

## Security & Cloud

### Oya Şanlı

paydeg@paydeg.com

How to tackle Security in the Cloud? We would like to begin with asking some questions like; what is Cloud computing?

Cloud Computing is a strategic approach that creates business value by changing the way of IT is produced and consumed.

Why is security tough?

Today, all users, business or home users want to access to their data anywhere from any device. Variation of devices also makes security tough to reach. Economy has also some affect, since we let employees to bring own device.

Where is the best place for my data? To answer this question we need to do some evaluations, and find some answer more questions like; is my notebook or are servers in my IT room safer? How much safer?

Is Cloud more or less secure then the traditional environment? Let's take a look at first our approach to security:

- People, hiring people for security
- Process, security should be in the initial design not afterthought, and via external auditing must be strengthen.
- Technology, using secure hardware and software

### Summary

What is Cloud computing? Who has control over what? What are the benefits? What are the potential issues? Why security is needed? What are the security principles? Why is security tough? What are the advantages and challenges of cloud computing in terms of security? Where is the best place for my data? Cloud security scenarios. What we may learn from scenarios?

This document tries to answer these questions while giving some real life examples. These examples may give the idea of our perspective of security and how can we deal with security in the cloud.

This document also tries to compare security issues in the cloud and via some scenarios it also tries to give information how to prevent them.

Too often—and for too many organizations— diminished budgets have resulted in degraded security programs. Risks are neither well understood nor properly addressed. The number of security incidents is on the rise.

To be effective, security must be integral to the way people think and work, not merely an afterthought or another item to be checked off a list.

**Keywords:** Cloud Computing, Security, Security in the Cloud, Time Sharing, Multi-tenancy, Responsibility split, E-commerce, PCI in the Cloud

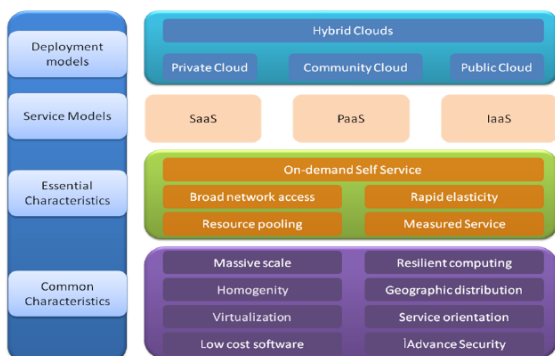
### Introduction

The idea of cloud computing is evolved out of;

- time sharing vision
- progresses faced from distributed computing through networking

- improvement online services

Cloud Computing is a strategic approach that creates business value by changing the way of IT is produced and consumed. Cloud computing is a movement that changes the business of IT.



### Definition of Cloud Computing

Cloud computing is a model for enabling 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 (NIST definition). This model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. Clouds are massively complex systems can be reduced to simple primitives that are replicated thousands of times and common functional units.

We think additionally there are 3 major points to that interest on Cloud Computing.

First, Decrease on the cost of hardware and increase on the storage capacity.

Second; exponentially growing size of the data. Especially in science, internet publishing and archiving the size of the data is growing exponentially.

And the third; well assimilation of web 2.0 applications and IT services- like FaceBook, Twitter and Google Plus usage.

Actually cloud computing is not a new technology not a new methodology neither a new infrastructure but it is a new way of delivering and using technologies and we are already using it for years with Hotmail, gmail and yahoo mail.

Basically, accessing low cost applications over internet and mutual commerce over internet forms the cloud computing environment.

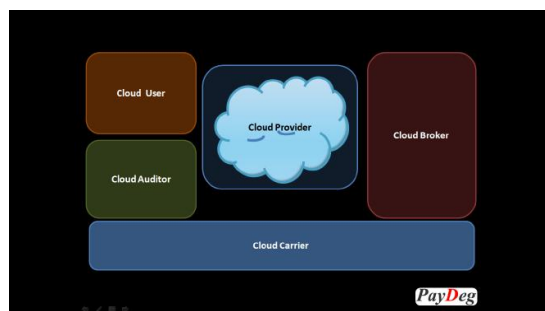
The prospect of a virtually unlimited capacity with little or minimal fees, limited obligations, increased flexibility, and agility is a dream come true.

Never forget; to be considered "cloud" they must be deployed on top of cloud infrastructure that has the essential characteristics

### Who Has Control Over What?

Before answering this question, we believe we should mention about roles in the Cloud.

There are three main roles: Cloud Service Consumer, Cloud Service Provider and Cloud Service Creator. Each role can be fulfilled by a single person or can be fulfilled by a group of people or an organization or a firm.



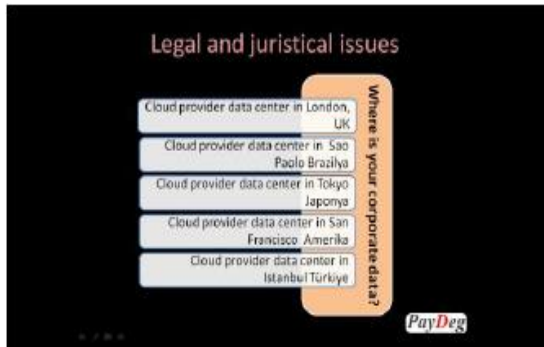
A cloud service consumer is an organization, a human being or an IT system that consumes (i.e., requests, uses and manages, e.g. changes quotas for users, changes CPU capacity assigned to a VM, increases maximum number of seats for a web conferencing cloud service) service instances delivered by a particular cloud service. The service consumer may be billed for all (or a subset of) its interactions with cloud service and the provisioned service instance(s).

The Cloud Service Provider has the responsibility of providing cloud services to Cloud Service Consumers. People acting in the role of a Cloud Service Provider and a Cloud Service Consumer at the same time would be a partner of another cloud service provider reselling cloud services or consuming cloud services and adding value add functionality on top, which would in turn be provided as a cloud service.

