways and by new types of service providers. It will also enable customers to use security technologies and techniques that are not otherwise cost-effective. Enterprises that use cloud-based security services to reduce the cost of security controls and address the new security challenges that cloud based computing will bring are most likely to prosper.

In this chapter, we describe a cloud based policy management framework that puts users in full control of their resources which may be scattered across multiple cloud service provid-
Policy Management in Cloud

In this section, we discuss policy management in cloud. First, we show how policy management systems in the cloud are heterogeneous using an example. Then, we describe the problem of policy management and its requirements in cloud computing environment. Finally, we present a cloud based policy management framework.

Use Case Scenario

In this section, we present a use case scenario to show heterogeneity of policy management systems and discuss how individual users and organizations that use cloud services can benefit from the policy management framework we propose.

Alice is a PhD student who uses multiple cloud services from different service providers for various purposes. She is working on a research project and wants to have access to the project files from anywhere. Sometimes she works at her office using her PC and other times she works at home or a coffee shop and uses her laptop. For synchronizing the project files, she uses Dropbox, a file hosting service which uses cloud computing to enable users to store and share files and folders with others across the Internet using file synchronization (http://www.dropbox.com). Sometimes she needs to share some of the project files she stores at Dropbox with her colleagues or her advisor.

She has accounts in Facebook, a social networking site that allows users to create a personal profile, add other users as friends and share information, to communicate with her friends and family (http://www.facebook.com). She has also a professional account in LinkedIn, a business-oriented social networking site with the purpose of maintaining a list of contact details of people users know and trust in business, to be in touch with professionals in her field (http://www.linkedin.com).

Alice may also have other documents and spreadsheets that include important content like financial data and she uses Google Docs, a service to create and share various types of files online and access them from anywhere (http://docs.google.com). Moreover, she stores some of her older files at Amazon S3, an online storage service that provides unlimited storage through a simple web services interface (http://aws.amazon.com/s3). She occasionally shares some of these files

