Challenges in Cloud Computing Security

Carlos B. Westphall, Carla M. Westphall, Rafael Weingärtner, Daniel R. dos Santos, Paulo F. da Silva, Pedro A. F. Vitti, Kleber M. M. Vieira

Networks and Management Laboratory
Federal University of Santa Catarina
Summary

- Cloud Computing Security Monitoring
- Federated Identity to Cloud Environment Using Shibboleth
- A Vision of Privacy on Identity Management Systems
- Risk-based Access Control Architecture for Cloud Computing
- RAClouds – Risk Analysis for Clouds
Cloud Computing
Security Monitoring
Outline

1. INTRODUCTION
2. RELATED WORKS
3. SECURITY CONCERNS IN CLOUD COMPUTING
4. CLOUD MONITORING
5. SECURITY CONCERNS IN SLA
6. CLOUD SECURITY MONITORING
7. CASE STUDY
Outline

8. KEY LESSONS LEARNED
9. CONCLUSIONS AND FUTURE WORKS
10. SOME REFERENCES
1. INTRODUCTION

- Numerous threats and vulnerabilities that become more important as the use of the cloud increases, as well as, concerns with stored data and its availability, confidentiality and integrity.

- Need for monitoring tools and services, which provide a way for administrators to define and evaluate security metrics for their systems.
1. INTRODUCTION

- We propose a cloud computing security monitoring tool based on our previous works on both security and management for cloud computing.

- Features of cloud computing such as virtualization, multi-tenancy and ubiquitous access provide a viable solution to service provisioning problems.
1. INTRODUCTION

- What are the new risks associated with the cloud and what other risks become more critical?

- We provide some background in security concerns in cloud computing, briefly describe a previous implementation of a monitoring tool for the cloud, show how security information can be summarized and treated under a management perspective.
2. RELATED WORKS

- Uriarte and Westphall [4] proposed a monitoring architecture devised for private Cloud that considers the knowledge requirements of autonomic systems.

- Fernades et al. [5] surveys the works on cloud security issues, addressing key topics: vulnerabilities, threats, and attacks, and proposes a taxonomy for their classification.
2. RELATED WORKS

- Cloud Security Alliance [6] has identified the top nine cloud computing threats. The report shows a consensus among industry experts.

- Mukhtarov et al. [7] proposed a cloud network security monitoring, which is based on flow measurements and implements an algorithm that detects and responds to network anomalies.
3. SECURITY CONCERNS IN CLOUDS

- Each cloud technology presents some kind of known vulnerability: Web Services, Service Oriented Architecture (SOA), Representational State Transfer (REST) and Application Programming Interfaces (API), virtualization, network infrastructure... [8].

- The usual three basic issues of security: availability, integrity and confidentiality are still fundamental in the cloud.
3. SECURITY CONCERNS IN CLOUDS

- Multi-tenant characteristic: one single vulnerable service in a virtual machine, exploitation of many services hosted in the same physical machine.

- Web applications and web services: susceptible to a lot of easily deployed attacks such as SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and session hijacking.
3. SECURITY CONCERNS IN CLOUDS

- Another important topic in cloud security is Identity and Access Management, because now data owners and data providers are not in the same trusted domain [9].

- The main security management issues of a Cloud Service Provider (CSP) are: availability management, access control management, vulnerability management, patch and configuration management, countermeasures, and cloud usage and access monitoring [10].
3. SECURITY CONCERNS IN CLOUDS

- The cloud is an easy target for an intruder trying to use its abundant resources maliciously, and the IDS also has to be distributed, to be able to monitor each node [11].

- Distributed Denial of Service (DDoS) attacks can have a much broader impact on the cloud, since now many services may be hosted in the same machine. DDoS is a problem that is still not very well handled.
3. SECURITY CONCERNS IN CLOUDS

- To maintain data security a provider must include, at least: an encryption schema, an access control system, and a backup plan [12].

- When moving to the cloud it is important that a prospective customer knows to what risks its data are being exposed. Some of the key points considered in this migration are presented in [13, 20, and 21].
3. SECURITY CONCERNS IN CLOUDS

- Legal compliance is fundamental when dealing with cloud computing. In the cloud world, it is possible that data cross many jurisdiction borders.

- Availability and confidentiality are critical to the telecommunications business and if services are being deployed in a public cloud without a proper SLA [15].
4. CLOUD MONITORING

- Our team has previously proposed and implemented an open-source cloud monitoring architecture and tool called the Private Cloud Monitoring System (PCMONS) [14].

- The architecture of the system is divided in three layers: Infrastructure; Integration; and view.
4. CLOUD MONITORING

- **Nagios**
  - View Layer
    - Node information gatherer
    - VM Monitor
    - Database
  - Integration Layer
    - Monitoring tool
    - Configuration Generator
  - Infrastructure Layer
    - Xen
    - OpenNebula
    - KVM
    - Eucalyptus

- **Cloud user**
  - View Layer Extensions
    - Action Module
    - Security Software scripts
  - Integration Layer Extensions
    - Cloud IDS
    - Web App Firewall
    - Encryption Software
    - Authentication Module
    - Vulnerability scanner
    - Network Firewall
    - Integrity Verification Software
    - Backup software
    - Anti-malware
    - ...
5. SECURITY CONCERNS IN SLA

- Providers must have ways to ensure their clients that their data is safe and must do so by monitoring and enhancing security metrics.

- SLAs may also be used in the definition, monitoring and evaluation of security metrics, in the form of Security SLAs, or Sec-SLAs [15].
6. CLOUD SECURITY MONITORING

- We now propose an extension to the PCMONS architecture and tool to enable security monitoring for cloud computing.

- We also present the security metrics which we consider adequate to be monitored in a cloud infrastructure and which provide a good picture of security as a whole in this environment.
6. CLOUD SECURITY MONITORING

- The tool uses data and logs gathered from security software available in the monitored systems, such as IDSs, anti-malware software, file system integrity verification software, backup software, and web application firewalls.

- The entities involved in the definition, configuration and administration of the security SLAs and metrics are:
6. CLOUD SECURITY MONITORING

- Cloud users; Cloud administrators; and Security applications.

