A Framework to Develop Security Policies for Cloud Computing

Vijay Kumar Damera¹, Suresh Pabboju² and Putta Narsaiah³

¹Department of Information Technology, MGIT, Hyderabad, A.P, INDIA
²Department of Information Technology, CBIT Hyderabad, A.P, INDIA
³Department of CSE, Vasavi College of Engg., Hyderabad, A.P, INDIA

ABSTRACT

Cloud Computing has become a buzzword of today. Security is the major challenge for cloud computing. The majority of companies deploying cloud computing solutions have no cloud-specific security policies and procedures in place and have no measures to approve or evaluate cloud applications that use sensitive or confidential information. There is no integrated model-based framework available to develop cloud security policies that deal with both internal and external security challenges. This paper proposes a framework to provide solution to the above problem. This framework is useful in specifying Cloud security requirements and to develop policies to meet them.

Keywords: Cloud Computing, Security, Security Policy and Malactivity.

1. INTRODUCTION

A carefully crafted security policy outlines what cloud computing service consumers and providers should do. It can save providers many hours of management time if they develop a security policy. The security policy is shaped by four things:

- What type of cloud service the provider hosts: Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).
- Whether it is public or private.
- How much control the consumer has over the operating systems, hardware, and software.
- How the user, resource, and data requests threshold policies are applied to each cloud service type

Cloud computing systems that consider security from the initial requirements and design stages are more secure. Security requirements are generally not analyzed early enough in the system development process, and few organizations proactively safeguard sensitive business information stored in the cloud because they lack cloud-specific security policies [1]. Due to the complexity of the cloud environment, effective testing demands that nonfunctional requirements such as those related to security be analyzed and policies be developed early to address them in the development process using a comprehensive approach that considers the entire cloud.

The unified modeling language (UML) [2] that is most often employed to bring out requirements was not initially designed to capture security requirements. The existing methods to analyze security requirements do not consider both internal and external threats in a structured manner.

Cloud computing is not necessarily any more secure internally than non cloud computing environments as internal threats have steadily increased over the past few years. Internal misusers generally have more knowledge of access to data and applications than external misusers. Although internal threats cannot be entirely eliminated, some effective barriers can be developed to mitigate them.

It is crucial to use an approach which is based on top-down method to analyze security requirements and to develop effective security policies. Security policies themselves do not solve problems but can complicate things if they are not clearly written and consistently observed. Policies do define an ideal toward which all organizational efforts should point. So, a systematic methodology and process are necessary to develop security policies for cloud computing systems. This approach must identify security requirements at different levels to address threats, through user scenarios, posed by both internal and external misusers and thus to develop clear cloud security policies that ensure the security of the cloud environment. The process presented here employs the high-order object oriented modeling technique [3] together with use cases [2], misuse cases [4] and malactivity swimlane diagrams [5].
2. BACKGROUND OF CLOUD COMPUTING

The boom in cloud computing over the past few years has led to a situation that is common to many innovations and new technologies: many have heard of it, but far fewer actually understand what it is and, more importantly, how it can benefit them. A common understanding of “cloud computing” is continuously evolving, and the terminology and concepts used to define it often need clarifying. Press coverage can be vague or may not fully capture the extent of what cloud computing entails or represents, sometimes reporting how companies are making their solutions available in the “cloud” or how “cloud computing” is the way forward, but not examining the characteristics, models, and services involved in understanding what cloud computing is and what it can become.

According to the National Institute of Standards and Technology, the cloud computing model grants 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 [6]. Cloud computing is still evolving; therefore, its definitions, applications, underlying technologies, issues, risks, and benefits continue to be refined.

Cloud service providers (CSPs) deliver applications and services that run in the cloud; that is to say, they are accessible through the web. A key attraction of cloud computing services is that they conceal the complexity of the infrastructure from developers and end users. Hence developers and users do not know or need to know what is in the cloud – they require only that it deliver the services they need. CSPs offer three basic services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). All these services offer scalability and multitenancy. In addition, they are self-provisioning and can be deployed through private, public, community, or hybrid cloud deployment modules.

2.1 Hierarchical cloud Architecture

This section presents hierarchical cloud architecture. Figure 1 shows a hierarchical design of cloud computing architecture. The figure is best explained from the bottom up. At the bottom is the system level, which serves as a foundation and the backbone of the cloud. It consists of a collection of data centers that supply the computing power in the cloud environment. At this level, there exist enormous physical resources such as storage disks, CPUs, and memories.

