# Adaption of Usage Management to Include Security Policy Enforcement
Progress Report

By: Edward Nava, Viswanath Nandina, Jose Marcio Luna

30 July 2012

## Introduction

Our previous months' efforts have been focused on developing an understanding of the cloud computing technologies and formulating strategies on how to extend usage management in way that can implement security policy based provisioning. As part of this process, we have begun the process of defining how such a system should operated and also generated a use case scenario that illustrates how the system would be used in an operational scenario. In parallel, we have also begun the preliminary development of software for a proof of concept demonstration of security policy based control.

## Initial Security Category Classification

The basis for provisioning cloud computing resources is the security category of the information being processed and generated. With any classification system, someone must make a determination that information must be protected in accordance with laws, regulations, corporate practice, etc. and the information is "marked" accordingly. In a similar manner, data and applications intended for use on a cloud computing system must be classified and marked so that usage and handling is done in accordance with the appropriate guidelines. This basic process is illustrated in the UML activity diagram shown below in figure 1.

In the classification process, a classifier will assign High, Moderate, or Low values to the security objectives of confidentiality, integrity, and availability. This is represented by the triple **SC**{C,I,A}. The security category information is encoded in XML and is stored in manner that allows for automatic access whenever the resource is accessed. (For data stored in a repository such as the Amazon S3 service, the XML data is stored directly with the data.) A typical XML entry might look like:

```
<?xml version="1.0" encoding="UTF-8"?>
<security_category>
   <confidentiality>H</confidentiality>
   <integrity>L</integrity>
   <availability>L</availability>
</security_category>
```

XACML is an XML based language and allows for custom extensions. So, this security category definition would be appropriate and could be used with the large repository of XACML library functions.

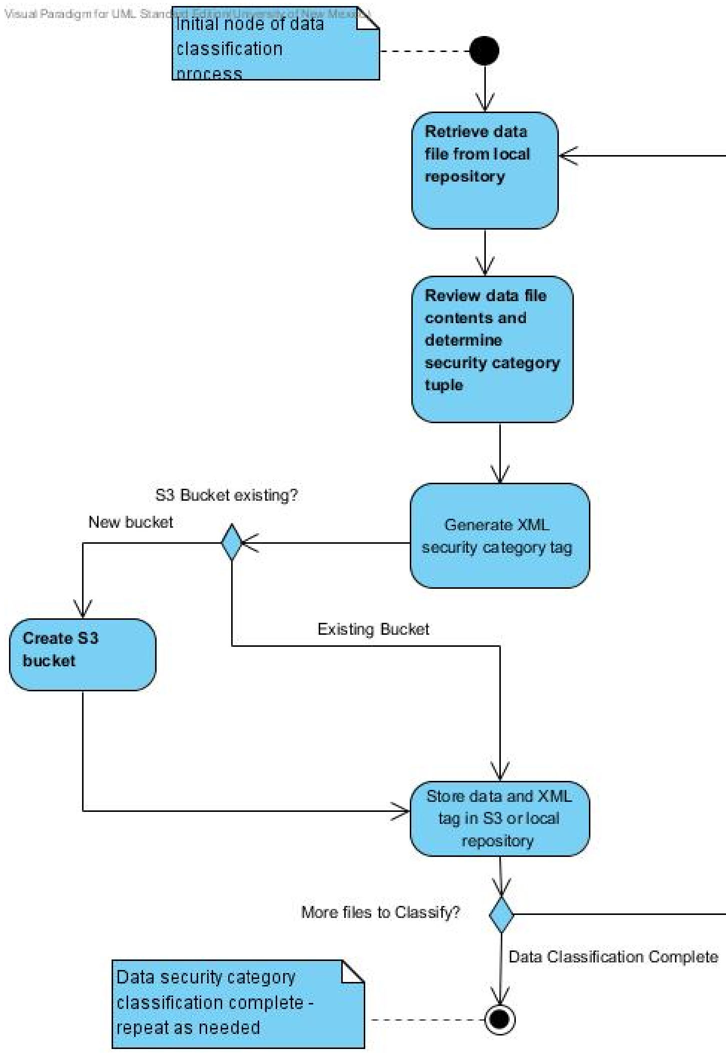
Visual Paradigm for UML Standard Edition(University of New Mexico)
Initial node of data classification process
Retrieve data file from local repository
Review data file contents and determine security category tuple
Generate XML security category tag
S3 Bucket existing?
New bucket
Existing Bucket
Create S3 bucket
Store data and XML tag in S3 or local repository
More files to Classify?
Data Classification Complete
Data security category classification complete - repeat as needed

**Figure 1 Data Classification Activity Diagram**

The data classification process is needed to identify which protective measures must be used when storing, transmitting, and using the data. Depending on the security category, measures such as encryption, message authentication coding, and redundant storage must be used. The use case scenario for initializing a system that uses data of different security categories is shown in figure 2.