POLICY MANAGEMENT IN CLOUD

Table 1. Security and privacy implications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Security Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outsourcing</td>
<td>Users may lose control of their data. Appropriate mechanisms needed to prevent cloud providers from using customers’ data in a way that has not been agreed upon in the past.</td>
</tr>
<tr>
<td>Extensibility</td>
<td>There is a tradeoff between extensibility and security responsibility for customers in different delivery models.</td>
</tr>
<tr>
<td>Multi-tenancy</td>
<td>Issues like access policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment.</td>
</tr>
<tr>
<td>Service Level Agreement</td>
<td>The main goal is to build a new layer to create a negotiation mechanism for the contract between providers and consumers of services as well as the monitoring of its fulfillment at run-time. Also, ensuring that cloud providers and clients comply with established SLAs.</td>
</tr>
<tr>
<td>Virtualization</td>
<td>There needs to be mechanisms to ensure strong isolation, mediated sharing and communications between virtual machines. This could be done using a flexible access control system to enforce access policies that govern the control and sharing capabilities of VMs within a cloud host.</td>
</tr>
<tr>
<td>Heterogeneity</td>
<td>Different cloud providers may have different approaches to provide security and privacy mechanisms, thus generating integration challenges.</td>
</tr>
<tr>
<td>Compliance &amp; Legal Issues</td>
<td>Cloud computing raises legal issues like liability, data protection, compliance, and data portability. There needs to be mechanisms to ensure that cloud providers and clients comply with existing regulatory requirements.</td>
</tr>
</tbody>
</table>
Table 2. Security and privacy challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Issues raised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and Identity Man-</td>
<td>• Interoperability issues resulting from using different identity tokens and different identity negotiation protocols.</td>
</tr>
<tr>
<td>agement</td>
<td>• Privacy concerns related to protection of private and sensitive information associated with users and processes.</td>
</tr>
<tr>
<td></td>
<td>• The effect of multi tenancy on the privacy of identity information.</td>
</tr>
<tr>
<td>Access control</td>
<td>• Domains’ diverse access requirements</td>
</tr>
<tr>
<td></td>
<td>• enough flexibility to capture dynamic, context or attribute/credential based access requirements</td>
</tr>
<tr>
<td></td>
<td>• integrate privacy protection requirements derived from complex rules</td>
</tr>
<tr>
<td></td>
<td>• generic access control interfaces for proper interoperability, which demands for a policy neutral access control specification and enforcement framework</td>
</tr>
<tr>
<td>Policy Integration</td>
<td>• Issues such as semantic heterogeneity, secure interoperability, and policy evolution management</td>
</tr>
<tr>
<td></td>
<td>• policy engineering mechanisms are needed to integrate access policies of different cloud service providers and define global access policies to accommodate all collaborators’ requirements</td>
</tr>
<tr>
<td></td>
<td>• semantic conflicts and/or inconsistencies among their policies</td>
</tr>
<tr>
<td>Trust Management</td>
<td>• very dynamic/transient and intensive interactions</td>
</tr>
<tr>
<td></td>
<td>• Capture a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements.</td>
</tr>
<tr>
<td></td>
<td>• support the establishment, negotiation and maintenance of trust to adaptively support policy integration</td>
</tr>
<tr>
<td>Service Management</td>
<td>• the traditional WSDL cannot fully meet the requirements of cloud computing services description</td>
</tr>
<tr>
<td></td>
<td>• issues like QoS, service price, and SLAs are critical in service search and service composition</td>
</tr>
<tr>
<td>Privacy and Data Protection</td>
<td>• By migrating workloads to a shared infrastructure, customers’ private information is on increased risk of potential unauthorized access and exposure.</td>
</tr>
<tr>
<td></td>
<td>• Provide a high degree of transparency into operations and privacy assurance.</td>
</tr>
<tr>
<td></td>
<td>• Privacy protection mechanisms need to be potentially embedded in all the security solutions</td>
</tr>
<tr>
<td></td>
<td>• Balancing between data provenance and privacy is a significant challenge in clouds where physical perimeter is abandoned</td>
</tr>
<tr>
<td>Organizational Security Manage-</td>
<td>• Shared governance can become a significant issue if not properly addressed</td>
</tr>
<tr>
<td>ment</td>
<td>• Dependence on the external entities can also raise fears about timely response to security incidents, and implementing systematic business continuity and disaster recovery plans.</td>
</tr>
<tr>
<td></td>
<td>• newer risks introduced by a perimeter-less environment, possible data leakage within multi-tenant clouds, and resiliency issues such as local disasters and economic instability of the providers</td>
</tr>
<tr>
<td></td>
<td>• Existing life cycle models, risk analysis and management processes, penetration testing and service attestation need to be critically re-evaluated to ensure that the potential benefits of clouds can be enjoyed by cloud clients.</td>
</tr>
<tr>
<td></td>
<td>• Insider attack surface is significantly extended when outsourcing data and processes to clouds.</td>
</tr>
<tr>
<td>Compliance &amp; Legal Issues</td>
<td>• Although some of the existing regulations can be applied to the cloud, the data protections laws are outdated and are not able to deal with all the legal problems raised in cloud landscape.</td>
</tr>
<tr>
<td></td>
<td>• Many laws in different countries restrict the transfer of data out of the country. Mechanisms are needed to deal with these situations and ensure compliance with the regulation.</td>
</tr>
<tr>
<td></td>
<td>• It is not clear what regulations are applicable when data is transferred across various jurisdictions in regional, national or international levels.</td>
</tr>
</tbody>
</table>
languages which are challenging tasks for her and most users like her. Moreover, introducing new access policy rules or modifying existing ones is problematic due to heterogeneity of these access policy mechanisms. Suppose Alice wants to modify an access policy rule to a resource or a set of resources, or a new colleague is added to her current project and she needs to share some resources with him. In order to do this, she needs to scan all her applications and services to modify access policy rules. In order to better manage security, Alice needs a centralized policy management system to have a better view on access policies applied to her resources. Cloud based policy management service not only allows Alice to centralize management of her access control policies but also enables her to find errors or inconsistencies in the specified access policies very quickly. The access control policies can be applied to a distributed set of resources hosted on various cloud service providers. It gathers information from all of the services Alice uses and provides her with an interface to centrally manage access to her resources regardless of where they are stored at and what cloud service provider they belong to.