Just above the system level is the virtualization level. Virtualization, the factor that facilitates cloud computing, is an abstraction of applications and services from the underlying physical services. It is achieved with the help of a hypervisor, a software or hardware that serves as a bridge between physical devices and virtual applications. This abstraction ensures that no application or service is tied directly on the hardware resources. This level manages the physical resources and allows sharing of their capacity among virtual instances of servers, which can be enabled or destroyed on demand. The physical cloud resources and their virtualization capabilities form the basis for delivering IaaS.

The user-level middleware includes software-hosting platforms such as Web 2.0 Interfaces that permit developers to create rich, cost-effective user interfaces for web-based applications. It also provides the programming environments and tools that ease the creation, deployment, and execution of applications in clouds. This level aims at providing PaaS capabilities.

3. THE HIGH-ORDER OBJECT – ORIENTED TECHNIQUE (HOOMT)

The HOOMT addresses a challenge faced by requirement analysts and software engineers to develop well-structured object-oriented software systems [3]. It incorporates the object-oriented paradigm seamlessly into a structured analysis [3]. It also permits the development of object, functional, and dynamic models hierarchically according to their abstraction levels. The process eliminates incompatibility between a flat object model, in which all modelling elements are analysed at a single level of abstraction, and hierarchical functional and dynamic models, in which modelling elements are analysed at multiple levels of abstraction. It uses hierarchical decomposition in the analysis and design of
object functionality and dynamic behaviour. HOOMT also has a unique starting point and incorporates non functional requirements.

It has three models:

- The high-order object model (HOOM),
- The hierarchical object information flow model (HOIFM), and
- The hierarchical state transition model (HSTM).

This work uses HOOM extensively to model the assets of the target system (i.e., the cloud) hierarchically.

3.1 Security Challenges Faced By Cloud Computing Systems

Cloud computing is prone to various kinds of external security risks such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. In addition, and particularly in the public cloud deployment module, since data is hosted by the CSP, trust, confidentiality, and privacy are also important issues. Finally, communication among clouds must be secured to prevent man-in-the-middle (MITM) attacks.

Although data stored in the cloud and other compute capabilities are not actually in the cloud; they reside in data centers housing hundreds of servers, thousands of networking cables, and other physical devices. Nonetheless, physical threats are among the greatest dangers to the cloud. Most CSPs are acutely aware of these threats to their core IT infrastructure from natural disasters, terrorist threats, fire, sabotage, and other phenomenon.

CSPs, especially IaaS providers, offer their customers the illusion of unlimited compute, network, and storage capacity, often coupled with a frictionless registration process that allows anyone with a valid credit card to register and begin using cloud services immediately [7]. The relative anonymity of these registration and usage models encourages spammers, malicious code authors, and other misusers, who have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from such attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well [7].

Researchers, however, have not generally operated on the notion that security should be built around the application, not the virtual machines; therefore, hypervisors are not sufficiently robust. Further, since communication with the hypervisor contains vital information, including account names and passwords, it must be secure. Like physical computers on a physical network, virtual machines have identical IP addresses. Nearby addresses, which are visible to users in the cloud, often share the same hardware. Thus, a misuser can determine which physical servers a victim is using within the cloud, implanting a malicious virtual machine at that location from which to launch an attack [8]. Finally, in a virtualized environment, it is relatively easy to steal an entire virtual server, along with its data, without anyone noticing. Virtual machines are encapsulated in virtual disk files that reside on a virtual host server; therefore, anyone with the right permissions can copy the disk file and access data on it.

4. THE APPROACH

4.1 Framework Of The Structured Development Of Cloud Security Policies

The approach used here to develop security policies in a cloud computing environment involves two phases: First, cloud security requirements are analyzed. Second, cloud security policies are developed, and measures are put in place to communicate and enforce them. Figure 2 shows a high-level view of the approach.

![Figure 2. A High-Level View of the Approach](image)

As noted above, the HOOMT, which is a major aspect of this approach to the analysis of cloud security policies, provides a structured object-oriented design methodology based on hierarchical model development (see figure 3). HOOMT allows every object in the cloud to be modeled comprehensively and verified systematically for completeness. The analysis process introduced here integrates use cases, misuse cases, and malactivity swimlane diagrams with the HOOM. The malactivity swimlane diagrams decompose misuse cases, revealing in detail the activities of misusers.
Also, detailed investigation of each incidence of malactivity permits development of more ways to prevent or mitigate such activity. This technique serves as a countermeasure for identified threats. Moreover, more threats can be identified this way, making possible the development of comprehensive cloud security policies. The result is a more efficient way to discover threats posed to cloud computing systems, both internally and externally. The structured development of the cloud security policies together with the relationships among the various diagrams at each level is shown in figure 3.