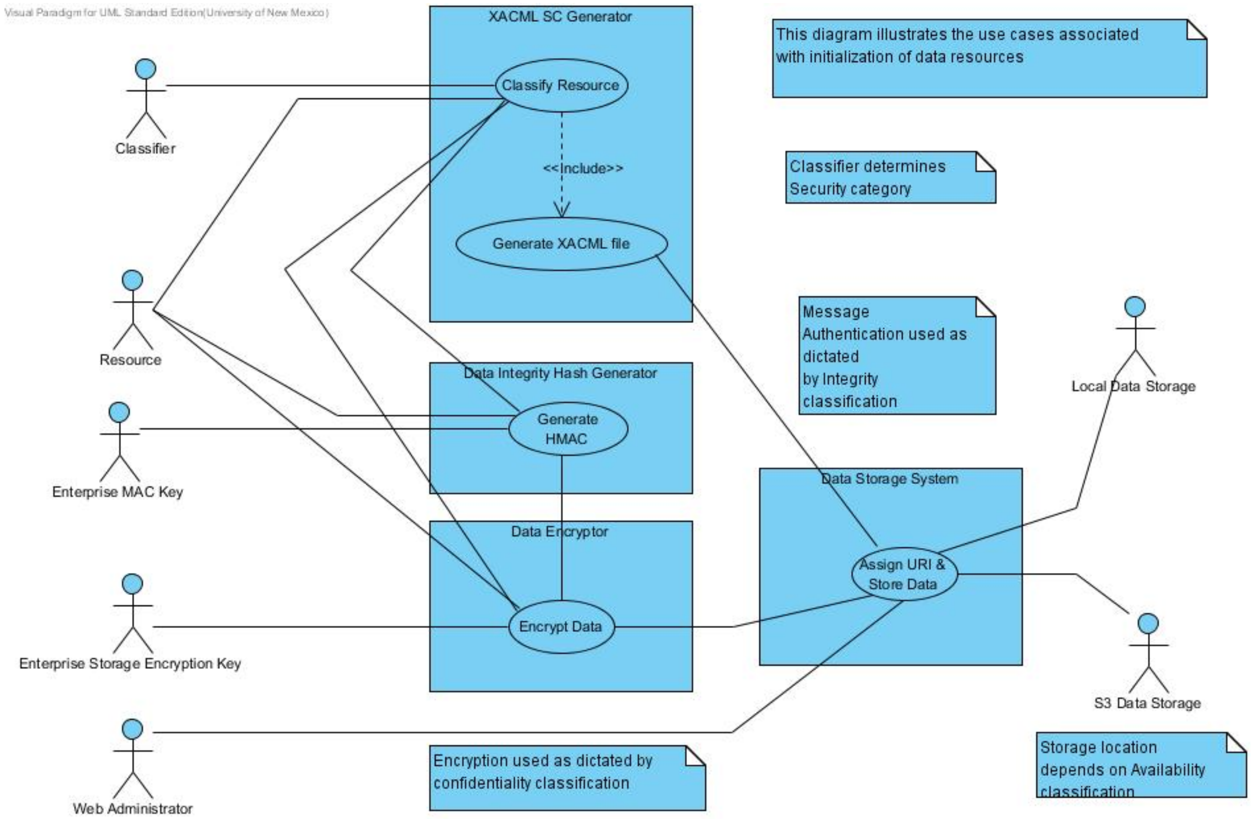
Visual Paradigm for UML Standard Edition(University of New Mexico)
XACML SC Generator
Classify Resource
<<Include>>
Generate XACML file
This diagram illustrates the use cases associated with initialization of data resources
Classifier determines Security category
Classifier
Resource
Message Authentication used as dictated by Integrity classification
Local Data Storage
Data Integrity Hash Generator
Generate HMAC
Enterprise MAC Key
Data Storage System
Data Encryptor
Assign URI & Store Data
Encrypt Data
Enterprise Storage Encryption Key
S3 Data Storage
Web Administrator
Encryption used as dictated by confidentiality classification
Storage location depends on Availability classification