Although defined as a separate role, it would also be possible that a Cloud Service Provider has Cloud Service Brokers in the same organization, i.e. it is not necessary that Cloud Service Provider and Cloud Service Broker are in separate organizations.

The Cloud Service Broker is responsible for gathering cloud services, which can be run by different Cloud Service Providers and by that exposed to Cloud Service Consumers. Typically, Cloud Service Creators build their cloud services by leveraging functionality which is exposed by a Cloud Service Providers. Auditor who is independently evaluating the security and performance of cloud services.(i.e CSA-Cloud Security Alliance).

Cloud Carrier who is providing the connectivity between cloud services and cloud users.



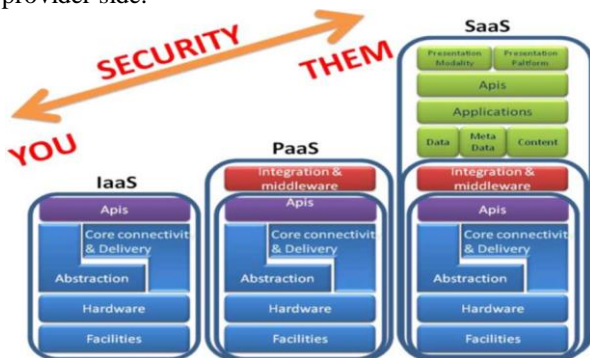
What is different about the cloud? Your data can be anywhere on the earth, jurisdictional issues will definitely complicate your road. Specifically, think about locations where certain security safeguards are illegal due to privacy constraints. Laws may cause security breaches.

Let's take a look at who has the control over security. Towards SaaS security concerns pass to provider. For IaaS though we may talk about three different services. If the infrastructure is in our IT room and if we are running the cloud then we have to deal with all security issues.

If our infrastructure is collocated, meaning third party is maintaining and running for us then we share the issues with the third party.

If we get an IaaS service from public provider then again we share the responsibility with the provider.

If we get SaaS service most of the responsibility is at provider side.



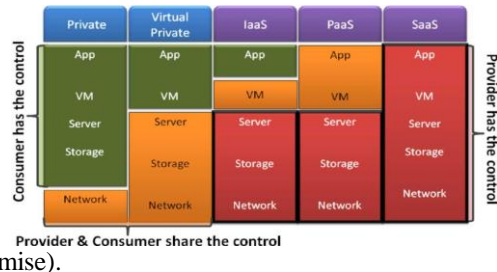
Take a look at the figure below, first three column can be considered as IaaS service model where provider provision processing, storage, networks, and other **If we do have some ideas about Cloud**

Computing benefits then we believe that we can make it more secure. Immediate benefits we face first in IT with reduce in cost. Well how this is happening?

It is happening with the billing model which is pay as per usage and non purchased infrastructure and low maintenance since no need to purchase the infrastructure.

In Efficiency.. It gives us energy efficiency in terms of cost savings as well as environmental responsibility.

fundamental computing resources to the consumer who is able to deploy and run arbitrary software, which can include operating systems and applications. At first column when the private cloud infrastructure is in our IT room (on premise), at second column when we rent the infrastructure from the provider and the infrastructure is only in our use (on premise hosted), at third column when we share the infrastructure of the public service provider (off

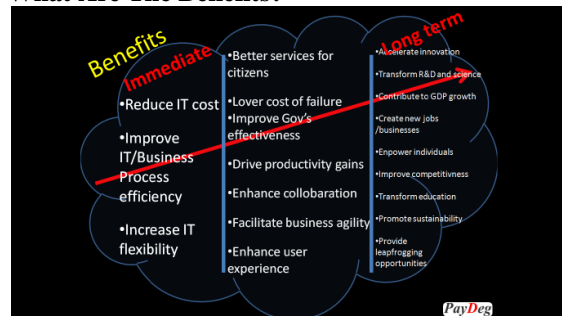


The green boxes shows that the control is at the consumer, orange boxes shows that control is shared and the red boxes shows that control is at the provider. Knowing who has over what control of the service is important in terms of be careful handling IT in the business world.

With PaaS the programming languages and tools are offered to consumers. Consumer can develop own applications and shares control over the virtual machines and applications. Provider has the control over the network, storage and servers.

Well for SaaS provider has the whole control. Consumer only has control over some configurations in the provided application

### What Are The Benefits?



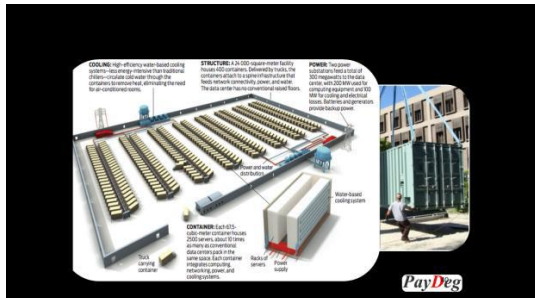
In terms of the operational efficiencies it accelerates the movement of IT service delivery closer to the efficiency and agility goals.

Cloud computing is an emerging technology that is revolutionizing IT infrastructures and flexibility, and software as a service (SaaS).

Cloud computing speed ups development and testing cycles, improves the quality of the application. Increase flexibility in IT by transforming computers from something that we buy and operate ourselves to

something that is operated by a third party.

During this economic time of recession, there are huge cost-reduction pressures and cloud computing allows businesses to do just that by tapping into cloud computing platforms on a pay-as-you-go basis.



Systems die? Move the container. We may recover a system today in under 30 minutes.. Virtualization gives that flexibility and to test new versions (or even different versions) of any operating system as installed into the "virtual" environment.

And Service Oriented Architecture enables innovation through collaboration and flexibility.

At next stage we would face with enhance collaboration and user experience; facilitate business agility and better services for citizens. We believe we all together in the world heading to this stage now.

Cloud computing will lead to increase in the standardization, scalability and usability wherever it's been used.

