A Survey of Cloud Computing Security: Issues, Challenges and Solutions

Elom Worlanyo (A paper written under the guidance of Prof. Prof. Raj Jain) Download 

Abstract

Cloud computing is a rapidly maturing technology that has given rise to a lot of recent innovations. As a delivery model for IT services, its capacity to stimulate growth by providing ready-made environments for various forms of development is unparalleled. Its very nature however makes it open to a variety of security issues that can affect both the providers and consumers of these cloud services. These issues are primarily related to the safety of the data flowing through and being stored in the cloud, with sample issues including data availability, data access and data privacy. Industry has hence developed various procedures such as data encryption and service authentication schemes to deal with them. This paper explores and examines various such security issues along with the various methods used in industry to ameliorate their possible detrimental effects.

Keywords

Cloud, Computing, Security, Encryption, Cloud Service Provider, Cloud Service Customer, IaaS, PaaS, SaaS, Public Cloud, Private Cloud, Threats, Vulnerability

Table of Contents:

1. Introduction

This paper seeks to identify and explore important security issues and challenges facing cloud computing, a

now fairly mature technology, along with the methods employed in industry to combat these problems. In order to achieve this goal, we must first understand the concepts behind this technology, as well as its underlying infrastructure. There are now many services being offered by vendors which have the label "cloud" attached to them, using this now fashionable term to entice members of the general public who may not necessarily know any better. In this introduction, we aim to give a succinct description of what cloud computing entails, and in so doing shed light on the various characteristics defining this technology.

Definition

Cloud computing, also known as on-demand computing, is a form of internet-based computing that allows end users to share information and resources. More formally, the National Institute of Standards and Technology (NIST) defines cloud computing as *a model for enabling ubiquitous, 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* [Jansen11] .

Characteristics [Ziao13]

NIST further specifies that cloud computing exhibits the following five characteristics in its operation :

A. On-demand self-service

A Cloud Service Customer (CSC) can use an online interface to allocate computing resources like additional computers or network bandwidth without human interaction with their Cloud Service Provider (CSP).

B. Broad network access

CSCs can access computing resources over networks such as the Internet from a variety of computing devices.

C. Resource pooling

CSPs can use shared computing resources to provide cloud services to multiple customers. Virtualization and multi-tenancy systems are typically used to both segregate and protect each customer and their data from other customers [ASD12] . They can also be used to make it appear to customers that they are the only user of a shared computer or software application.

D. Rapid elasticity

This refers to the quick and automatic balancing of the amount of available computer processing, storage and network bandwidth as required by customer demand.

E. Pay-per-use measured service

This involves customers only paying for the computing resources that they actually use, and being able to monitor their usage. The service purchased by customers can be quantified and measured

It is hence worth noting that a vendor adding the words "cloud" or "as a Service" to the names of their products and services does not automatically mean that the vendor is selling cloud computing as per the NIST definition. Customers sharing resources is at the heart of cloud computing, and as such looks to be a potential

area of concern regarding security. Let us now look at the infrastructure that actual cloud computing services utilize in order to clarify this.

2. Cloud Computing Infrastructure

Even based on the brief overview given so far, we can see some potential security pitfalls looming: sharing resources that are not in one's control with others is always likely to be a venture fraught with risks. In this section we look at the infrastructure that implements the concepts detailed previously in order to better grasp the intricacies of the possible security problems we might face.

2.1 Cloud Service Models

The amount of resources exposed over a network can depend on the type of service that a vendor is providing to its customers. Different services give rise to different security concerns, and may even lead to different parties being responsible for handling said concerns.