### 4.2 Cloud Security Requirement Analysis

Figure 4 outlines the process of analyzing to cloud security requirements. The process begins with the development of a context object diagram (COD) for the cloud computing system; this is considered as a high-order object. This COD represents the entire cloud computing system and shows its interactions with external objects such as users, either internal or external. The COD also serves as the starting point for the analysis process.

The next step is to identify use cases that describe how the cloud computing system responds to requests from users. These cases capture the behavioral requirements of the cloud computing system with detailed scenarios derived from the cloud’s functionalities. Next, each use case is analyzed thoroughly to determine how it could be subverted. Based on this analysis, misuse cases and misusers, either internal or external, that can harm the cloud computing system are identified. The misuse cases also reveal the various threats posed to the cloud at each level of the hierarchical model.

![Figure 3. Framework of the Structured Development of Cloud Security Policies](image)

To identify security requirements that can serve as countermeasures to these misuse cases, the actions taken by misusers must be understood in detail. Malactivity swimlane diagrams can be used to further decompose misuse cases. Decomposition reveals the details of such misuse events and thus permits identification of more threats. It also permits the inclusion of both hostile and legitimate activities and determines the point at which prevention and mitigation options can be added to these activities to serve as countermeasures. Based on the countermeasures, security requirements are specified.

The COD is further decomposed and the cycle repeated, generating cloud security requirements at the end of every cycle. The term decompose refers to a process that reveals the subcomponents of the cloud object at a lower level [9]. The decomposition and security requirements analysis process continues until a stage is reached at which the cloud objects are primitive and corresponding use and misuse cases are fully explored [9]. At that point, the cloud security requirements are refined by checking for inconsistencies and ambiguities. They serve as a deliverable at the end of the first phase of the approach.

![Figure 4. Cloud Security Requirements Process](image)
4.3 Cloud Security Policy Development, Communication And Enforcement

In this framework, the security policies for cloud computing systems are based on the cloud security requirements through the security requirements analysis process. Policies and requirements are not necessarily mapped one-to-one. Usually, one requirement can be satisfied by a set of security policies. These requirements are high-level statements of countermeasures that will adequately prevent or mitigate identified misuse cases and are dependent on rigorous analysis of threats to the cloud at each level [7], as described above. Consequently, security policies are developed and integrated into the development of the cloud computing system. This approach provides a framework of best practices for CSPs and makes security policies tenable. The policies ensure that risk is minimized and that any security incidents are met with an effective response [7]. The process of developing these policies permits authorized security personnel to monitor and probe security breaches and other issues pertaining to cloud security.

The process begins with a statement articulating the motivation for developing such a policy, describing the malactivities to be governed by it, and listing the cloud assets to be protected. The problem the policy is designed to resolve is articulated. In general, the overall benefit of the policy is described. Next, those individuals or groups who must understand and observe this policy in order to perform their job are identified. Any exceptions to this policy are also noted.

At this point, the policy itself is articulated, including a description of what is actually covered by the policy, the responsibilities of the various individuals or groups involved, and the technical requirements that each individual or device must meet to comply with the policy.

Finally, once cloud security policies have been developed, they must be disseminated to users, staff, management, vendors, third party processors, and support personnel. The complexity of the cloud environment demands that some, if not all, policies be communicated to consumers. Enforcing these policies is also an essential part of the process. This is accomplished by establishing a record that those involved have read, understood, and agreed to abide by the policies, and by discussing how violations will be handled. Figure 5 illustrates the process described above to develop security policies for cloud computing systems.

![Figure 5. Cloud Security Policy Development Process](image)

5. Conclusion

Cloud computing is becoming popular and represents the future of computing. Before it can be embraced by individuals and enterprises, however, the issue of security must be addressed. Early consideration of security in cloud computing systems places it on a par with other functional requirements of the system and significantly improves the security of the system. This paper has successfully addressed these security issues, by developing a process to determine security requirements and develop policies for a cloud computing system level-by-level in a structured manner. This
methodology analyzes security requirements by identifying threats posed by misusers both external and internal to a system.

References