As long term we see promoting sustainability, transforming education to empower individuals and accelerate innovation as benefits of cloud computing.

### What Are The Potential Issues?

Most of the documents we read about security in the Cloud three main issues were mentioning;

- Data residency - time delay between data being requested and delivered
- Security and confidentiality of data being stored outside the company
- Business buy-in; convincing companies of the infrastructure and reliability

We think, since laws differ from country to country and an agreement is signed for service, we should also consider laws for data residency and security.

Cloud Computing providers are not inherently insecure. Depending on the security posture of a particular organization, you might even find that some Cloud providers may have superior security postures to that of your own organization.

### Why Security Is Needed?

The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Protecting IT systems can be as important as protecting other organizational resources, such as money, physical assets, or employees.

In a private-sector business, having good security is usually secondary to the need to make a profit. Security, then, ought to increase the firm's ability to make a profit. In a public-sector, security is usually secondary to the sector's providing services to citizens. Security, then, ought to help improve the service provided to the citizen.

Let's take a closer look at principles.

### What Are The Security Principles?

Many approaches and methods can be used to secure IT systems. The principles are to be used when developing computer security programs and policy and when creating new systems, practices or policies. We think it is important to mention about general security principles first.

There are two main drivers of security;

- Risk; risk of loss is the business driver for security. There is a need to perform risk assessments to understand own exposure to risk of loss.
- CIA; Confidentiality, integrity and availability are the prime objectives for what security measures aim to achieve.
  - o Confidentiality; data is only shared to and between authorized actors.
  - o Integrity; data can be assured to be authentic, trustworthy and complete. Integrity is a concept of consistency of actions, values, methods, measures, principles, expectations, and outcomes.
  - o Availability; access for delivering, storing and processing data when required. Availability is the degree to which data is in a specified operable and committable state at the start of a mission, when the mission is called for at an unknown, i.e., a random, time.

Here are OECD's guidelines for the security of Information Systems; they are also valid for Cloud Computing:

- Accountability - The responsibilities and accountability of owners, providers and users of information systems and other parties- should be explicit.
- Awareness - Owners, providers, users

and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures- for the security of information systems.

- Ethics - The Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interest of others are respected.

- Multidisciplinary - Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints.....

- Proportionality - Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm.

- Integration - Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.

- Timeliness - Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.

- Reassessment - The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

- Democracy - The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society. The OECD Guidelines were developed in 1992 by a group of international experts to provide a foundation from which governments and the private sector, acting singly and in concert, could construct a framework for securing IT systems.

For Cloud we can add;

- Openness: Openness is of primary importance in an enterprise environment. This includes support for all major platforms, runtimes, languages, support for major industry standards, published interfaces and algorithms, no security by obscurity, documented trust and threat models, and support for Common Criteria, and similar formal security validation programs.

- Design for privacy: In the current age of data sharing, privacy becomes increasingly more important. Solutions should highlight the use of private information and corresponding data protection mechanisms, and enable the principles of notice, choice, and access.

- Policy-based access to services: Service consumption will be controlled by policy.

Policies will be held externally from applications.

- Multi-tenancy: A Cloud Computing model must support isolation among multiple tenants of the Cloud.

According to NIST, all of the 33 IT security principles are grouped into the following 6 categories: Security Foundation, Risk Based, Ease of Use, Increase Resilience, Reduce Vulnerabilities, and Design with Network in Mind.

However, including security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed. Ultimately, organization managers have to decide what level of risk they are willing to accept, taking into account the cost of security controls.

Keep in mind while planning about security there are five phases which are:

- Initiation Phase - the need for a system is expressed and the purpose of the system is documented.

- Development/Acquisition Phase - the system is designed, purchased, programmed, developed, or otherwise constructed. Activities include determining security requirements, incorporating security requirements into specifications, and obtaining the system.

- Implementation Phase - the system is tested and installed or fielded. Activities include installing/turning on controls, security testing, certification, and accreditation.

- Operation/Maintenance Phase - the system performs its work. Activities include security operations and administration, operational assurance, and audits and monitoring.

- Disposal Phase - IT system life-cycle involves the disposition of information, hardware, and software. Activities include moving, archiving, discarding or destroying information and sanitizing the media. Security must be incorporated and addressed from the initial planning and design phases to disposal of the system.

Many important issues in computer security involve users, designers, implementers, and managers. A broad range of security issues relate to how these individuals interact with computers and the access and authorities they need to do their job. No IT system can be secured without properly addressing these security issues.

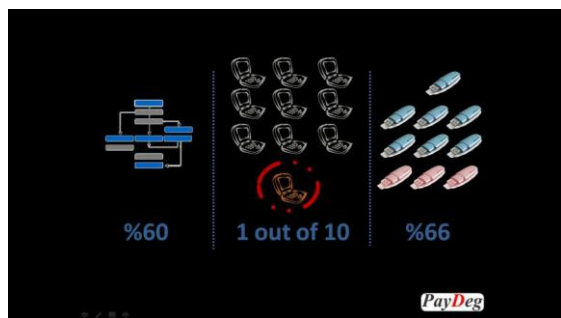
- Staffing
- Position definition
- Position sensitivity
- Screening
- Employee training and awareness
- User administration

- Account management
- Audit & Management reviews
- Detecting unauthorized/illegal activities
- Termination

It is critical to back up software and data. Frequency of backups will depend upon how often data changes and how important those changes are. Backup copies should be tested to ensure they are usable. Backups should be stored securely.

### Why Is Security Tough?

Nowadays, users want to access their data anywhere from any device. So users' credentials are on any device. As you may see from the slide majority of the security risk comes from inside. 60% of data may reside on unsecure desktops or laptops or usb's. According to FBI at US 1 out of 10 laptops is stolen within 12 months of purchase. Please don't forget Cloud cannot prevent malicious insider.