- Data Security Metrics, Access Control Metrics and Server Security Metrics are shown in Table I, Table II, and Table III, respectively.

- If a virtual machine has had a huge number of failed access attempts in the last hours we may want to lock any further access.
## 6. CLOUD SECURITY MONITORING

### TABLE I. DATA SECURITY METRICS

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted Data?</td>
<td>Indicates whether the data stored in the VM is encrypted</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>The algorithm used in the encryption/decryption process</td>
</tr>
<tr>
<td>Last backup</td>
<td>The date and time when the last backup was performed</td>
</tr>
<tr>
<td>Last integrity check</td>
<td>The date and time when the last file system integrity check was performed</td>
</tr>
</tbody>
</table>
6. CLOUD SECURITY MONITORING

TABLE II. ACCESS CONTROL METRICS

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Accesses</td>
<td>The number of valid access attempts in the last 24 hours</td>
</tr>
<tr>
<td>Failed access attempts</td>
<td>The number of failed access attempts in the last 24 hours</td>
</tr>
<tr>
<td>Password change interval</td>
<td>The frequency with which users must change passwords in the VM’s operating system</td>
</tr>
</tbody>
</table>
# 6. CLOUD SECURITY MONITORING

## TABLE III. SERVER SECURITY METRICS

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Number of malware detected in the last anti-malware scan</td>
</tr>
<tr>
<td>Last malware scan</td>
<td>The date and time of the last malware scan in the VM</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Number of vulnerabilities found in the last scan</td>
</tr>
<tr>
<td>Last vulnerability scan</td>
<td>The date and time of the last vulnerability scan in the VM</td>
</tr>
<tr>
<td>Availability</td>
<td>Percentage of the time in which the VM is online</td>
</tr>
</tbody>
</table>
7. CASE STUDY

- We have implemented the metrics presented in Tables I-III and gathered the data generated in a case study.

- The following software were used to gather the security information: dm-crypt (encryption), rsync (backup), tripwire (filesystem integrity), ssh (remote access), clamAV (anti-malware), tiger (vulnerability assessment) and uptime (availability).
# 7. CASE STUDY

<table>
<thead>
<tr>
<th>metric</th>
<th>status</th>
<th>timestamp</th>
<th>duration</th>
<th>severity</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>oneadmin i-322 stratus</td>
<td>AVALABILITY</td>
<td>OK</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
</tr>
<tr>
<td>CIPHER</td>
<td>OK</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>AES</td>
</tr>
<tr>
<td>SSH_VALID</td>
<td>OK</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>25</td>
</tr>
<tr>
<td>IS_ENCRYPTED</td>
<td>OK</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>yes</td>
</tr>
<tr>
<td>LAST_BACKUP</td>
<td>OK</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>2014-08-14 18:30:48</td>
</tr>
<tr>
<td>LAST_INTEGRITY</td>
<td>OK</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>2014-08-14 10:23:50</td>
</tr>
<tr>
<td>LAST_MALWARE_SCAN</td>
<td>OK</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>2014-08-14 10:02:42</td>
</tr>
<tr>
<td>VULNERABILITIES</td>
<td>CRITICAL</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>111</td>
</tr>
<tr>
<td>MALWARE_FOUND</td>
<td>CRITICAL</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>5</td>
</tr>
<tr>
<td>PASSWORD_INTERVAL</td>
<td>OK</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>180 days</td>
</tr>
<tr>
<td>SSH_FAIL</td>
<td>WARNING</td>
<td>2014-08-14 15:58:51</td>
<td>4d 1h 16m 40s</td>
<td>1/4</td>
<td>545</td>
</tr>
</tbody>
</table>
7. CASE STUDY

- It represents how the metrics are shown in Nagios and it is possible to see the vision that a network administrator has of a single machine.

- The metrics HTTP CONNECTIONS, LOAD, PING, RAM and SSH are from the previous version of PCMONS and are not strictly related to security, but they are show combined.
8. KEY LESSONS LEARNED

- The tool helps network and security administrator perceive violations to Sec-SLAs and actively respond to threats.
- The major piece of technology used to provide security in the cloud is cryptography.
- Data leakage and data loss are possibly the greatest concerns of cloud users.
- Backup and recovery are also fundamental tools to ensure the availability of customer data.
8. KEY LESSONS LEARNED

- SLAs are fundamental to provide customers with the needed guarantees.

- Definition of requirements and the monitoring of security metrics remain an important open research topic.

- The major decisions in this work were related to the security metrics and the software used to provide the necessary security data.
8. KEY LESSONS LEARNED

- The idea of analyzing logs to obtain security data is classical in information security and it seemed like a natural approach to our challenges.

- To read, parse and present the data we chose to use the Python programming language because it already formed the base of PCMONS (Private Cloud Monitoring System).
8. KEY LESSONS LEARNED

- Setting up a reliable testing environment was also extremely important to the success of the project.

- An important feature of this extension of PCMONS is that it can run over OpenNebula, OpenStack and CloudStack.

- The use of scripting languages in the development process, such as Python and Bash Script allowed us to define the metrics.
9. CONCLUSION AND FUTURE WORK

This work described:

- A few of our previous works in the field of Cloud Computing and how to bring them all together in order to develop a cloud security monitoring architecture; and

- The design and implementation of a cloud security monitoring tool, and how it can gather data from many security sources inside VMs and the network.
9. CONCLUSION AND FUTURE WORK

As future work:

- We can point to the definition and implementation of new metrics and a better integration with existing Security SLAs; and

- It would be important to study the integration of the security monitoring model with other active research fields in cloud security, such as Identity and Access Management and Intrusion Detection Systems.
10. REFERENCES

References indicated in this presentation:


10. REFERENCES

References indicated in this presentation:


10. REFERENCES

References indicated in this presentation:


10. REFERENCES

References indicated in this presentation:


10. REFERENCES

References indicated in this presentation:


10. REFERENCES

References indicated in this presentation:


10. REFERENCES

References indicated in this presentation:


Federated Identity to Cloud Environment Using Shibboleth
Content at a Glance

• Introduction and Related Works
• Cloud Computing
• Identity Management
• Shibboleth
• Federated Multi-Tenancy Authorization System on Cloud
  – Scenario
  – Implementation of the Proposed Scenario
  – Analysis and Test Results within Scenario
• Conclusions and Future Works
Introduction

- **Cloud computing systems**: reduced upfront investment, expected performance, high availability, infinite scalability, fault-tolerance.

