**Cloud Application Secured Design**

*A TOPIC PAPER*

*SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF GRADE IN*

**SECURE SOFTWARE DESIGN AND PROGRAMMING**

IN

**COMPUTER SCIENCE**

BY

**Harsh Loomba** (G00905405)



**DEPARTMENT OF COMPUTER SCIENCE**

**GEORGE MASON UNIVERSITY**

**FAIRFAX, VIRGINIA**

**CONTENTS**

|  |  |  |
| --- | --- | --- |
|  | **Topic** | **Page #** |
| **1** | **Introduction** | 3 |
|  | **1.1. Cloud Computing And Essential Features** | 3 |
|  | **1.2. Cloud Service Model** | 4 |
|  | **1.3. Cloud Deployment Model** | 5 |
| **2** | **Security Concerns In Cloud** | 7 |
|  | **2.1. Vulnerability In Cloud** | 7 |
|  | **2.2 Combat The Security Challenges** | 8 |
|  | **2.3. Security Solution Features** | 8 |
| **3** | **Intel's Proposition of Cloud Security** | 10 |
|  | **3.1. Provisioning Module** | 10 |
|  | **3.2. Intel IAM Federation/SSO Module** | 11 |
|  | **3.3 OTP Module** | 11 |
|  | **3.4 Software Service Token Module** | 12 |
|  | **3.5 Compliance Module** | 12 |
| **4** | **References** | 13 |

1. **Introduction**

This paper introduces Intel’s proposition for secured cloud enterprise applications. The solution is primarily based on three essential features – user automatic account provisioning/de-provisioning, cloud federation/SSO and strong multi factor and context based authentication.

* 1. **Cloud Computing And Essential Features**

According to AT&T, cloud is a location independent online utility service which is available on-Demand. Cloud computing is internet based computing where shared resources, software and information are available to anyone from any location based on the security designed on the cloud. It promises not just cost efficiency but also faster, easier and more flexible infrastructure for businesses. Cloud computing is not immune to risks and ethical objections, but the fact is that it promises great advantages which attract businesses of different size.

Figure 1: Cloud Computing Characteristics

Figure 2: Key Driver of Cloud adoption

* 1. **Cloud Service model**

Cloud providers offer three service models, information is partially fetched from [**David A. Wheeler\_2014**], as mentioned below:

1. Software as a service (SaaS)

* Application offered as a service on demand.
* Single instance runs on the cloud and serves multiple users.
* Accessible from various client devices: thin client interface (web browser) or program interface. User doesn’t need to manage or control underlying infrastructure.

1. Platform as a service (PaaS)

* Provides a platform by integrating an operating system, middleware, application software and development environment.
* User gets the capability to deploy onto the cloud consumer created or acquired application using tools supported by the provider.
* User does not manage or control underlying infrastructure but has control over the deployed application and configuration settings in hosting environment.

1. Infrastructure as a service (IaaS)

* Delivers basic storage and computing capabilities as a service over the network.
* Computing components are pooled and made available to handle workloads.
* User does not manage or control underlying infrastructure but has control over OS, storage and deployed applications.