Computers and the environments in which they operate are dynamic. System technology and users, data and information in the systems, risks associated with the system, and security requirements are ever-changing. Changes in the system or the environment can create new vulnerabilities. These issues make it necessary to reassess periodically the security of IT systems.

Managers need to understand both their organizational mission and how each information system supports that mission. After a system's role has been defined, the security requirements implicit in that role can be defined. Security can then be explicitly stated in terms of the organization's mission.

Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending upon the particular IT system.

Without proper training on how and when to use security controls such as virus-detection package, the user may apply the package incorrectly and, therefore, ineffectively. As a result, the user may mistakenly

believe that if their system has been checked once, that it will always be virus-free and may inadvertently spread a virus. Therefore, proper training and awareness of parties is a must.

File permissions are always tricky, also in Cloud, and most users are not even aware of how to set them. So everyone can read the documents which are supposed to be confidential.

Another main issue is patching problem. Having multiple operating systems with different versions or different applications with different security patches within company causes losing time and money.

If one forgets to apply a patch causes security breach which also refers to lose data, therefore again lose time and money.

Old pcs and servers usually are kept around IT room for test purposes or they are running some software package that is impossible to migrate to another machine. These machines no longer getting patches or their old operating systems often come with inherent security holes that no patching can fix.

Still we occasionally end up with users being granted local admin rights inappropriately. This often happens while troubleshooting a problem. After making the user local admin to see if problem fixed, usually to take back privilege is forgotten.

VPN may also cause risks.. For a power user it is not so hard to set up VPN access on their machine. Problems with the unauthorized machine can easily spread over the VPN. Certain mistakes are made in programming, like SQL injection and cross-site scripting vulnerabilities. For example, WordPress Eco-Annu third party plug-in suffers from a remote SQL injection vulnerability. Since it is hard to change software once it has been installed, there is a need to keep them up to date.

In some cases misusing technology in the cloud causes security risks too.

When an organization's information and IT systems are linked with external systems, management's responsibilities extend beyond the organization. Security is constrained by societal factors; security measures should be selected and implemented with recognition of the rights and legitimate interests of others. This may involve balancing the security needs of information owners and users with societal goals. Economy has also some affect, since we let employees to bring own device. When employees leave their user credentials go with the device. And forgetting to remove user access from servers causes some security breaches.

Physical environment security like fire safety factors, plumbing leaks, physical access control and mobile and portable systems should be well thought.

Documentation should never be left out. Security documentation should be designed to fulfill the needs of the different types of people who use it. The security of a system also needs to be documented, including security plans, contingency plans, and security policies and procedures.

### What Are The Advantages And Challenges Of Cloud Computing In Terms Of Security?

Cloud computing is replacing large corporate data centers and unnecessary, expensive private server infrastructure.

Firms' and governments' users are adopting cloud computing because it eliminates capital investment in hardware and facilities as well as reduces operations labor.

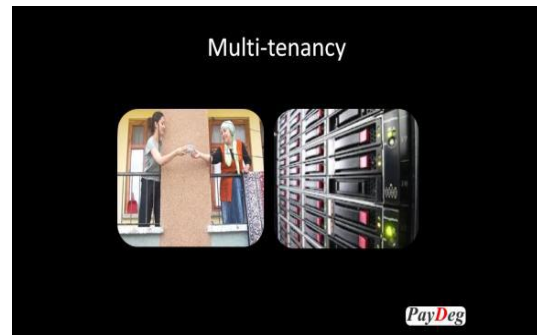
Let's take a look at the advantages Cloud Computing may bring in terms of security;

- Shifting public data to a external cloud reduces the exposure of the internal sensitive data
- Hypervisor Protection Against Network Attacks
- Fault Tolerance and Reliability
- Dedicated Security Team
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Greater Resiliency
- Data Fragmentation and Dispersal
- Redundancy / Disaster Recovery - Greater Investment in Security Infrastructure
- On-Demand Security Controls
- Simplification of Compliance Analysis Low-Cost Disaster Recovery and Data Storage Solutions
- Real-Time Detection of System Tampering
- Rapid Re-Constitution of Services

### How about security challenges?

- Trusting vendor's security model and vendor lock-in
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can't be examined
- Loss of physical control – loss off governance
- Logging challenges
- Data dispersal and international privacy laws
  - EU Data Protection Directive and U.S. Safe Harbor program
  - Exposure of data to foreign government and data subpoenas
  - Data retention issues

- Multi-tenancy - Need for isolation management



- Data ownership issues
  - Dependence on secure hypervisors
  - Security of virtual OSs in the cloud
  - Possibility for massive outages
  - Encryption needs for cloud computing
    - Encrypting access to the cloud resource control interface
    - Encrypting administrative access to OS instances
    - Laws about encryption keys
  - Public cloud vs internal cloud security
  - Lack of public SaaS version control
- Before going further we need to take a look at security relevant cloud components;
- Cloud Provisioning Services
  - Cloud Data Storage Services
  - Cloud Processing Infrastructure
  - Cloud Support Services
  - Cloud Network and Perimeter Security
  - Elastic Elements: Storage, Processing, and Virtual Networks

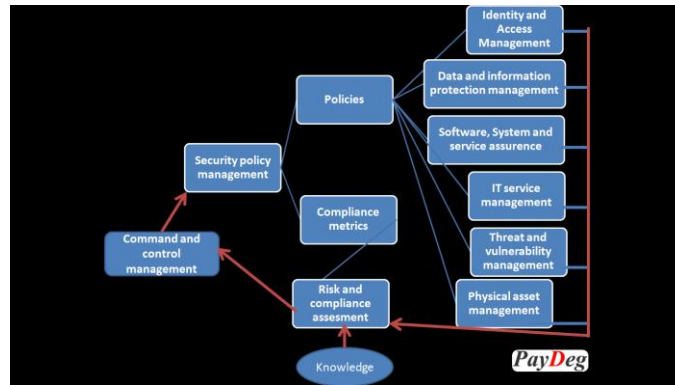
Clouds typically have single security architecture but have many customers with different demands.