- **IAM (Identity and Access Management)** plays an important role in controlling and billing user access to the shared resources in the cloud.
Introduction

• IAM systems need to be protected by federations.

• Some technologies implement federated identity, such as the SAML (Security Assertion Markup Language) and Shibboleth system.

• The aim of this paper is to propose a multi-tenancy authorization system using Shibboleth for cloud-based environments.
Related Work

• R. Ranchal et al. 2010 - an approach for IDM is proposed, which is independent of Trusted Third Party (TTP) and has the ability to use identity data on untrusted hosts.

• P. Angin et al. 2010 - an entity-centric approach for IDM in the cloud is proposed. They proposed the cryptographic mechanisms used in R. Ranchal et al. without any kind of implementation or validation.
This Work

• Provide identity management and access control and aims to: (1) be an independent third party; (2) authenticate cloud services using the user's privacy policies, providing minimal information to the Service Provider (SP); (3) ensure mutual protection of both clients and providers.

• This paper highlights the use of a specific tool, Shibboleth, which provides support to the tasks of authentication, authorization and identity federation.

• The main contribution of our work is the implementation in cloud and the scenario presented.
The NIST Cloud Definition Framework

**Deployment Models**
- **Private Cloud**
- **Community Cloud**
- **Public Cloud**

**Service Models**
- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**

**Essential Characteristics**
- On Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

**Common Characteristics**
- Massive Scale
- Resilient Computing
- Homogeneity
- Geographic Distribution
- Virtualization
- Service Orientation
- Low Cost Software
- Advanced Security

NOVEMBER 16TH, LISBON, PORTUGAL

Based upon original chart created by Alex Dowbor
Identity Management

- Digital identity is the representation of an entity in the form of attributes.
Identity Management

• **Identity Management (IdM)** is a set of functions and capabilities used to ensure identity information, thus assuring security.

• **An Identity Management System (IMS)** provides tools for managing individual identities.

• **An IMS involves:**
  – User
  – Identity Provider (IdP)
  – Service Provider (SP)
IMS

- **Provisioning**: addresses the provisioning and deprovisioning of several types of user accounts.
- **Authentication**: ensures that the individual is who he/she claims to be.
- **Authorization**: provide different access levels for different parts or operations within a computing system.
- **Federation**: it is a group of organizations or SPs that establish a circle of trust.
• The OASIS SAML (Security Assertion Markup Language) standard defines precise syntax and rules for requesting, creating, communicating, and using SAML assertions.

• The Shibboleth is an authentication and authorization infrastructure based on SAML that uses the concept of federated identity. The Shibboleth system is divided into two entities: the IdP and SP.
Shibboleth

• The **IdP** is the element responsible for authenticating users: Handle Service (**HS**), Attribute Authority (**AA**), Directory Service, Authentication Mechanism.

• The **SP** Shibboleth is where the resources are stored: Assertion Consumer Service (**ACS**), Attribute Requester (**AR**), Resource Manager (**RM**).

• The **WAYF** ("Where Are You From", also called the Discovery Service) is responsible for allowing an association between a user and organization.
In Step 1, the user navigates to the SP to access a protected resource. In Steps 2 and 3, Shibboleth redirects the user to the WAYF page, where he should inform his IdP. In Step 4, the user enters his IdP, and Step 5 redirects the user to the site, which is the component HS of the IdP. In Steps 6 and 7, the user enters his authentication data and in Step 8 the HS authenticate the user. The HS creates a handle to identify the user and sends it also to the AA. Step 9 sends that user authentication handle to AA and to ACS. The handle is checked by the ACS and transferred to the AR, and in Step 10 a session is established. In Step 11 the AR uses the handle to request user attributes to the IdP. Step 12 checks whether the IdP can release the attributes and in Step 13 the AA responds with the attribute values. In Step 14 the SP receives the attributes and passes them to the RM, which loads the resource in Step 15 to present to the user.
Federated Multi-Tenancy Authorization System on Cloud

• **IdM can be implemented in several different types of configuration:**
  - IdM can be implemented in-house;
  - IdM itself can be delivered as an outsourced service. This is called Identity as a Service (IDaaS);
  - Each cloud SP may independently implement a set of IdM functions.

• **In this work, it was decided to use the first case configuration: in-house.**
Configurations of IDM systems on cloud computing environments

IdP functions are delivered as services (IDaaS)

IdP is managed in-house

Standardized API for IDM

Applications are delivered as services (SaaS)

NOVEMBER 16TH, LISBON, PORTUGAL
Federated Multi-Tenancy Authorization System on Cloud

- This work presents an authorization mechanism to be used by an academic institution to offer and use the services offered in the cloud.
- The part of the management system responsible for the authentication of identity will be located in the client organization.
- The communication with the SP in the cloud (Cloud Service Provider, CSP) will be made through identity federation.
- The access system performs authorization or access control in the environment.
- The institution has a responsibility to provide the user attributes for the deployed application SP in the cloud.
- The authorization system should be able to accept multiple clients, such as a multi-tenancy.
Scenario

- A service is provided by an academic institution in a CSP, and shared with other institutions. In order to share services is necessary that an institution is affiliated to the federation.
- For an institution to join the federation it must have configured an IdP that meets the requirements imposed by the federation.
- Once affiliated with the federation, the institution will be able to authenticate its own users, since authorization is the responsibility of the SP.
Scenario - Academic Federation sharing services in the cloud
Implementation of the Proposed Scenario

• A SP was primarily implemented in the cloud:
  – an Apache server on a virtual machine hired by the Amazon Web Services cloud.
  – Installation of the Shibboleth SP.
  – Installation of DokuWiki, which is an application that allows the collaborative editing of documents.
  – The SP was configured with authorization via application, to differentiate between common users and administrators of Dokuwiki.
Implementation of the Proposed Scenario – Cloud Service Provider
Implementation of the Proposed Scenario – cloud IdP
Implementation of the Proposed Scenario

- The JASIG CAS Server was used to perform user authentication through login and password, and then passes the authenticated users to Shibboleth.
- The CAS has been configured to search for users in a Lightweight Directory Access Protocol (LDAP). To use this directory OpenLDAP was installed in another virtual machine, also running on Amazon's cloud.
- To demonstrate the use of SP for more than one client, another IdP was implemented, also in cloud, similar to the first. To support this task Shibboleth provides a WAYF component.
Analysis and Test Results within Scenario

- In this resulting structure, each IdP is represented in a private cloud, and the SP is in a public cloud.