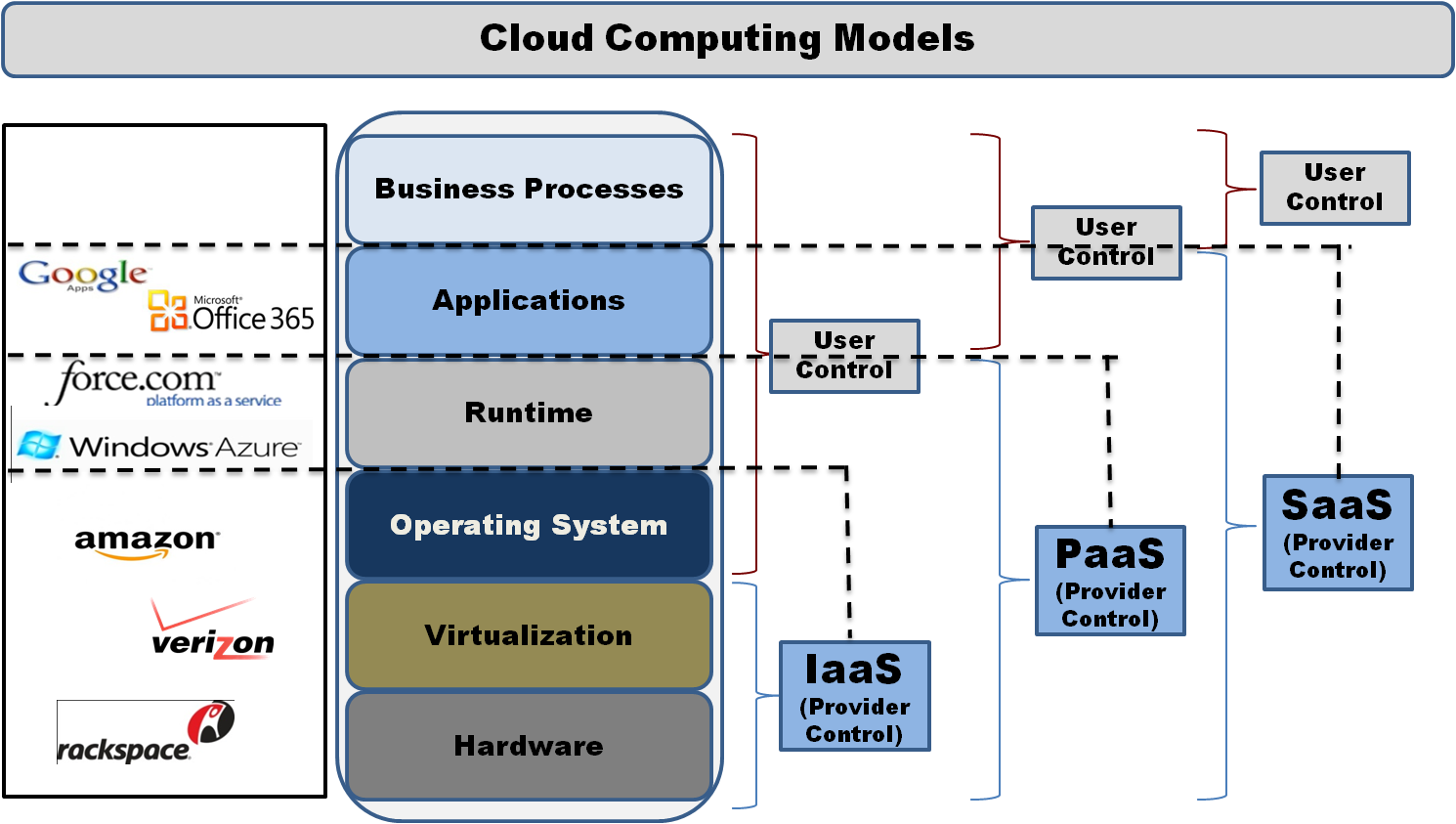


Figure 3: Cloud Computing Model

* 1. **Cloud Deployment Model**

Underlying diagram shows cloud deployment models

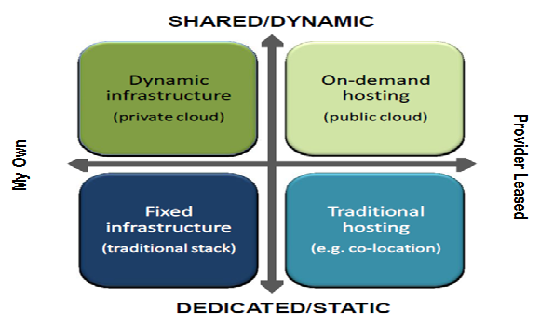


Figure 4: Deployment Models

1. **Private Cloud: Low security risk**

* Enterprise owned
* Functionalities not exposed to users

1. **Public Cloud: More security risk**

* Cloud providers
* Functionalities may vary

1. **Hybrid Cloud: High security risk**

* Mix of private and public cloud
* High customization

1. **Security Concerns In Cloud**

According to Gartner, cloud computing has “unique attributes” that requires risk assessment in areas such as Data security, application and data compliances, application portability, multi-vendor process management, cloud lifecycle management, less maturity of virtualization within the environment, organization visibility and control over cloud infrastructure.