Clouds should attempt to provide configurable security mechanisms.

When we come to security and data privacy across IaaS, PaaS and SaaS;

- Identity and Access Management (IAM)
  - IdM federation (SAML, WS-Federation, Liberty ID-FF)
  - Strong authentication standards (HOTP, OCRA, TOTP)
  - Entitlement management (XACML)
- Data Encryption (at-rest, in-flight), Key Management
  - PKI, PKCS, KEYPROV (CT-KIP, DSKPP), EKMI
- Records and Information Management (ISO 15489)
- E-discovery EDRM: Electronics Discovery Reference Model

Architectural view of security for cloud may help us to understand security management includes policies as much as compliance metric;



architecture but have many customers with different demands.

Clouds should attempt to provide configurable security mechanisms.

When we come to security and data privacy across IaaS, PaaS and SaaS;

- Identity and Access Management (IAM)
  - IdM federation (SAML, WS-Federation, Liberty ID-FF)
  - Strong authentication standards (HOTP, OCRA, TOTP)
  - Entitlement management (XACML)
- Data Encryption (at-rest, in-flight), Key Management
  - PKI, PKCS, KEYPROV (CT-KIP, DSKPP), EKMI
- Records and Information Management (ISO 15489)
- E-discovery EDRM: Electronics Discovery Reference Model

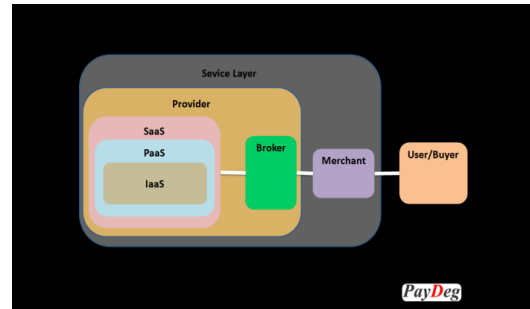
Architectural view of security for cloud may help us to understand security management includes policies as much as compliance metric;

Cloud network and perimeter security;

- Advantages
  - Distributed denial of service protection
  - VLAN capabilities
  - Perimeter security (IDS, firewall, authentication)
- Challenges
  - Virtual zoning with application mobility

There are some additional issues;

- Issues with moving PII and sensitive data to the cloud
  - Privacy impact assessments
- Using SLAs to obtain cloud security
  - Suggested requirements for cloud SLAs
  - Issues with cloud forensics



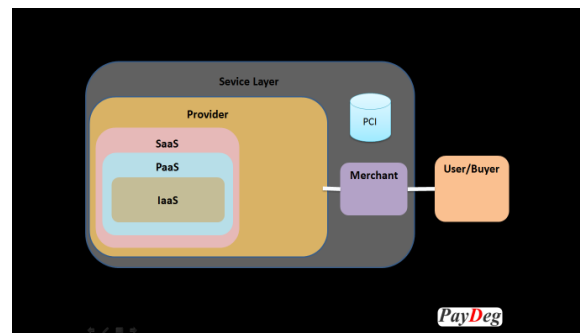
You should decide where is good place for your data after evaluating issues we mentioned in this document.

### Cloud Security Scenarios

Let's take a look at the chains here; every chain must be secure in order to serve secure from service layer. Of course user/buyer side must provide own security too.

There are a few security scenarios to keep service layer secure, here are they;

For scenarios let us consider credit card information Scenario 1;

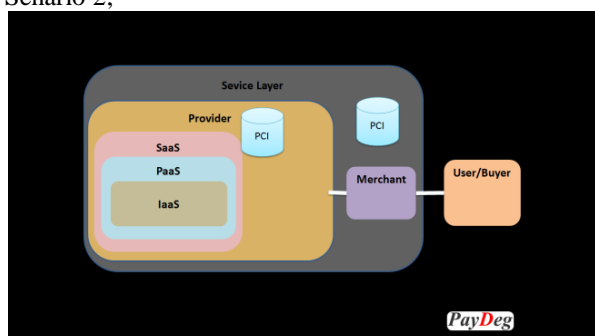


All PCI controls and card data at merchant side, so cloud service provider has no responsibility over card data.

Leakage can be through:

- Excel spreadsheet on cloud systems
- Application screenshots with card numbers
- Finance and HR documents with PANs(Primary account numbers)
- Other Office formats with PAN information
- Text dumps from poorly-written/legacy applications

Senario 2;



In this scenario, merchant uses cloud provider(s) for testing, training, backup systems, data storage, etc. So PAN data is transmitted through cloud and stored in cloud, but no payment data is processed in cloud.

The use case may range from a simple cloud or hybrid backup to offsite storage of historical data. No PANs are processed in the cloud in a clear-text form, but only persist on cloud-deployed systems in encrypted form.

We may have three cases here;

1. Unencrypted PANs at cloud service provider - result; no PCI (Payment card Industry) compliance possible, merchant has the responsibility. In
2. Encrypted with provider having the key - implies; provider must be PCI-OK. If provider has NO key. In PaaS case, the data is not likely to be encrypted by a key not visible to CP. Thus, the cloud systems are in scope (down to VM layer) and it is most likely that the cloud provider will be responsible for most of the controls (must be PCI compliant Service Provider), but merchant will be responsible for application security controls. then Cloud environment can be claimed to be out of scope in that case merchant has the responsibility.
3. Encrypted with provider NOT having the key - implies; presumably, provider may be NOT PCI-OK. Merchant deals with PCI DSS.

If we look at the core of the provider side;

- SaaS –For example; credit cards in Salesforce customer records – can be replaced in case 2, merchant and provider shares responsibilities. Can also be in case 3; the data is not encrypted by a key not visible to cloud

provider. Thus, the cloud systems are in scope (down to VM layer) and it is most likely that the cloud provider will be responsible for most of the controls (must be PCI compliant SP).