**Limitations of the Existing Policy Management Systems**

In this section, we analyze the scenario described previously in order to identify limitations of existing access control mechanisms for the cloud and determine requirements that an access control mechanism should have to be able to address those limitations and be an appropriate candidate for the cloud environment. Some of the limitations of the existing policy management mechanisms are as follows.

- **Authorization mechanisms are bound to service providers:** each cloud service provider employs its own authorization model where access control mechanism is bound to the service and application. In some cases these access control mechanisms can only address simple scenarios where data is either made public or accessible only by a predefined set of users of the application. This limits the configuration of the application and it cannot be easily adapted to particular user’s security requirements. Alice, for example, must use the mechanisms provided by Dropbox, Facebook, LinkedIn, Google-Docs, Amazon S3, and Mint which may not necessarily meet all her security requirements. These mechanisms may not allow Alice to group users and assign access rights to such groups or may not support fine-grained access control policy rules. Most security novice users probably choose their preferred services based on their functionality rather than based on their security features. However, security conscious users may decide to leave cloud service providers which do not support particular security features.

- **There is no unified policy management system:** There is no unified policy management system used among different cloud service providers. Cloud services are controlled by different authorities and often use different policy specification mechanisms. This leads to access control policies that are composed using diverse and possibly incompatible policy languages. For example, Dropbox uses a simple access control model while Facebook supports a more flexible and expressive access control language. Therefore, Alice is unable to define access control rules only once and apply these rules to her various resources such as photos, video clips and documents which are spread across different cloud Services. Moreover, if Alice decides to move some of her resources from one cloud service provider to another, for example from Dropbox to Amazon S3, then she may not be able to reuse already
defined policies and may need to define these policies again.

- **There is no unified policy management tool:** There is no unified policy management tool used by all cloud service providers. Various cloud service providers deploy different access control solutions and may force users to use their specific policy management tools. This may result in an inconvenient and inconsistent user experience. For example, Alice, to be able to share her resources efficiently and securely, must learn how to use interfaces and management tools at all her cloud services which may differ significantly from one service provider to another. Underlying mechanisms used by these services often are different and incompatible with each other, thus cannot be easily reused for distributed resources hosted at various cloud service providers. Some of these tools are not usable which defeats the purpose of access control system and negatively impacts the intended use of the tool.

- **The access control policies are heterogeneous:** The access control policies in existing solutions are distributed and heterogeneous. As a result, users cannot have a consolidated view of the access control policies applied to their resources over the cloud. In our scenario, Alice does not have a holistic view of the access control policies applied to her information and resources at Dropbox, Facebook, LinkedIn, Google-Docs, Amazon S3, and Mint. Furthermore, with the increasing amount of resources that Alice may store on the various cloud service providers, another challenge is how to manage relations between access policies and resources. Additionally, with the heterogeneity of access policies, in order to introduce new access control policies or modify existing ones, users need to go over all cloud service providers and configure access control policies appropriately which is a challenging task.

Based on the discussion about the aforementioned shortcomings, we believe that approaches to access control for cloud computing environment should enable users to control how their information is shared and with whom. The users should be a core part of access control system and should be able to easily determine how the shared information will be used, and what the consequences of sharing this information are.

However, it appears that existing authorization mechanisms do not support these properties. We need to come up with a usable policy management solution that addresses challenges of the cloud environments and the limitations of existing access policy management systems. The access control solution should provide the granularity, simplicity and usability required to respond to security and privacy challenges in the highly collaborative user-centered cloud environment. The proposed framework should be user centric enabling users to set their access control policies for resources with the use of their preferred policy management system in a centralized location. It should also provide users with usable and unified policy management interfaces and tools and allow them to have a consolidated view of the policies being applied to their resources. At the same time, it should preserve privacy of the users and their access policies and offer a representation-agnostic policy management.

**The Cloud Based Policy Management Framework**

We next present a cloud-based framework that efficiently delivers policy management services. It is built on the concept of centrally expressing user’s security requirements that are applied to a user’s resources scattered across the cloud. Such security requirements are expressed in the form of access control policies to protect users’ resources.
Policy Management in Cloud

distributed across multiple cloud service providers. The framework provides the capabilities to the customers to manage access policies for services and products running on a cloud infrastructure which are accessible through usable interfaces. The customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities. Figure 1 shows a high level view of the framework which includes four main components: cloud user, policy management service provider, cloud service provider, and requester. In the following, we provide a brief overview of each of these components.