* 1. **Vulnerability in cloud**

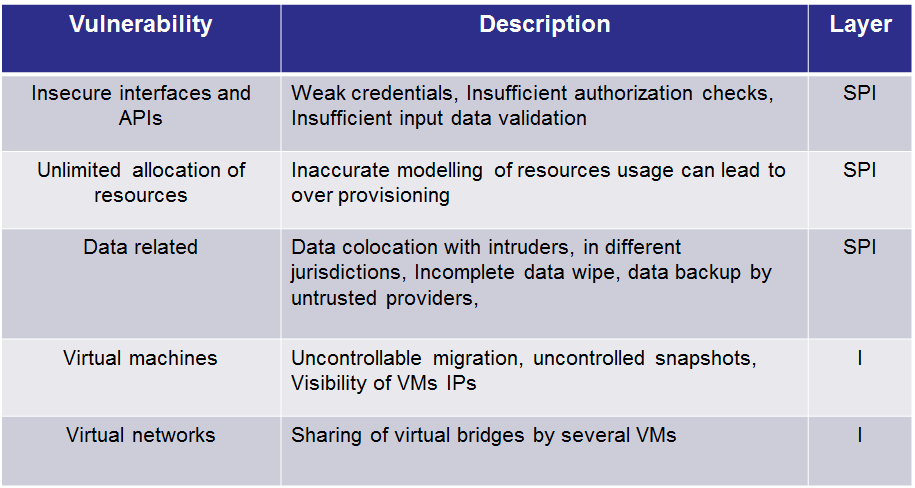
****

Figure 5: Vulnerabilities in Cloud

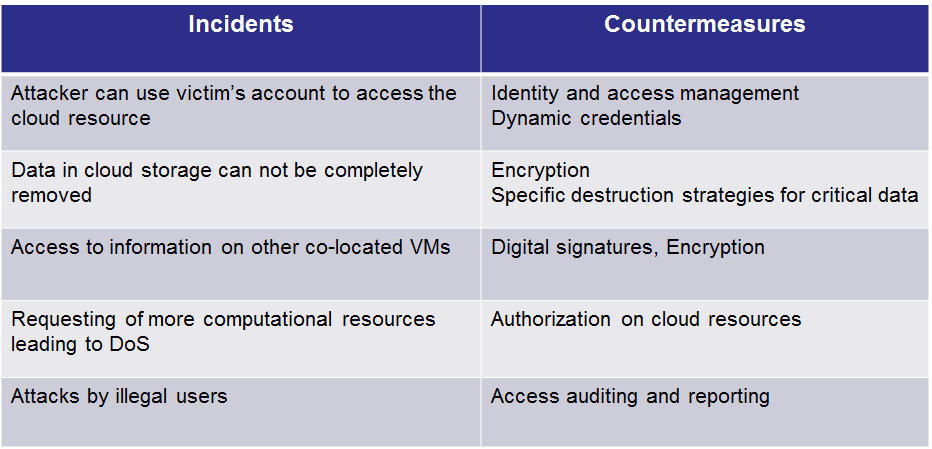


Figure 6: Incidents and Countermeasures

* 1. **Combat the security Challenges**

Following are the security challenges for the cloud applications, fetched information from [**Intel\_Cloud\_Builders\_McAfee\_March\_2012**]

1. Multiple logins/weak security

* Users have different credentials for each cloud application, stored natively in those applications.
* Users tend to create weak passwords when there are too many passwords to remember.
* This compromises the security when application is accessible from outside the firewall.