- PaaS - Force.com or Google Application Engine application that contains PANs. Can be replaced in case 3 and cloud service provider with merchant shares the responsibility. The data is not likely to be encrypted by a key not visible to cloud provider.

In case 3; for example Force.com or google app engine - it is most likely that the cloud provider will be responsible for most of the controls (must be PCI compliant service provider), but merchant will be responsible for application security controls.

- IaaS - Backup or other storage of PANs. In case 2; for example; Salesforce- Merchant and provider share the responsibilities. Cloud service provider encrypts the data and/or can decrypt it. If cloud provider has no key then, cloud environment can be claimed to be out of scope

In case 3; for example; VMs in the cloud, EC2 instances- Merchant deals with PCI DSS, provider may not know anything about it and there is no way for cloud service provider to decrypt the data.

IaaS service may retain complete control of, and therefore be responsible for, the ongoing security and maintenance of all operating systems, applications, virtual configurations (including the hypervisor and virtual security appliances), and data. In this scenario, the cloud provider would only be responsible for maintaining the underlying physical network and computing hardware.

SaaS service offering may encompass management of all hardware and software, including virtual components and hypervisor configurations. In this scenario, the entity may only be responsible for protecting their data, and all other security requirements would be implemented and managed by the service provider.

To be compliant in this scenario; If provider encrypts the data, they need to be a compliant service provider. If merchant encrypts the data, they may want to still hire a compliant service provider, but they don't have to.

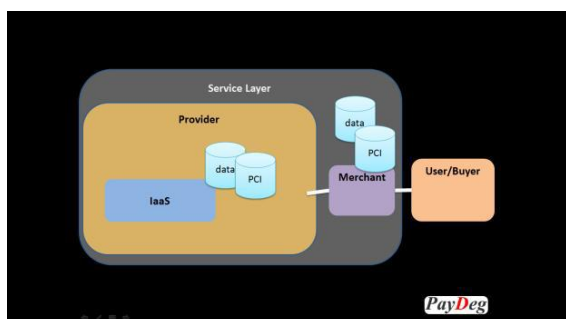
Contract - SLA should include the service provider achieving and maintaining compliance. Merchant should be able to verify the encryption of data and also require proof of how the service provider satisfies their requirements.

Here is the control matrix by Cloud Security Alliance;

PCI/DSS Requirement	Merchant	Cloud provider
Secure application development: R6	IaaS, PaaS	SaaS
Update OS: R6	IaaS (joint)	IaaS (joint), PaaS, SaaS
Log management: R10	IaaS (joint), PaaS (joint)	IaaS (joint), PaaS (joint), SaaS
Render PANs unreadable: R3.4	IaaS, Maybe: PaaS	SaaS, Maybe: PaaS
Physical access control: R9	None	IaaS, PaaS, SaaS
Vulnerability scanning: R11.2	IaaS (joint – per system), PaaS (joint)	IaaS (joint), PaaS (joint), SaaS
Penetration tests: R11.3	IaaS (joint), PaaS (joint), SaaS (joint) – degree varies	IaaS (joint), PaaS (joint), SaaS (joint) – degree varies
Security policy: R12	IaaS, PaaS, SaaS (all joint)	IaaS, PaaS, SaaS (all joint)
Wireless security: R11.1	None	IaaS, PaaS, SaaS

In case of a provider data leak, merchant should be prepared to;

- handle the incident as if it happened with them and
- transfer regulated data to another provider



Scenario 3;

Merchant uses public IaaS cloud and processes cards and possibly stores them as well in the cloud. So, PAN data stored, passed through and processed in the cloud at provider. Cloud provider must be PCI-ok.

For this scenario;

- Encryption - all at merchant side
- Password management – both at merchant and provider side
- Incident response - true shared
- Physical security – all at cloud provider side

There is responsibility split in this scenario; Merchant;

- Application security
- Updating OS- guest Os
- Scoping
- Monitoring
- Log management – guest OS and applications

Provider;

- Physical – access control
- Network
- Encryption
- Key management
- System security
- Parts of application security
- Updating OS- host OS
- Log management- host OS, management systems

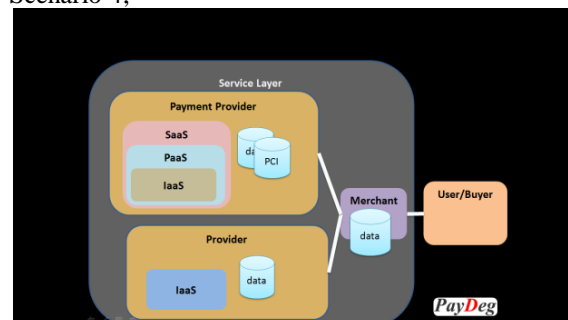
Owning the infrastructure does not mean owner has to manage it. Cloud IaaS service provider owns the firewall appliances but Merchant, other cloud service provider or 3rd party manages the appliances.

But there are 2 basic facts;

- Merchant can't do PCI DSS without the cloud service provider
  - Cloud service provider can't make merchant compliant
- Merchants, have to obtain cloud service provider's PCI evidence before doing own assessment.

	Cloud Customer Responsibility		
	Cloud Service Provider Responsibility		
	Type of Cloud Service		
Area of Responsibility	IaaS	PaaS	SaaS
Data			
Software, User Applications			
Operating systems, Databases			
Virtual Infrastructure			
Computer and Network hardware			
Data Center (Physical facility)			

Scenario 4;



Merchant – ecommerce or stores uses public cloud IaaS provider, processes cards and possibly stores them as well in the cloud, and uses a dedicated cloud service provider for payment processing, not hosting cloud service provider.

The communication from the payment provider to the Cloud service provider’s web front end can never contain cardholder data.

The more payment provider takes on, the better: PCI stays in their cloud.