- **Cloud User:** A cloud user uses different cloud service providers for various purposes. The cloud user is in charge of managing access policies on the policy management service provider which in turn will be used by cloud service providers to control access to the protected resources when a requester attempts to access them. The cloud user is also responsible for registering the cloud service providers at the policy management service provider so they can communicate the specified access policies.

- **Policy Management Service Provider (PMSP):** A policy management service provider enables the cloud users to define, edit and manage their access policies. The cloud users can specify their policies in natural language which in turn are translated by the policy management service provider into a machine readable policy language. It also conducts a conflict resolution on the policies to find and resolve possible conflicts and finally exports the policies into target cloud service providers. Therefore, a policy management service provider acts as a policy administration point (PAP) and a policy information point (PIP).

- **Cloud Service Provider (CSP):** A cloud service provider offers one or more cloud services that are used by cloud users. A cloud service provider controls access to the protected resources based on the policies specified by the cloud users. It evaluates access requests made by a requester against applicable policies and is in charge of making access decisions and enforce-

*Figure 1. The high level overview of the proposed framework*
Policy Management in Cloud

When a requester attempts to access the protected resources, it is the role of the cloud service provider to make those decisions. Therefore, a cloud service provider acts as a policy decision point (PDP) and policy enforcement point (PEP).

• **Requester:** A requester is an application controlled by a person or a company that interacts with a cloud service provider in order to get access to a protected resource belonging to the specific cloud user. It can be a cloud service provider that accesses resources stored in another cloud service provider.

**The Cloud Service Provider (CSP)**

As shown in Figure 2, each cloud service provider keeps a repository of all the resources that cloud users store and has its own access control system that makes decisions and enforces them based on input from the policy management service provider. The policy framework does not impose any restrictions on what access control model the cloud service providers use and how they make decisions to whether grant an access request or deny it, and enforce those decisions. It means that each service provider has its own policy engine and may use a simple access control matrix or a complex flexible policy engine. Each cloud service provider has also a local policy base to store policies and an authorization API that is used by the policy management service provider to export access policies into the cloud service providers.

**The Policy Management Service Provider (PMSP)**

The policy management service provider (PMSP) is the most important part of the framework and as shown in Figure 2, has two main components, the policy editor and the policy server as explained next.

- The policy editor acts as policy administration point (PAP) and provides interfaces for cloud users to manage access policies in a single centralized location. It facilitates the policy management process for cloud us-

*Figure 2. The proposed framework*
Policy Management in Cloud

ers by allowing them to specify their policies in natural language. It also handles the cloud service provider registration process which will be explained later. Moreover, it includes a policy recommendation unit that uses information related to the cloud user and its resources to recommend some policies; needless to say that the cloud user can accept these recommended policies, modify them or ignore them.

- The policy server acts as policy information point (PIP) and is responsible for interacting with the policy editor and the cloud service providers as well as translating the policies specified by the cloud user into a machine readable policy language. It keeps a repository of registered cloud service providers associated with each cloud user. It is also responsible for the resource discovery process which we will explain later. After the cloud user registers its cloud service providers at the PMSP, the PMSP communicates with each cloud service provider to find resources and stores them in a global resource repository which contains all resources and their association with cloud users and cloud service providers. These resources are presented in policy editor interface to the cloud user to help him/her in specifying policies. Moreover, it receives the policies specified by cloud user in policy editor, parses them, transfers them into machine readable policy language and stores them at a policy base. The output policy language could be XACML (http://www.oasis-open.org/committees/xacml/) or an OWL-based policy language such as Rei (http://rei.umbc.edu). Since there is no one agreed-upon policy language that all cloud service providers use, the framework should have capability to provide the output policies in multiple languages to support as many cloud service providers as possible. Next, the policy server detects and resolves possible conflicts among access policies. And the final step is to export policies into the cloud service providers; the policy server first separates the policies related to each cloud service provider based on the resource-provider association and then exports them into the associated cloud service provider using its authorization API.

The Policy Management Process

At a high level, interactions among components of the proposed framework include the following steps: registering cloud service providers, resource discovery, specifying policies, and exporting policies which are discussed below.

