Introduction to Cloud Security

94% of enterprises **use cloud** computing

According to Right Scale's annual State of the **Cloud** Report for 2019, 91% of businesses used public **cloud** and 72% used a private one. Most enterprises actually utilize both options – with 69% of them opting for a hybrid **cloud** solution.

Cloud providers utilizing virtualization technologies combined with self-service capabilities for computing resources via the Internet to run applications in cloud. In this process virtual machines from multiple organizations have to be co-located on the same physical server in order to maximize the efficiencies of virtualization and run the applications (each application runs in a virtual machine).

Whereas the managed service provider (MSP) model ensures that the customers’ applications and data are secure (because the applications run on a dedicated server hence more secure because of the security mechanisms enforced by the MSPs).

Security ranked first as the greatest challenge or issue of cloud computing, hence the methodology for ensuring application and data security and compliance integrity for those resources that are moving from on-premises(MSP) to public cloud environments is important aspect to learn.

Once we talk about cloud security we need to examine security in all the three types of service models.

a)Software as a Service: model of software deployment in which an application is licensed for use as a service provided to customers on demand.

b)Platform as a Service: all of the facilities required to support the complete life cycle of building and delivering web applications and services are available to developers, IT managers, and end users entirely from the Internet.

PaaS offerings include workflow facilities for application design, application development, testing, deployment, and hosting, as well as application services such as team collaboration, web service integration and marshalling, database integration, security, scalability, storage, persistence, state management, application versioning, application instrumentation, and developer community facilitation.

c)Infrastructure as a Service : Rather than purchasing servers, software, data center space, or network equipment, clients buy these resources as a fully outsourced service. The service is typically billed on a utility computing basis, and the quantity of resources consumed (and therefore the cost) typically reflects the level of activity.

We need to evolve best security practices to be followed the cloud vendors.

Although there is a significant benefit to leveraging cloud computing, security concerns have led organizations to hesitate to move critical resources to the cloud. Corporations and individuals are often concerned about how security and compliance integrity can be maintained in this new environment.

1. PCI DSSPayment Card Industry Data Security Standard) is a security standard developed and maintained by the [PCI Council](https://www.pcisecuritystandards.org/about_us/leadership). Its purpose is to help secure and protect the entire payment card ecosystem.  
   Protect your system with firewalls
2. Configure passwords and settings
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Regularly update and patch systems
7. Restrict access to cardholder data to business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to workplace and cardholder data
10. Implement logging and log management
11. Conduct vulnerability scans and penetration tests
12. Documentation and risk assessments

Before diving into the PCI requirements, you will also want  to find out out [which SAQ applies to your business.](https://www.securitymetrics.com/blog/pci-standards-which-pci-saq-right-my-business) While most requirements will stay the same, there are some differences in the work you’ll need to do based on your SAQ.

The Sarbanes-Oxley Act (or SOX Act) is a U.S. federal law that aims to protect investors by making corporate disclosures more reliable and accurate. The Act was spurred by [major accounting scandals,](https://corporatefinanceinstitute.com/resources/knowledge/other/top-accounting-scandals/) such as Enron and WorldCom (today called MCI Inc.), that tricked investors and inflated stock prices. Spearheaded by Senator Paul Sarbanes and Representative Michael Oxley, the Act was signed into law by President George W. Bush on July 30, 2002.

The Health Insurance Portability and Accountability Act of 1996 (**HIPAA**) is a federal **law** that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

**Key Management Interoperability Protocol Specification (KMIP)**

**Internet Print protocol(IPP)**

**IPP - Security**

* **Looked at threats and methods of attack**
* **Identified a number of generic security services**
* **Mapped methods of attack against generic security services**
* **Started searching for suitable Internet security standards and implementations**
* **Encourage input from IETF security experts**

Baseline Security Practices

1. **Security Management (People)**