According to the NIST there are three main types of services that a given Cloud Service Provider (CSP) will offer [Jansen11] . These are:

Infrastructure as a Service (IaaS)

In this model, the vendor provides physical computer hardware, including data storage, CPU processing and network connectivity.The vendor may share their hardware among multiple Cloud Service Customers (CSC) by using virtualization software. IaaS allows customers to run, control and maintain operating systems and software applications of their choice, but the vendor typically controls and maintains the physical computer hardware. This leads to the customer being more responsible for handling their own data security with the vendor being more responsible for physical security, since they own and manage the physical devices being used as infrastructure. Examples of IaaS vendor services include GoGrid, Amazon Elastic Compute Cloud (EC2) and Rackspace Cloud.

Platform as a Service (PaaS)

In this model, the vendor provides not only Infrastructure as a Service, but also the operating systems and server applications that their customers use. PaaS lets customers use the vendor's cloud infrastructure to deploy user made web applications/software. Typically the vendor controls and maintains the physical computer hardware, operating systems and server applications while the customer only controls and maintains their developed software applications. Customers would therefore be mainly responsible for any security exploits that could target their applications, while the vendor is not only responsible for physical security, but also for any security exploits that could target network connections, data storage and data access. Examples of PaaS vendor services include Google App Engine, Force.com, Amazon Web Services Elastic Beanstalk, and the Microsoft Windows Azure platform.

Software as a Service (SaaS)

In this model, the vendor provides customers with software applications using their cloud infrastructure and cloud platforms. These end user applications are typically accessed by users via web browser, as such there is no need to install or maintain additional software. The vendor typically controls and maintains the physical computer hardware, operating systems and software applications while the customer only controls and

maintains certain application configuration settings specific to them. The vendor is mainly responsible for ensuring all forms of security in this service. Examples of SaaS vendor services include Google Docs, Google Gmail and Microsoft Office 365.

From this subsection, it is fairly clear by now that the level of responsibility shared between CSPs and CSPs differs based on the service model being employed.

2.2 Cloud Deployment Models

Another factor that can change the amount of exposure a given cloud network has is its deployment model. This refers to the manner in which the cloud network is structured, and there are four main models, namely:

Public cloud

In this model, a CSC uses a vendor's cloud infrastructure which is shared publically via the Internet with many other CSCs. This model is the most exposed and as such has a variety of inherent security risks that need to be considered.

Private cloud

In this model, a CSC has exclusive use of cloud infrastructure and services located at the CSC's premises or off site, and which are managed by the CSC or a CSP. This model has reduced potential security concerns compared to the public cloud since there is increased control.

Community cloud

In this model, a private cloud is shared by several CSCs with similar security requirements. This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud.

Hybrid cloud

This model consists of any viable combination of the cloud deployment models mentioned above.

The information provided in the preceding chapters can be summarized visually using the following illustration adapted from the NIST:

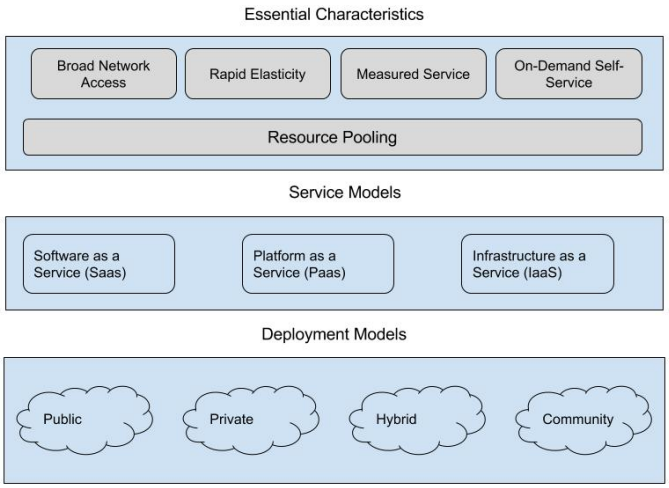

Figure 1 - NIST Visual Model of Cloud Computing Definition [CSA11]

Figure 1 is a brief overview of the various layers involved in the provision of a cloud computing service. First, the CSP must decide on a deployment model depending on the nature of the service provided, as well as the customers involved. The needs of the CSC is also a leading factor in the type of service model provided. No matter which service and deployment models are chosen, however, all cloud services contain the five essential characteristics represented in the uppermost layer.