1. Manual Provisioning

* User access is not automatically provisioned/de-provisioned with cloud applications.
* User access remains even after the user is no longer with the organization.
* This increases the cost of administering users due to lack of automated processes.

1. Lack of visibility

* There is no centralized view of ‘who has access to what’ when users access cloud.
* This results in SaaS users lacking oversight or authorization leading to sensitive data leakage and compliance risks.
* The traditional solutions have to retrieve access logs from each cloud apps and have them consolidated and correlated for visibility.

1. Single factor authorization

* In case of on premise applications, a single factor authentication may be sufficient.
* Stronger authentication is required for critical applications in cloud so as to have a higher confidence in identity proofing and user validation
  1. **Security Solution Feature**

1. Control

* Manages the identity lifecycle with policy driven automatic account provisioning/de-provisioning to cloud apps.
* Minimizes the risk of unauthorized access by enforcing user identity and context based authorization, eliminating passwords through federation trust.

1. Visibility

* Centralized management and reporting of user access. Monitors users, administrators and API access activity.

1. Strong authentication

* Built in OTP solution for multi-factor authentication.

1. Compliance

* Maintains audit records of identity life-cycle events and correlates a user’s cloud activities with on premise logs for compliance.
* Detecting and deleting orphan account.

1. Connector

* In built identity and cloud connector with a choice of authentication source (LDAP, RDBMS, SAML, Social network, etc.).
* Cloud connectors to allow federated SSO and integration with IDM systems with support of standards like SAML, OAuth and OpenID.

1. **Intel’s Proposition Of Cloud Security**

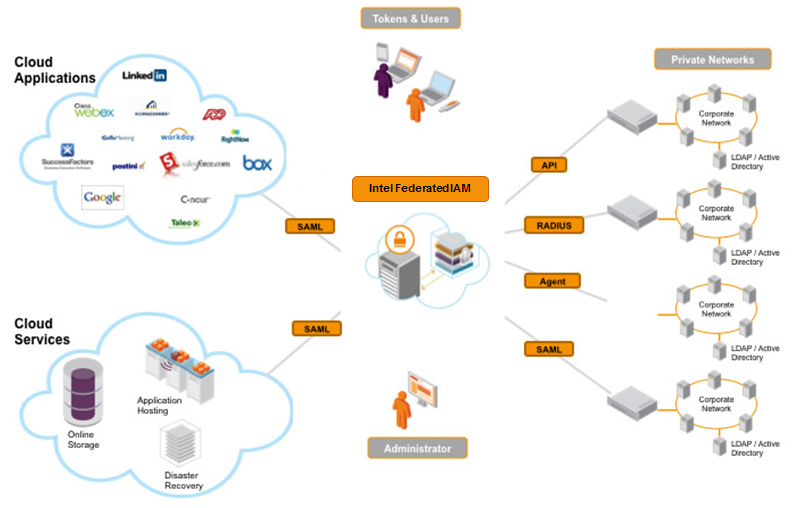
Solution combining user account provisioning, cloud federation/SSO and strong multi factor and context based authentication. 

Figure 7: Identity Access Management Solution

The above figure depicts the centralized identity access management system which manages the security throughout the enterprise. Intel’s Proposition security design system consists of 5 modules, information has been fetched from [**Intel\_Cloud\_Builders\_McAfee\_March\_2012**]

**3.1. Provisioning Module**

This module has functions for distribution, synchronization, compilation, and follow-up of identity and attributes information. Two-way provisioning is also supported, which means that connected systems can be both source and receiver of identity and attribute information. The product is a policy-based service that can flexibly leverage the rules and policies decided on within a company regarding the handling of identity and attribute information to a set of automated actions. It can communicate by web service or directly with all modern databases or LDAP.