What is PCI compliance? Payment Card Industry Data Security Standards (PCI DSS) are network security and business practice guidelines adopted by Visa, MasterCard, American Express, Discover Card, and JCB to establish a “minimum security standard” to protect customer’s payment card information. It’s a requirement for all merchants that store, transmit, or process payment card information.

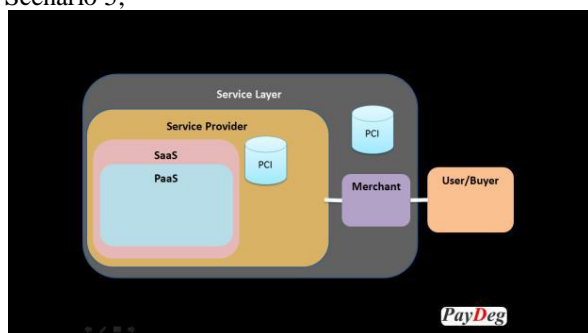
### How does my business become PCI compliant?

You can either use PayPal Website Payments Standard, Email Payments, or Payflow Link.\* Or if you are storing, transmitting, or processing payment card information, you must:

- Build and maintain a secure network to protect payment card information
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Pass quarterly remove vulnerability scans
- And more ...

For this scenario; merchant is responsible for other PCI DSS controls and assuring that service provider is compliant and maintaining PCI compliance and implementing other requirements on merchant data.

Scenario 5;



PaaS PCI;

- Merchant – ecommerce or stores
- Use public cloud PaaS provider
- Processes cards and possibly stores them as well in the cloud

Description of the scenario;

- A major ecommerce website
- Uses cloud service provider for a broad spectrum of tasks, including payments
- Cloud provider may be PCI-ok
- Credit card data stored/passed in the cloud
- Credit card data processed in the cloud
- Merchant does NOT control the OS/VMs at the cloud service provider

A major difference between IaaS and PaaS is the amount of control over the system available to users of the services. IaaS provides total control, PaaS typically provides no control. This also means virtually zero administration costs for PaaS whereas IaaS has administration costs similar to a traditional computing infrastructure.

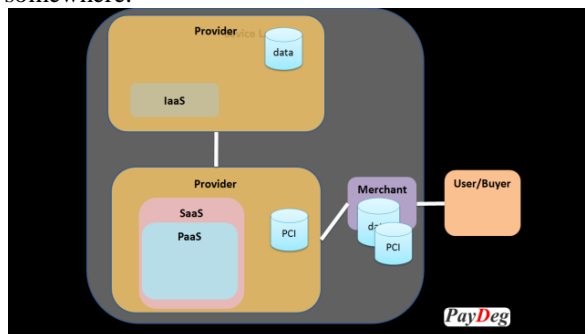
One of the main differences between PaaS and IaaS is the level of control and administration available. With PaaS services such as Azure and Google App Engine once the application is deployed to the cloud no access to server software or the underlying operating system is available for administration.

If PaaS cloud service provider is not PCI-ok (Force.com, Azure) then the only way to PCI is complete “3rd party payment takeover” like in Scenario 4.

If PaaS cloud service provider is PCI-ok then build the control matrix like in Scenario 3.

Scenario 6;

Merchant – ecommerce or stores - use public cloud PaaS or SaaS provider, who uses public IaaS provider to processes cards and possibly stores them ... somewhere.



We may describe like;

- A major ecommerce website
- Uses cloud service provider for a broad spectrum of tasks, including payments
- Their provider uses another cloud provider
- Some cloud providers MAY BE PCI-OK
- Credit card data stored/passed in the cloud
- Credit card data processed in the cloud

Merchant’s cloud provider’s cloud service provider is

NOT merchant’s cloud provider! However, the merchant is still responsible if some controls are NOT implemented by provider’s cloud service provider.

### What We May Learn From Scenarios?

- It is better to have the payment processor handle more and merchant/cloud service provider handle less of the PCI burden
  - Cloud service provider may do it, but MERCHANT is responsible and need to validate it
  - Finally, we CAN have PCI in the cloud!
  
  - A few recommendations;
  - Follow the scenarios as templates for your projects
  - Learn to scope in the cloud
  - Make a matrix of shared responsibility (and “keep it with you at all times”)
  - Remember: MERCHANT is on the hook, even if cloud service provider does it (as per PCI DSS)
  - Use PCI + cloud security thinking for other sensitive data: SSN, PHI, financials, etc
  - Involve legal in SLA and other discussions about regulated data in the cloud (!)
  - Scan for YOUR sensitive data being put in the cloud by business partners – in THEIR clouds
  - “Trust but verify” principle MUST be applied to your cloud service provider
- Now let’s take a look at some real life examples;

1. GE moved 400,000 desktops from Microsoft Office to Google Apps and then migrated them to Zoho for privacy concerns.<sup>1</sup>

- Architecture
- Open source
- Linux hosts
- Xen virtualization (virtual machine monitor)
- Apache Hadoop (file system)

So it is important to evaluate the company’s security needs first and then cloud service security.

2. New York Times

- Used EC2 and S3 to convert 15 million scanned news articles to PDF (4TB data)
- Took 100 Linux computers 24 hours (would have taken months on NYT computers)
- “It was cheap experimentation, and the learning curve isn’t steep.” – Derrick Gottfrid.<sup>2</sup>

For some jobs extra security may not be needed, and cloud can ease the jobs.

3. Nasdaq

- Uses Amazon S3 to deliver historic stock and fund information
- Millions of files showing price changes of entities over 10 minute segments
- “The expenses of keeping all that data online [in Nasdaq servers] was too high.” – Claude Courbois, Nasdaq VP

- Created lightweight Adobe AIR application to let users view data

4. New Jersey Transit Wins InfoWorld 100 Award for its Cloud Computing Project<sup>3</sup>

- Use Salesforce.com to run their call center, incident management, complaint tracking, and service portal
- 600% More Inquiries Handled
- 0 New Agents Required
- 36% Improved Response Time

5. U.S. Army uses Salesforce CRM for Cloud-based Recruiting<sup>4</sup>

- U.S. Army needed a new tool to track potential recruits who visited its Army Experience Center.
- Use Salesforce.com to track all core recruitment functions and allows the Army to save time and resources.