The results highlighted two main use cases:
- **Read access to documents**
- **Access for editing documents**
Conclusions

• The use of federations in IdM plays a vital role.
• This work was aimed at an alternative solution to a IDaaS. IDaaS is controlled and maintained by a third party.
• The infrastructure obtained aims to: (1) be an independent third party, (2) authenticate cloud services using the user's privacy policies, providing minimal information to the SP, (3) ensure mutual protection of both clients and providers.
Conclusions

• This paper highlights the use of a specific tool, Shibboleth, which provides support to the tasks of authentication, authorization and identity federation.

• Shibboleth was very flexible and it is compatible with international standards.

• It was possible to offer a service allowing public access in the case of read-only access, while at the same time requiring credentials where the user must be logged in order to change documents.
Future Work

• We propose an alternative authorization method, where the user, once authenticated, carries the access policy, and the SP should be able to interpret these rules.
• The authorization process will no longer be performed at the application level.
• Expanding the scenario to represent new forms of communication.
• Create new use cases for testing.
• Use pseudonyms in the CSP domain.
Some References


Some References


A Vision of Privacy on Identity Management Systems
Agenda

1. Background
   - Privacy
   - Identity management
   - Federation

2. Challenges

3. Conclusions

4. References
Privacy

Definition

- It is a fundamental human right [2]
- It is the control of release of personal data [1]
- It should be a vital characteristic of computing systems
### Characteristics of privacy [3]

- Undetectability
- Unlinkability
- Confidentiality
Privacy/Paradigms

<table>
<thead>
<tr>
<th>Paradigms of privacy [4]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy as a control</td>
</tr>
<tr>
<td>Privacy as confidentiality</td>
</tr>
<tr>
<td>Privacy as practice</td>
</tr>
</tbody>
</table>
Privacy

Legislation to protect users’ privacy

- Health Insurance Portability and Accountability Act (HIPAA) – USA [6]
- Gramm-Leach-Bliley Act – USA [7]
- The Internet Bill of Rights – Brazil [8]

Legislations main goal

- Protect users against unwilling data disclosure and processing
Identity management/Access control model

Attribute Based Access Control (ABAC)

- Attributes are properties/characteristics of entities
- It uses attributes relevant for the request context
- It evaluates rules against attributes of entities
Identity definition
- Set of attributes that represent a user or a system
- Also known as personally identifiable information (PII)

Example

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>11111010101</td>
</tr>
<tr>
<td>Name</td>
<td>John</td>
</tr>
<tr>
<td>Last name</td>
<td>Smith</td>
</tr>
<tr>
<td>SSN</td>
<td>403289440</td>
</tr>
<tr>
<td>email</td>
<td><a href="mailto:john.smith@home.com">john.smith@home.com</a></td>
</tr>
<tr>
<td>roles</td>
<td>manager</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Identity management

Definition

- The process of managing users’ identity attributes [9]
- It deal with collection, authentication, and use of identities’ attributes
- It provides means to create, manage and use identities
- Allows single sign on (SSO) and single log out (SLO)
Roles in Identity management systems (IMS) [10]

- Users
- Identity
- Identity provider (IdP)
- Service provider (SP)
<table>
<thead>
<tr>
<th>Credential definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes used to authenticate a user a single user</td>
</tr>
<tr>
<td>e.g. a pair of login and password, biometrics or digital certificates</td>
</tr>
</tbody>
</table>
Identity management/Basic processes

Authentication
- Performed at the IdP
- It uses a credential to confirm identity

Authorization
- Mostly performed at the SP
- It uses users’ attributes sent from the IdP to SP
- SP deliberates about the resource delivery
Identity management environment

Single administrative domain
Federation

Definition

- An association of service providers and identity providers
- It allows users to access resources in multiple administrative domains (ADs)
- Users authenticate with their home AD
Federation/picture
Federation/technologies

Exchange data format
- Security Assertion Markup Language (SAML)
- OpenId Connect (JSON)
## Federation/technologies

### Frameworks/tools
- Authentic 2
- Higgins (Personal Data Service)
- OpenAM
- OpenId connect
- Ping federate
- Shibboleth
<table>
<thead>
<tr>
<th>Project</th>
<th>Open Source?</th>
<th>Has a protocol</th>
<th>Owner</th>
<th>Data format</th>
<th>Who uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shibboleth</td>
<td>Yes</td>
<td>No</td>
<td>Internet2</td>
<td>SAML 1/2</td>
<td>Academia</td>
</tr>
<tr>
<td>OpenAM</td>
<td>Yes</td>
<td>No</td>
<td>ForgeRock</td>
<td>SAML 1/2, OpenID Connect</td>
<td>Industry</td>
</tr>
<tr>
<td>Authentic 2</td>
<td>Yes</td>
<td>No</td>
<td>Entr’ouvert</td>
<td>SAML 2, OpenID 1/2</td>
<td>Low adherence</td>
</tr>
<tr>
<td>OpenID Connect</td>
<td>Yes</td>
<td>Yes</td>
<td>OpenID</td>
<td>OpenID Connect (Json)</td>
<td>Industry/ academy</td>
</tr>
<tr>
<td>Higgins</td>
<td>Yes</td>
<td>No</td>
<td>Eclipse</td>
<td>SAML</td>
<td>Low adherence</td>
</tr>
<tr>
<td>Ping Federate</td>
<td>No</td>
<td>No</td>
<td>PingIdentity</td>
<td>SAML e OpenID</td>
<td>Industry</td>
</tr>
</tbody>
</table>
Cloud challenges