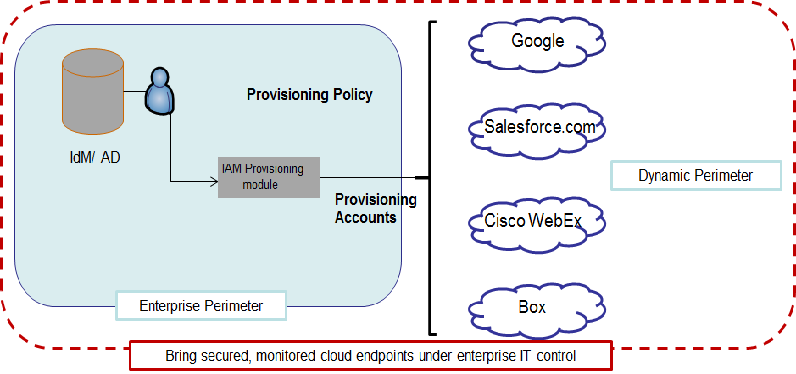


Figure 8: IAM provisioning Module

**3.2. Intel IAM Federation/ SSO Module**

This module (information is drawn from [**federated-identity-mgr\_2014**]) provides seamless single sign-on for enterprise users to cloud applications. It provides Connectors which connects IAM system to common identity sources (Active directory, LDAP, databases, Facebook, Google) and to popular SaaS, PaaS platforms are included in the package. Federated authorization and authentication protocols are based on Security Assertion Markup Language (SAML 2.0), XACML and OPENID that can connect intern identity providers with corporate identities and authorization policy. Risk based access is the additional feature which makes the authentication system more robust. Using static or contextual information, the risk assessment determines whether a user’s request to access information should be permitted, denied or permitted with some further authentication.

Additional Functionalities of SSO module to safeguard the IAM system

1. Identity Connector – Ability to connect to authentication sources such as LDAP, JDBC database, AD, OpenID, social network, SAML, X.509, OTP. Subsequently, retrieve user identity from IDP (identification provider) and pass it onto cloud services for maintaining SSO functionality.
2. Cloud Connector – Connector (such as SAML, Proprietary SaaS connector, Token based) to enable trusted federation with SaaS.
3. Application adapter – Used in service provider mode. Internal apps can be integrated for SSO by token approach.
4. Cloud Authenticator – Users choose the IDP they want to authenticate with for accessing the application.

**3.3. OTP Module**

Leverage existing enterprise identity repository for two-factor authentication. Due to the presence of OTP, security policy is dynamically enforced on factors: Geo-location, IP address, etc.

**3.4. Software service token module (STS)**

It’s the identity mediation service for establishing trust and facilitating compliance by managing identities. It validates and issues a variety of identity formats between applications and services and ties together applications running on disparate sources.

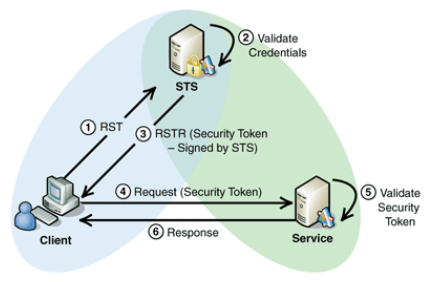


Figure 9: STS Module

**STS module Use Case**:

* Client sends an authentication request with accompanying credentials to STS.
* STS verifies and issues a security token to assert client’s authentication with STS.
* Client sends the token to the web service/SaaS application.
* SaaS verifies the token and authenticates the client into cloud.

**3.5. Compliance Module**

Establish better control of user’s access by understanding who users are, and their roles and responsibilities. It ensures authorized access to applications and define processes for review, approval, exception and remediation.

**4. References**

[Intel\_Cloud\_Builders\_McAfee\_March\_2012] <http://www.intelcloudbuilders.com/docs/Intel_Cloud_Builders_McAfee_March_2012.pdf>

[federated-identity-mgr\_2014] <http://www.emc.com/collateral/data-sheet/h9040-federated-identity-manager-ds.pdf>

[David A. Wheeler\_2014] http://www.dwheeler.com/essays/cloud-security-virtualization-containers.html