Step 1: Registration of CSPs at PMSP

In this step a cloud user registers all cloud service providers he/she uses at the policy management service provider. This can be achieved by providing the location of the cloud service provider to PMSP. For example, a resource owner may provide the URL of their host application to PMSP by typing it into a text field on a Web page. When the location of the cloud service provider is provisioned to the PMSP, it uses the host-meta discovery mechanism (http://tools.ietf.org/html/draft-hammer-hostmeta-13) to obtain a host-meta document from the cloud service provider. Such a document defines the location of a user authorization URL among other items. The PMSP then uses the user authorization URL to initiate the process of acquiring authorization to communicate with particular cloud service provider. When a PMSP receives the host-meta document from the cloud service provider, it obtains the cloud user’s authorization information to communicate with this cloud service provider. This is achieved by receiving a verification code authorized by resource owner from the cloud service provider. At the end of this step, a PMSP is able to communicate with
the cloud service provider to discover resources and also export access policies specified by the cloud user.

**Step 2: Resource Discovery by PMSP**

After a cloud user registers cloud service providers at the PMSP, we have a repository of all cloud service providers at the PMSP. Next, the PMSP communicates with each of the cloud service providers to discover the resources stored in them. We recommend using POWDER-S or Semantic POWDER (http://www.w3.org/2007/05/powders) for resource description. The Protocol for Web Description Resources (POWDER) facilitates the publication of descriptions of multiple resources such as all those available from a website (http://www.w3.org/TR/powder-dr). These descriptions are always attributed to a named individual, organization or entity that may or may not be the creator of the described resources. Its main unit of information is the Description Resource (DR), one or more of which are contained in a POWDER document. Processing such a document yields RDF triples describing the resources that are within the scope of the DRs. POWDER documents are written in XML and have relatively loose semantics, however, POWDER-S is developed to support Semantic POWDER of Description Resources.

For the cloud service providers that do not support/use POWDER-S, the host-meta discovery mechanism can be used for resource discovery. It contains information about individual resources controlled by the cloud service provider.

**Step 3: Specification of Access Policies at PMSP**

There have been some efforts to allow users to specify policies in controlled natural language. IBM’s SPARCLE tool aims to enable users to enter policy rules in natural language (http://www.research.ibm.com/sparcle). The same system can be adopted to be used in our framework for policy specification. However, it uses structured entry methods and guided natural language which is a kind of controlled natural language for policy specification. The goal here is to allow cloud users to specify their policies in natural language without any restriction. Our framework does not impose any constraints on how cloud users specify access policies.

**Step 4: Translation of Access Policies by PMSP and Exporting them into CSPs**

After the access policies are specified in natural language, the PMSP parses the policy, identifies policy elements, and transforms the policy into machine-readable language. Next, a conflict detection and resolution is done on the policies to remove potential conflicts. Then, using the association between resources and cloud service providers, the policies are separated based on target cloud service provider. Finally, the access policies are exported into their related cloud service provider using an authorization API. In order to export policies into the host applications, we use the W3C Rule Interchange Format (RIF) which is a format to exchange rules between rule engines that operate over both XML and RDF data (http://www.w3.org/TR/rif-overview). RIF is a standard for exchanging rules among rule systems, in particular among Web rule engines. Although it provides more than just a format, the concept of format is essential to the way it is intended to be used. The ultimate medium of exchange between different rule systems is XML and central idea behind the rule exchange through RIF is that different systems will provide syntactic mappings from their native languages to RIF dialects and back. The systems can talk through a suitable dialect, which they both support. In order to be able to communicate rule sets from one system to another, the mappings should be semantics-preserving. Due to its extension mechanisms, RIF is an ideal language to investigate machine-readable first-order logic rules.
The Framework Deployment

In general, for the PMSP to be able to export policies into the cloud service providers, it should be able to exchange data with the CSPs. The ideal situation for PMSP is that cloud service provider supports well known policy languages such as XACML and provides required APIs to exchange data with the PMSP. However, some cloud service providers may not be willing to do any changes and do not support well known policy languages. In this case, it is the responsibility of the PMSP to generate policies in a format that the cloud service provider understands. It is clear that the more machine readable formats the PMSP provides and the more CSPs offer APIs, the more PMaaS would be deployed. The requester sends access requests to the CSP, and the CSP handles them locally. Our proposed framework does not impose any limitations on the requester and the CSP’s decision making functionality. The requester can send a request to access protected resources similar to every other system. The CSP, checks the request against its policy base; makes decision, and grants or denies the access to the requester based on access policies defined by the cloud user.