- Data management
- Data security
- Data privacy
Challenges on IMS

Lack of user control over PIIs stored on IdP

- Attributes stored out of user’s boundaries
- Administrators with permissions and means to access user’s attributes
- Attributes vulnerable to unwilling access and disclosure
Challenges on IMS

Awareness of disclosure process
- Users are the owners of their attribute
- They must know which data is being disclosed
- They should be able to select/unselect any attribute
Challenges on IMS

Awareness of disclosure process

App XYZ would like to:

1. Know who you are on Google
2. View your email address
3. View your basic profile info

By clicking Accept, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.
Challenges on IMS

Absence of disclosure support during dissemination process

- The dissemination process is a complex task
- The amount of attributes and its combination is huge
- Users do not have know-how to decide which set of attributes can bring more or less risk
Challenges on IMS

Absence of disclosure support during dissemination process
Challenges on IMS

Lack of means to control disclosed attributes

- Can the SP store the attributes? for how long?
- Can it be disseminated to third parties?
- Attributes control enforcement on SPs is a hard problem to solve
- The use of policies with the disclosed attributes can bring some light to this problem
- The use of policies brings up another problem. The policy enforcement on SPs
Conclusions

- There are no definitive answers for the present issues (for now)
- Privacy of attributes on IMS is a recent topic
- Mechanisms to provide effective control of attributes for users are still open for debates
- Disclosure support methods should be carefully studied and added to IMS
- Policy enforcement on SPs is an open problem to solve
Our work

We are researching methods:

- To provide users with control and privacy on attributes
- To assure privacy of attributes between providers interactions (SP-IdP, SP-SP)
- Support for users during the disclosure process
Our work

Funding
- Brazilian Funding Authority for Studies and Projects (FINEP)

Project
- Brazilian National Research Network in Security and Cryptography project (RENASIC)
- Conducted at Federal University of Santa Catarina (UFSC) in the Networks and Management laboratory (LRG).
The end

Discussion moment

- Questions
- Doubts
- Discussions
References

[1] Landwehr, Carl and Boneh, Dan and Mitchell, John C and Bellovin, Steven M and Landau, Susan and Lesk, Michael E.
Privacy and cybersecurity: The next 100 years.

The Universal Declaration of Human Rights.

[3] Birrell, Eleanor and Schneider, Fred B
Federated identity management systems: A privacy-based characterization.

[4] Diaz, Claudia and Gürses, Seda
Understanding the landscape of privacy technologies.

95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
References II


*HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996.*


*GRAMM-LEACH-BLILEY ACT.*

[8] Civil, Casa

*Lei N° 12.965, DE 23 abril de 2014.*

[9] Chadwick, David W

*Federated identity management.*
Foundations of Security Analysis and Design V.

[10] Bertino, Elisa and Takahashi, Kenji

Artech House.
Risk-based Access Control Architecture for Cloud Computing
Agenda

- Introduction
- Related work
- Risk-based access control
- Proposed architecture
- Implementation and experiments
- Conclusion and future work
Introduction

• Cloud computing is a successful paradigm and cloud federations aim to make it even more efficient and scalable by sharing resources among providers

• In highly distributed, dynamic and heterogeneous environments, traditional access control models present problems, such as: scalability, flexibility and the use of static policies

• Dynamic access control models, like risk-based, provide greater flexibility and are able to handle exceptional requests (“break the glass”)
Introduction

• We present a model for dynamic risk-based access control for cloud computing

• The system uses quantification and aggregation of risk metrics that are defined in risk policies, which are created by the owners of the cloud resources

• It is built on top on an XACML architecture and allows the use of ABAC coupled with risk analysis
Related Work

• Fall et al. [1] - presents the first idea of risk-based AC for cloud. Propose using NSA RAdAC, but show no implementation

• Arias-Cabarcos et al. [2] - proposes the use of a fixed set of risk metrics for establishing identity federations in the cloud

• Sharma et al. [3] - uses risk-based AC on top of RBAC for cloud e-Health. Their model has 3 metrics (Confidentiality, Integrity and Availability)
Risk-based Access Control

• Traditional access control models employ static authorization, i.e., every decision is pre-established, based on the policies

• The idea behind dynamic access control is that the access requests must be analyzed taking into account contextual and environmental information such as security risk, operational need, benefit and others

• Real applications may require the violation of security policies, and the support for exceptional access requests is known as “break the glass”
Risk-based Access Control

- Uses a function that evaluates in “real time” each request

- Risk analysis can be qualitative, with levels of risk, or quantitative, where risk is usually defined as: Probability X Impact

- Many approaches to risk quantification: fuzzy logic, machine learning, probabilistic inference, …
  - usually based on the history of users and access
Proposed Architecture

• XACML extension. ABAC and risk-based are taken in parallel and then combined to reach a final decision.
  • Combination rules: Deny overrides, Permit overrides, ABAC precedence, Risk precedence

• Risk decision is based on XML risk policies associated to a resource. A policy defines a set of risk metrics, how to quantify and aggregate them and an acceptable risk threshold

• Quantification and aggregation methods can be local (in the CSP) or external, defined by the resource owner as a web service

• The CSP has a basic risk policy, defining the maximum risk level accepted by it
Overview

XACML core components

- Policy Enforcement Point (PEP)
- Policy Decision Point (PDP)
- Policy Administration Point (PAP)
- Policy Information Point (PIP)
- Obligation Service

Risk Engine

- Risk Policies
- Risk Quantification Web Service

New components
Decision process
Case study - cloud federation

• Identity and Access Management is a big challenge when setting up a cloud federation

• It involves a notion of trust, which is usually mediated by an identity federation, this has two major issues:
  • trust agreements and interoperability

• To decrease the level of trust needed among participating clouds, we incorporate the notion of risk

• Also, interoperability may be increased, because a missing attribute in a message may also be considered as a risk factor, instead of stopping communication
Case study - cloud federation
Considerations

- The architecture allows a flexible AC system

- Risk analysis may be too subjective
  - The support of Obligations is essential