At the end Sun Microsystems CTO Greg Papadopoulos Sunny vision of the future

– Users will “trust” service providers with their data like they trust banks with their money

– “Hosting providers [will] bring ‘brutal efficiency’ for utilization, power, security, service levels, and idea-to-deploy time” –CNET article

– Becoming cost ineffective to build data centers

– Organizations will rent computing resources  
– Envisions grid of 6 cloud infrastructure providers linked to 100 regional providers

### Conclusion

As a result of small research made by PayDeg, people mostly think about guards in front of the bank when they have been asked what comes first in their mind about security (güvenlik). At Google search of “güvenlik” also resulted with security guards firms.

At Google search of “security” resulted with “security essentials” and meaning of security in Wikipedia. PayDeg believes in Turkey still most valuable thing is money while it is information for<sup>53</sup> other countries.

---

<sup>53</sup> 1 <http://arstechnica.com/information-technology/2008/10/washington-dc-latest-to-drop-microsoft-for-web-apps/>

2 <http://www.infoworld.com/d/cloud-computing/early-experiments-in-cloud-computing-020>

3 <http://www.salesforce.com/showcase/stories/njtransit.jsp>

4 [http://www.nextgov.com/nextgov/ng\\_20081126\\_1117.php](http://www.nextgov.com/nextgov/ng_20081126_1117.php)

For that reason as scenarios PayDeg consider credit card information on e-commerce. Please don't forget, for the e-commerce good security on the buyer's system also benefits the seller; the buyer's system is less likely to be used for fraud or to be unavailable or otherwise negatively affect the seller. (The reverse is also true.)

With this paper PayDeg wants to unroll possible security scenarios. One may produce more scenarios out of those ones.

In conclusion, knowing about the security principles, roles, services and possible scenarios lets us choose proper security options and functions in the Cloud.

References And Further Reading.

We read many pdf and used some content out of them.

- Introduction and Architecture Overview
- IBM Cloud Computing Reference Architecture 2.0
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A –June 2004 – 33 IT security principles
- An Introduction to Computer Security: The NIST Handbook (NIST Special Publication 80012 <http://csrc.nist.gov/nistpubs/800-12> ).
- Generally Accepted Principles and Practices for Securing Information Technology Systems - Marianne Swanson, Barbara Guttman
- DPLaw\_world\_handbook\_2012.pdf
- Datasheet-ISF.pdf
- Datasheet\_PlatformISF.pdf
- Architecting-VMware-vCloud.pdf
- Private-VMware-vCloud-Service-Definition.pdf
- Public-VMware-vCloud-Service-Definition.pdf
- Operating-VMware-vCloud.pdf
- book\_eucalyptus\_beginners\_guide\_uec\_editi on1.pdf
- Eucalyptus\_Overview.pdf
- enomaly\_Intel\_Cloud\_Builder.pdf
- abiquo\_enterprise\_edition\_datasheet.pdf
- abiquo\_community\_edition\_datasheet.pdf
- Webinar-ISF-CreatePrivateCloudsforCriticalApplications.pdf
- CSC\_Papers\_2010\_Building\_a\_Cloud\_Computing\_Specification.pdf
- An Architectural View of Security for Cloud.pdf
- Security Principles for
- Cloud and SOA.pdf

We watched a few presentation;

How Google tackles IT security and what you can learn from it.

We also checked it out the websites of the companies; <http://www.edrm.net/resources/more-resources/data-protection-laws>  
[http://www.eecs.berkeley.edu/~rcs/research/intereactive\\_latency.html](http://www.eecs.berkeley.edu/~rcs/research/intereactive_latency.html)

<http://thecustomizewindows.com/2012/12/paas-model-and-architecture-of-google-app-engine/>  
[http://blogs.computerworld.com/data\\_center\\_utilization\\_15\\_of\\_11\\_8\\_million\\_is\\_a\\_big\\_number](http://blogs.computerworld.com/data_center_utilization_15_of_11_8_million_is_a_big_number)  
<http://www.techrepublic.com/blog/10things/10-security-problems-you-might-not-realize-you-have/2768>

<http://www.gtri.gatech.edu/ctisl>

<http://platform.com/> <http://eucalyptus.com/>

[http://www.eucalyptus.com/resources/cloud-myths-dispelled?mkt\\_tok=3RkMMJWWfF9wsRonuKXJZKXonjHpfsX67uosUa6g38431UFwdcjK Pmjr1YYDSdQhcOuuEwcWGog8xRlbG%2ByMbJRV6Q%3D%3D](http://www.eucalyptus.com/resources/cloud-myths-dispelled?mkt_tok=3RkMMJWWfF9wsRonuKXJZKXonjHpfsX67uosUa6g38431UFwdcjK Pmjr1YYDSdQhcOuuEwcWGog8xRlbG%2ByMbJRV6Q%3D%3D)

<http://www.enomaly.com/>

<http://www.abiquo.com/>

<http://www.vmware.com/>

<http://www.vmware.com/cloud-computing/cloud-architecture/vcat-toolkit.html>

<http://www.windowsazure.com/en-us/>

<http://msdn.microsoft.com/en-us/library/windowsazure/dd179367.aspx>

<http://aws.amazon.com/ec2/>

<http://www.cloudstandardscustomerCouncil.org/uc.htm>

<http://cloud-computing.learningtree.com/2010/08/25/comparing-paas-and-iaas/>

This document is based on Security principles and security scenarios on e-commerce for cloud computing.

This document is part of my speech at Academic IT Conference at Akdeniz University, Turkey. <http://ab.org.tr/ab12/ab12-cerceve.html>