**Figure 2 Data Classification and Storage Use Case Diagram**

## User Access of Cloud Resources

Ultimately, a user will need to access resources to accomplish some computational task. The user will first have to be authenticated and the usage context must be determined; a user accessing data with high confidentiality might be undesirable if he or she is accessing the system on a mobile device on a public wireless network and context verification can be used to deny this type of access.  Once the user is authenticated by the usage management system, then a web server can present them with links to resources for with they are authorized access.  The user access use case is shown below in figure 3.

When a user clicks on a link to a advertized web application, we assume that the program processes information of a predetermined security category and the control system instantiates a virtual machine that is configured to add the protective measures necessary for the information.  Similarly, if a user clicks on a data link, the control system automatically instantiates a virtual machine with the protection measures needed for the information so that the user can process the data with the generic applications that reside on all virtual machine images, such as word processors.

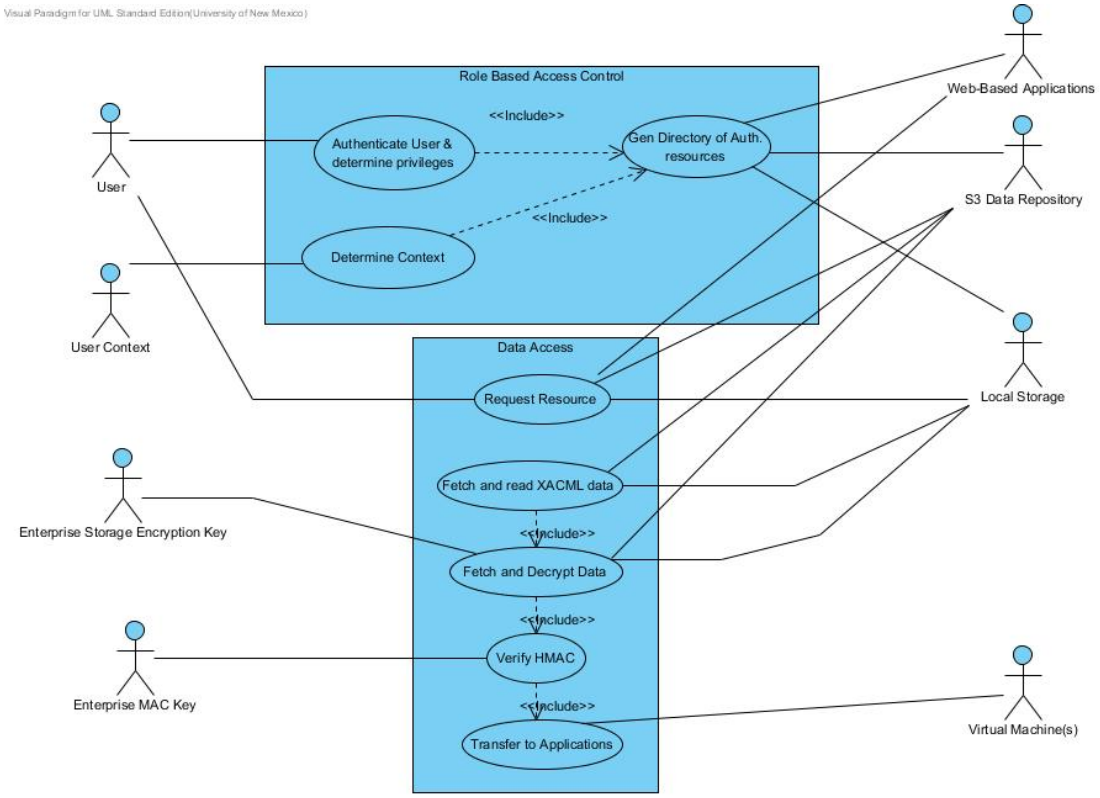

**Figure 3 User Resource Access Use Case Diagram**

## Operational System Use Case

In a planning scenario for an Unmanned Air Vehicle (UAV) reconnaissance mission, the planner typically must use information from multiple sources in order to develop a plan. This information is aggregated and processed, along with mission objectives, to form a mission plan. As technology advances, this process can be envisioned to be implemented with disparate information and computing resources, as is now done in a cloud computing environment for commercial applications. Information might be supplied by one coalition partner and the actual computing might be done on another coalition partner's hardware. The availability of high speed networks makes this type of operation very likely.