One approach to implement the authorization API is to use RESTful Web service technology, which enables the remote invocation of the methods for the different parties involved. A RESTful Web service is implemented in the MPSP side and the CSPs are implemented as RESTful clients. The authorization API establishes a secure channel to the PMSP using SSL. Authentication of the provider and server is done using OAuth (http://www.oauth.net) which is an open protocol to allow secure API authorization in a simple and standard method from web applications and a simple way to publish and interact with protected data. The authorization API provides methods to insert, remove, update, access, and search information in the policy base.

Whenever cloud user changes his policies, the PMSP applies the required updates and communicates them with the target cloud service providers. This could be done by push and pull strategy. In push strategy, whenever there is a change, the PMSP updates the policies and exports them to target CSPs while in pull strategy, the CSP initiates the communication and checks for possible policy changes/updates in certain time periods. However, we believe that push strategy is more efficient in this situation. Since the associations between policies, resources, and cloud service providers have been already identified, the PMSP only needs to relate the changes to target cloud service providers and export them. Similarly, whenever cloud users add/remove resources to/from cloud service providers, appropriate updates need to be done. However, in this case we believe that pull strategy is better because resources are stored in cloud service providers and whenever there is a change; CSPs can inform the PMSP to get updated policies.

Advantages and Disadvantages of the Proposed Framework

In the following, we discuss some of the advantages the cloud based policy management service has over existing systems.

- Access policy specification functionality is externalized from cloud service providers and can be done in a centralized location for all cloud providers. Decisions about who has access to what resources are made locally and enforced by each cloud service provider. However, the specification of policies for all resources and services is done centrally in a single location.
- Cloud users use a unified policy management system to control access to all their resources scattered over the cloud. They do not need to deal with various policy management systems bound to each cloud service provider.
Cloud users compose access control policies using natural language and do not need to use various policy specification languages. They do not need to learn different policy languages employed by various cloud service providers and can simply specify policies using natural language.

Cloud users use a single management tool to compose access policies which allows them to have a consistent user experience when managing these policies. They do not need to learn to work with different interfaces and tools that may even not be usable.

Since access policies are composed using a single policy management tool and hosted in a single location, cloud users have a consolidated view of the access policies applied to their resources.

If cloud users move their resources from one cloud service provider to another for any reason, they do not need to redefine all the policies again. For example, if Alice moves one document from GoogleDocs to Amazon S3, she does not need to redefine the policies associated with that document in Amazon S3.

It is easier for users to introduce new access control policies and modify existing ones when needed.

With existing systems, the cloud user is limited to the functionality provided by the cloud service providers’ policy engine. However, our proposed framework may be able to apply extra policies by transforming them into the provider’s policies. For instance, in Facebook Alice can share her location but she is not able to define any temporal constraint on that. If she wants to share her location at some specific times, she cannot do it in Facebook but she can do it using our proposed framework. She can specify a policy that her location should be private between 8 am and 5 pm everyday otherwise it can be shared with friends. Our system exports a policy into the Facebook at 8 am that makes Alice’s location private and when the time is 5 pm, it exports another policy into the Facebook to share her location with friends.

Despite all the advantages the proposed framework provides, it has some drawbacks.

- The question may arise regarding privacy of cloud user’s identity and privacy of his policies and the concern is that cloud users have to trust PMaaS provider to provide their identifications in different cloud service providers and specify their access policies using the PMaaS. We assume that there is enough level of trust between cloud user and PMaaS provider to deploy the service. However, the PMaaS could be deployed as private cloud within an organization’s premise or fully controlled by an individual user to avoid privacy concerns.

- In order to successfully deploy the framework, the cloud service provider should provide some kind of APIs to exchange data with the PMSP and support output languages of the PMSP. In real world, however, some cloud service providers may not be willing to do any changes and the PMSP is responsible to generate policies in a format that the cloud service providers understand. In order to increase its deployment, the PMSP should provide more machine readable formats and we need to incentivize the CSPs to offer APIs for interaction with the PMaaS.