- Risk policies allow the use of many risk metrics, using diverse quantification and aggregation methods from different sources

- The main limitation is the performance overhead due to the processing of the risk policies and the quantification of the risk metrics
Implementation

- Three stages:
  - Access control architecture; Cloud federation; Risk quantification and aggregation methods

- Python, ndg-xacml, ZeroMQ, web.py, peewee, MySQL, OpenNebula

- Two risk policies implemented for tests:
  - Sharma et al. [3] : \((a \times p1) + (i \times p2) + (c \times p3) + \text{pastScore}\)
Experiments - risk policy

<rp:risk-policy version="1.0" xmlns:rp="http://inf.ufsc.br/~danielrs">
  <rp:resource id="1"/><rp:user id="1"/>
  <rp:metric-set name="sharma2012">
    <rp:metric>
      <rp:name>Confidentiality</rp:name>
      <rp:quantification>https://localhost:8443/quantify-conf</rp:quantification>
    </rp:metric>
    <rp:metric>
      <rp:name>Availability</rp:name>
      <rp:quantification>https://localhost:8443/quantify-avail</rp:quantification>
    </rp:metric>
    <rp:metric>
      <rp:name>Integrity</rp:name>
      <rp:quantification>https://localhost:8443/quantify-int</rp:quantification>
    </rp:metric>
  </rp:metric-set>
  <rp:risk-threshold>1.5</rp:risk-threshold>
</rp:risk-policy>
Experiments

TABLE I. PERFORMANCE OF RISK POLICIES

<table>
<thead>
<tr>
<th>Policy</th>
<th>min. (ms)</th>
<th>max. (ms)</th>
<th>avg (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XACML</td>
<td>0.925</td>
<td>4.278</td>
<td>1.040</td>
</tr>
<tr>
<td>XACML+[34]</td>
<td>1.986</td>
<td>11.973</td>
<td>2.436</td>
</tr>
<tr>
<td>XACML+[33]</td>
<td>4.395</td>
<td>14.234</td>
<td>5.352</td>
</tr>
</tbody>
</table>

TABLE II. PERFORMANCE WITH A VARYING NUMBER OF METRICS

<table>
<thead>
<tr>
<th>Number of metrics</th>
<th>min. (ms)</th>
<th>max. (ms)</th>
<th>avg (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.832</td>
<td>12.130</td>
<td>2.243</td>
</tr>
<tr>
<td>10</td>
<td>2.612</td>
<td>12.876</td>
<td>3.171</td>
</tr>
<tr>
<td>100</td>
<td>10.922</td>
<td>60.442</td>
<td>14.030</td>
</tr>
<tr>
<td>1000</td>
<td>96.041</td>
<td>175.245</td>
<td>121.383</td>
</tr>
<tr>
<td>10000</td>
<td>1168.511</td>
<td>1517.364</td>
<td>1361.025</td>
</tr>
</tbody>
</table>

TABLE III. PERFORMANCE WITH LOCAL AND EXTERNAL METRICS

<table>
<thead>
<tr>
<th>Case</th>
<th>min. (ms)</th>
<th>max. (ms)</th>
<th>avg (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1.057</td>
<td>9.372</td>
<td>1.46</td>
</tr>
<tr>
<td>B</td>
<td>1.824</td>
<td>15.564</td>
<td>4.574</td>
</tr>
<tr>
<td>C</td>
<td>1556.182</td>
<td>2813.56</td>
<td>1726.71</td>
</tr>
<tr>
<td>D</td>
<td>3247.563</td>
<td>10350.5</td>
<td>4220.6</td>
</tr>
</tbody>
</table>
Experiments

Figure 4 shows the growth in time spent to reach an access decision as the number of metrics increase. The X axis is the number of metrics and the Y axis is the time spent in milliseconds. The solid line with square markers is for local metrics, the dashed line with circular markers is for remote metrics.}

Arias-Cabarcos et al. [36] describe current issues in FIM and the need for a risk-based access control model. The NSA RAdAC model is introduced in this paper. The paper presents a dynamic risk-based access control model for cloud computing, with an application to cloud e-health. The architecture is built as an XACML extension, which focuses on the application of a similar model to cloud computing, with an extension to the RBAC model to include risk analysis.

The model is implemented on top of RBAC, so it uses role delegation along with the risk analysis. Risk-based access control models are an alternative and, as the authors argue, more suitable for cloud computing, because these systems are dynamic and naturally federations. The architecture is based on: administrative capacity and costs, policy coverage, extensibility and performance. The coverage of policies and extensibility of administrative capacity and costs, only adding the need to manage risk policies. The performance of the system can be shown through the implementation of risk-based access control models presented in related work. The performance of the system was evaluated quantitatively and we can draw some conclusions from the experiments. It can be seen that using the risk-based model the system performs correctly and, therefore, its security. This is why there are no experiments related to the security of the system presented in this paper.

Risk-based access control models are an alternative and, as the authors argue, more suitable for cloud computing, because these systems are dynamic and naturally federations. The architecture is based on: administrative capacity and costs, policy coverage, extensibility and performance. The coverage of policies and extensibility of administrative capacity and costs, only adding the need to manage risk policies. The performance of the system can be shown through the implementation of risk-based access control models presented in related work. The performance of the system was evaluated quantitatively and we can draw some conclusions from the experiments. It can be seen that using the risk-based model the system performs correctly and, therefore, its security. This is why there are no experiments related to the security of the system presented in this paper.

This work is an improvement on our previous work [32], which focused on the application of a similar model to cloud computing. The model is implemented on top of RBAC, so it uses role delegation along with the risk analysis. Risk-based access control models are an alternative and, as the authors argue, more suitable for cloud computing, because these systems are dynamic and naturally federations. The architecture is built as an XACML extension, which focuses on the application of a similar model to cloud computing, with an extension to the RBAC model to include risk analysis.

Several works describe authentication and authorization in cloud computing. Britton and Brown [33] present a quantification method considering pre-federation and post-federation stages. There is no reference architecture that allows its extension. Despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation, despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation, despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation.