A typical mission planning activity for a UAV mission involves the aggregation of information with different security characteristics. Three specific characteristics are confidentiality, integrity, and availability. In a mission planning scenario, one input could be general map information. Map information could come from freely available sources, such as Google Maps, and would have a low confidentiality rating. Additional map information might be provided by a coalition partner and might have a low confidentiality rating, but would have a high integrity requirement.  Mission planning also requires meteorological data to calculate to flight and loiter times, as well as to assure that the mission will be successful.  The meteorological data would have a high availability requirement.  Specific vehicle performance characteristic data, such as ceiling, range, top speed, etc., would likely have a high confidentiality rating and would require protection throughout its use.  Mission specific requirements, simulation results, and resulting mission plan would have high confidentiality requirements and would require protective measures.

The multiple information sources used to perform simulations will have different security category characteristics.  Simulations will be used to generate the mission plan, which will generally have a high confidentiality requirement.  Because the simulation software will combine multiple sources of information that have varying security category ratings, it must be executed in an environment that is configured for the highest security category associated with the input and output data.

In a web based operational environment, a mission planner will access the planning software using a browser and clicking on a link associated with the application.  The user will be authenticated and authorized access to the application and associated data sources through Usage Management mechanisms.  As the environment is based on cloud computing technology, then as the user clicks on the application link, a virtual machine configured to meet all requirements of the application and source data security categories is instantiated.   (Security category requirements for the application must be predefined and will be based on the highest security category characteristics of the input data.)  Then, the user will select the appropriate input data sources and generate the mission plan.

The handling of all data and applications will be done in accordance with policies implemented in a cloud control system.  Data storage repositories and computational resources will be established and configured to meet security category requirements.  Policies for the usage of these resources will govern the operation of the cloud control system.  However, an operational environment is very dynamic and a means of adapting to dynamic conditions will be required.  For example, today’s ally is sometimes tomorrow’s adversary and so a cloud control system must include provisions for dynamically changing the policies on which the control actions are based.  For example, the control system might provision virtual machines in one coalition partner’s computing enterprise and changing conditions might require that the computing tasks be moved to another computing environment, requiring re-keying operations and temporarily relaxing security category requirements while virtual machine images are being reconfigured.  To adapt to changing conditions, an authorized administrator will have the capability to reconfigure the cloud computing provisioning system as needed.

Ultimately, the operation of this policy based cloud control usage management system is intended to implement the measures necessary to protect information according to the associated security categories, in a manner that is transparent to the mission planner. The control system is designed to fully leverage the available computing resources without requiring the user to be knowledgeable about instantiating and configuring virtual machines.

## Implementation Experiments

A first step in implementing an automatic control system is to develop a capability to store resources and the associated security category information. Once resources are stored, then controlled access to them is needed. To accomplish the first step, we have begun development and testing of software to access Amazon S3 compatible storage systems and our goal is to implement the functionality represented in figures 1 and 2.

We have also begun development of a demonstration capability for usage management of cloud based resources with a role-based access control implementation. This module will serve as the front end for the virtual machine control system; it will instantiate virtual machines that are appropriate for the security category of the user requested resources.

Coupled with the usage management operations, a virtual machine control system will begin operation with a goal of achieving the desired computational performance levels by adding additional or shedding virtual machines as appropriate.

## Summary and Future Efforts:

Our recent efforts have been focused on converting our abstract conceptual ideas to more detailed versions, and beginning the implementation of experimental systems on operational cloud computing hardware. We will continue to develop software that provides a resource classification and storage capability, a user interface to an access control mechanism, and control of cloud computing resources. We will also generate additional UML diagrams as part of the design process, including a component diagram which illustrates the interactions between the various subsystems.

We have also begun the generation of a Software Requirements Specification (SRS). The initial version reflects the system requirements at a high level of abstraction, which corresponds to the research that we have done thus far. As we experiment to determine feasibility of the concepts, the SRS will be modified to add more detail.