**FUTURE RESEARCH DIRECTIONS**

The issue of integrating policies has been addressed to ensure secure interoperation and policy engineering mechanisms are provided to integrate access
policies of different policy domains and define global access policies. Secure interoperation can be achieved in centralized or decentralized fashion. In a centralized approach, a global policy is created that mediates all accesses and is appropriate for a cloud application that is composed of various services with different requirements and is more or less fixed. In a more dynamic environment, the domains are transient and may need to interact for a very specific purpose and centralized approaches are not appropriate in such cases. Decentralized approaches are needed in such cases.

One key aspect of the complex cloud computing environments is the semantic heterogeneity among policies. There needs to be ways for automatic detection of semantic conflicts among different service providers’ policies. Use of ontology is the most promising approach to address the semantic heterogeneity issue. Combination of OWL 2 and SWRL for policy management has the following advantages:

- It offers high expressiveness by providing a wide variety of constructors to describe knowledge.
- Its reasoning could be implemented using rule-based engines which offer good performance.
- It provides scalable reasoning without sacrificing too much expressive power.
- It provides separation between domain description and policy description.
- It provides heterogeneity management and interoperability among different cloud service providers.

An OWL based framework is desirable to support semantic heterogeneity management across multiple service providers. For such a framework, a system-driven policy framework to facilitate the management of security policies in heterogeneous environments and policy enforcement architecture are essential.

CONCLUSION

The key features of the cloud, among many, that exacerbate the security and privacy issues include outsourcing of data and applications which generate significant concerns related to trust, multi-tenancy, heterogeneity of services, and compliance. Cloud computing is still in its infancy and although security issues are delaying its adoption, it is growing and we need to provide security mechanisms to ensure that cloud computing benefits are fully realized.

We have proposed a cloud based policy management framework that puts users in full control of their resources which may be scattered across multiple cloud service providers. It is designed to give cloud users a unified control point for specifying authorization policies, who and what can get access to their data, content, and services, no matter where all those things live on the cloud. It relies on a user’s centrally located policy manager of those resources and enables users to manage access policies using a centralized policy manager which provides usable interfaces for specifying access policies and exporting them to the cloud service providers on behalf of the user.

We described various components of the framework in detail and explained how these components interact with each other to provide the desired service to customers. We also discussed how to deploy the proposed framework and what are the challenges we face when trying to use the framework with real world applications and services. Furthermore, we have discussed advantages that the proposed framework has over existing systems. There are some privacy concerns that need to be taken into account for its successful deployment. However, with some efforts to incentivize the CSPs to offer appropriate APIs and establishing enough trust for customers, the proposed framework can be deployed and used in real world.
REFERENCES


Policy Management in Cloud


ADDITIONAL READING


KEY TERMS AND DEFINITIONS

Access Control: Access control systems provide the essential services of authorization that determines what actions a subject is allowed to do on an object. In access control systems, subjects are the entities that perform actions and objects are the entities representing resources on which the action is performed.

Cloud Computing: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud Service Provider: A cloud service provider is an entity that offers one or more cloud based services that are used by cloud users.

Interoperability: Interoperability refers to the ability of systems to work together, exchange information, and use the exchanged information without any restricted access or implementation.

Policy Management: The process of defining, modifying and managing access control policies in a system is called policy management.

Semantic Heterogeneity: Semantic heterogeneity means that different entities in a system have differences in interpretation of the meaning of data are source of semantic heterogeneity.

Semantic Interoperability: Semantic interoperability is the ability of computer systems to communicate information in a way that the exchanged information can be automatically and meaningfully interpreted by the receiving system the same as the transmitting system intended. In order to achieve semantic interoperability, both systems should use a common information exchange reference model and they should derive the same inferences from the same information.

Semantic Web: The Semantic Web is a web of data that can be processed directly and indirectly by machines. It is a system that enables machines to understand and respond to complex human requests based on their meaning. The Semantic Web is not a separate Web but an extension of the current one, in which information is given well-defined meaning, better enabling computers and people to work in cooperation.