Hu et al. [35] recommend assessing an access control system based on: administrative capacity and costs, policy coverage, extensibility and performance. The coverage of policies and extensibility of administrative capacity and costs, only adding the need to manage risk policies. The performance of the system can be shown through the implementation of risk-based access control models presented in related work. The performance of the system was evaluated quantitatively and we can draw some conclusions from the experiments. It can be seen that using the risk-based model the system performs correctly and, therefore, its security. This is why there are no experiments related to the security of the system presented in this paper.

The authors argue that traditional access control models, currently implemented in most cloud solutions, are not enough to ensure the security of these environments when it is necessary to have a greater flexibility to enable efficient information sharing in critical environments. The development of access control systems for cloud computing is of great importance, because these systems are fundamental to enable the security of these environments.

Several works describe authentication and authorization in cloud computing. Britton and Brown [33] present a quantification method considering pre-federation and post-federation stages. There is no reference architecture that allows its extension. Despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation, despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation, despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation.

Hu et al. [35] recommend assessing an access control system based on: administrative capacity and costs, policy coverage, extensibility and performance. The coverage of policies and extensibility of administrative capacity and costs, only adding the need to manage risk policies. The performance of the system can be shown through the implementation of risk-based access control models presented in related work. The performance of the system was evaluated quantitatively and we can draw some conclusions from the experiments. It can be seen that using the risk-based model the system performs correctly and, therefore, its security. This is why there are no experiments related to the security of the system presented in this paper.

Risk-based access control models are an alternative and, as the authors argue, more suitable for cloud computing, because these systems are dynamic and naturally federations. The architecture is based on: administrative capacity and costs, policy coverage, extensibility and performance. The coverage of policies and extensibility of administrative capacity and costs, only adding the need to manage risk policies. The performance of the system can be shown through the implementation of risk-based access control models presented in related work. The performance of the system was evaluated quantitatively and we can draw some conclusions from the experiments. It can be seen that using the risk-based model the system performs correctly and, therefore, its security. This is why there are no experiments related to the security of the system presented in this paper.

Several works describe authentication and authorization in cloud computing. Britton and Brown [33] present a quantification method considering pre-federation and post-federation stages. There is no reference architecture that allows its extension. Despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation, despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation, despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation.

Hu et al. [35] recommend assessing an access control system based on: administrative capacity and costs, policy coverage, extensibility and performance. The coverage of policies and extensibility of administrative capacity and costs, only adding the need to manage risk policies. The performance of the system can be shown through the implementation of risk-based access control models presented in related work. The performance of the system was evaluated quantitatively and we can draw some conclusions from the experiments. It can be seen that using the risk-based model the system performs correctly and, therefore, its security. This is why there are no experiments related to the security of the system presented in this paper.

The authors argue that traditional access control models, currently implemented in most cloud solutions, are not enough to ensure the security of these environments when it is necessary to have a greater flexibility to enable efficient information sharing in critical environments. The development of access control systems for cloud computing is of great importance, because these systems are fundamental to enable the security of these environments.

Several works describe authentication and authorization in cloud computing. Britton and Brown [33] present a quantification method considering pre-federation and post-federation stages. There is no reference architecture that allows its extension. Despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation, despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation, despite the fact that there are proposals in the literature for its use in the cloud, they are very specific to a given situation.

Hu et al. [35] recommend assessing an access control system based on: administrative capacity and costs, policy coverage, extensibility and performance. The coverage of policies and extensibility of administrative capacity and costs, only adding the need to manage risk policies. The performance of the system can be shown through the implementation of risk-based access control models presented in related work. The performance of the system was evaluated quantitatively and we can draw some conclusions from the experiments. It can be seen that using the risk-based model the system performs correctly and, therefore, its security. This is why there are no experiments related to the security of the system presented in this paper.

Risk-based access control models are an alternative and, as the authors argue, more suitable for cloud computing, because these systems are dynamic and naturally federations. The architecture is based on: administrative capacity and costs, policy coverage, extensibility and performance. The coverage of policies and extensibility of administrative capacity and costs, only adding the need to manage risk policies. The performance of the system can be shown through the implementation of risk-based access control models presented in related work. The performance of the system was evaluated quantitatively and we can draw some conclusions from the experiments. It can be seen that using the risk-based model the system performs correctly and, therefore, its security. This is why there are no experiments related to the security of the system presented in this paper.

The authors argue that traditional access control models, currently implemented in most cloud solutions, are not enough to ensure the security of these environments when it is necessary to have a greater flexibility to enable efficient information sharing in critical environments. The development of access control systems for cloud computing is of great importance, because these systems are fundamental to enable the security of these environments. The authors argue that traditional access control models, currently implemented in most cloud solutions, are not enough to ensure the security of these environments when it is necessary to have a greater flexibility to enable efficient information sharing in critical environments. The development of access control systems for cloud computing is of great importance, because these systems are fundamental to enable the security of these environments.
Conclusion

• AC systems for the cloud are of great importance and traditional AC models are not enough for the cloud

• Risk-based AC tend to be very specific to a given scenario, we tried to make it more general, to be applied in a CSP

• We presented, implemented and evaluated the performance of our architecture

• As future work, we would like to: integrate the architecture into a mature cloud federation project; implement other risk quantification methods; improve the performance of external metrics (caching, concurrent requests, …); and develop a reference set of risk metrics for the cloud
References


RAClouds – Risk Analysis for Clouds
• Introduction

• Related Work

• Approach of the Proposed Solution
Introduction

• The safety evaluation of providers is a big challenge for CCs (CSA, 2011)

• Risk analysis includes (ISO 27005, 2011):
  – Identification of the need for controls
  – Evaluation of the efficiency of controls
• Risk Analysis can assist the CC
  – for the selection and maintenance of your CSP

• But consider:
  – Business requirements
  – Broad scope of risk
  – Regardless of CSP
Introduction

• The lack of these principles generates:
  – Disregard the requirements of the client's business
  – Limited selection of possible security requirements
  – Customer distrust regarding disclosure of risks encountered
Propose a computational model in which a *CC* (consumer cloud) can perform risk analysis in a *CSP* (Cloud Service Provider) so:

- Adherent (needs CC);
- Comprehensive (proper scope);
- Independent (relative to CSP)
Related Work

- **Dey (2013):** integration with mobile devices;
- **Zhou (2013):** performance testing;
- **Kolluru (2013):** Client connection to the cloud;
- **Lor (2012):** applications in federations of clouds;
Related Work

• **Grobauer (2012):** Mapping specific vulnerabilities of cloud computing;

• **Rot (2013):** Study of threats in the cloud;

• **Luna (2012):** SLAs for cloud security;

• **Bleichertz (2013):** assessment by the CC;

• **Grezele (2013):** risks related to cloud database;
Related Work

• Ristov (2012): Risk analysis based on ISO 27001;
• Ristov (2013): Risk Analysis for OpenStack, Eucalyptus, OpenNebula and CloudStack environment;
• Mirkovié (2013): ISO 27001 controls the cloud;
• Bhensook (2012) and Ullah (2013):
  – Effort CSA for safety assessment
  – CloudAudit model
  – Based on ISO 27001
• Hale (2012): SecAgreement for monitoring security metrics;
• Zech (2012): Risk analysis of external interfaces;
• Wang (2012): analysis of risk based CVE;
• Khosravani (2013): a case study of the requirements of CC;
• Lenkala (2013): metrics for risk analysis in the cloud;
• Liu (2013): Risk assessment in virtual machines;
Proposed Solution
Proposed Solution

- **Agent ISL:**
  - Definition of threats and vulnerabilities
  - Risk describes a descriptor using RDL - *Risk Definition Language*
  - Specifies the form of risk assessment through a WSRA - *Risk Analyser WebService*
  - RDLs and provides WSRAs for RACloud
Proposed Solution

• **Agent CC:**
  – Definition of information assets
  – Complements the RDL with the impact of information
  – Provides extension to the RDL RACloud
  – Start the assessment and receive results
• CSP Agent:
  – Imports RDLs RACloud
  – Implements calls to WSRAs
  – Make the Call of risk assessments of ISLs
## Proposed Solution

<table>
<thead>
<tr>
<th>Simbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_x$</td>
<td>Treat defined by ISL “x”</td>
</tr>
<tr>
<td>$A_y$</td>
<td>Information Asset defined by CC “y”</td>
</tr>
<tr>
<td>$V_z$</td>
<td>Vulnerability defined by ISL “z”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Simbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$eaf(T_x,w)$</td>
<td>Exposure analysis function of $T_x$ on CSP “w”</td>
</tr>
<tr>
<td>$iaf(A_y)$</td>
<td>Impacto analysis function of $A_y$</td>
</tr>
<tr>
<td>$daf(V_z,w)$</td>
<td>Deficiency analysis function of $V_z$ on CSP “w”</td>
</tr>
<tr>
<td>Simbol</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>$DE_{T,x,w}$</td>
<td>Degree of Exposure related with $T_x$ and $w$. $eaf(T_x,w)=DE_{T,x,w}$</td>
</tr>
<tr>
<td>$DI_{A,y}$</td>
<td>Degree of Impact related with $A_y$. $iaf(A_y)=DI_{A,y}$</td>
</tr>
<tr>
<td>$DD_{V,z,w}$</td>
<td>Degree of Deficiency related with $V_z$ and $w$. $daf(V_z,w)=DD_{V,z,w}$</td>
</tr>
<tr>
<td>Simbol</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td>$E_{T,V}$</td>
<td>Event relating $T$ with $V$</td>
</tr>
<tr>
<td>$\alpha(T_x,V_z)$</td>
<td>Function correlating $T$ and $V$</td>
</tr>
<tr>
<td></td>
<td>$\alpha(T_x,V_z)=E_{T,V}$</td>
</tr>
<tr>
<td>$fp(E_{T,V})$</td>
<td>Function of probability of $E_{T,V}$</td>
</tr>
<tr>
<td></td>
<td>$fp(E)=(DE_{T,x,w}+DD_{V,z,w})/2$, or,</td>
</tr>
<tr>
<td></td>
<td>$fp(E)=\text{matrix}(DE_{T,x,w},DD_{V,z,w})$</td>
</tr>
<tr>
<td>$P_E$</td>
<td>Probability of $E_{T,V}$</td>
</tr>
<tr>
<td></td>
<td>$fp(E_{T,V})=P_E$</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>$R_{E,A}$</td>
<td>Risk relating E and A</td>
</tr>
<tr>
<td>$\beta(E,A_y)$</td>
<td>Function correlating E and $A_y$  \ $\beta(E,A_y)=R_{E,A}$</td>
</tr>
<tr>
<td>$raf(R_{E,A})$</td>
<td>Risk analysis function of $R_{E,A}$  \ $raf(R_{E,A})=(P_E + DIA_y)/2$  \ ou  \ $raf(R_{E,A})=matriz(P_E,DIA_y)$</td>
</tr>
<tr>
<td>$DRIE,A$</td>
<td>Degree of risk related with $R_{E,A}$  \ $raf(R_{E,A})=GR_{E,A}$</td>
</tr>
</tbody>
</table>
Proposed Solution

• Model is organized into:

  – **Specification phase**: environmental risk analysis is configured;

  – **Evaluation Phase**: risk analysis is performed;
Proposed Solution

• Component Specification:
  – *Registry Manager*: Records CC, CSP and ISL manager;
  – *RDL Manager*: descriptors of risk (threat + vulnerability) manager;
  – *RDL Manager Extensions*: Extensions RDL (information assets) manager;
Proposed Solution
Proposed Solution

- **Components of Evaluation:**
  - *Risk Analysis*: Does the coordination between other internal components;
  - *RA Processor*: establishes relationships and makes the calculation of risk;
  - *Impacts Evaluation*: assessing the impact on CC;
  - *CSP Proxy*: call for testing the ISL;
  - *WSRA Evaluation*: evaluation of safety requirements;
Proposed Solution
Proposed Solution
• Multiple ISLs can act in defining RDLs and WSRAs (coverage)

• The related works do not meet these characteristics

• Are usually focused on specific evaluations by PHC itself, without considering the CC
Discussion
Discussion