From the information obtained in this section, we can see that delving into all possible security issues would be well outside the scope of this paper. As such, we will limit ourselves to examining in depth security issues affecting mainly public clouds since the bulk of the security challenges facing most cloud services are represented there. We will begin this discussion in the next section.

3. Security Threats and Vulnerabilities

As mentioned earlier, we will limit the scope of our security survey to the most ubiquitous of clouds - the public cloud. First, we introduce the basic security considerations for this deployment model, then we examine and categorize the threats specific to CSPs and CSCs.

3.1 Basic Security Risk Considerations

There are a number of areas that are at risk of being compromised and hence must be secured when it comes to cloud computing. Each area represents a potential attack vector or source of failure. By risk analysis, five key such areas have been identified:

Organizational Security Risks

Organizational risks are categorized are categorized as the risks that may impact the structure of the organization or the business as an entity [Dahbur11] . If a CSP goes out of business or gets acquired by another entity, this may negatively affect their CSPs since any Service Level Agreements (SLA) they had may have changed and they would then have to migrate to another CSP that more closely aligns with their needs. In addition to this, there could be the threat of malicious insiders in the organization who could do harm using the data provided by their CSCs.

Physical Security Risks

The physical location of the cloud data center must be secured by the CSP in order to prevent unauthorized on-site access of CSC data. Even firewalls and encryption cannot protect against the physical theft of data. Since the CSP is in charge of the physical infrastructure, they should implement and operate appropriate infrastructure controls including staff training, physical location security, network firewalls. It is also important to note that the CSP is not only responsible for storing and process data in specific jurisdictions but is also responsible for obeying the privacy regulations of those jurisdictions.

Technological Security Risks

These risks are the failures associated with the hardware, technologies and services provided by the CSP. In the public cloud, with its multi tenancy features, these include resource sharing isolation problems, and risks related to changing CSPs, i.e. portability. Regular maintenance and audit of infrastructure by CSP is recommended.

Compliance and Audit Risks

These are risks related to the law. That is, risks related to lack of jurisdiction information, changes in jurisdiction, illegal clauses in the contract and ongoing legal disputes. For example, depending on location, some CSPs may be mandated by law to turn over sensitive information if demanded by government.

Data Security Risks

There are a variety of data security risks that we need to take into account. The three main properties that we need to ensure are data integrity, confidentiality and availability. We will go more into depth on this in the next subsection since this is the area most at risk of being compromised and hence where the bulk of cloud security efforts are focused.

These risk categories have been further split between CSPs and CSCs and are illustrated in the following two diagrams:

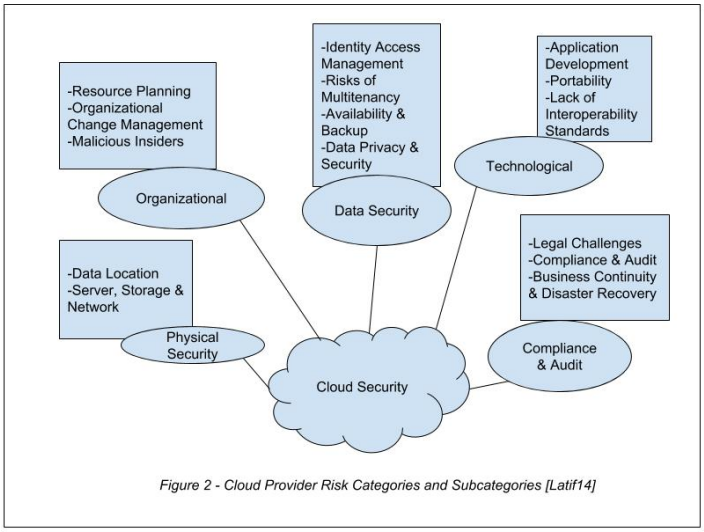

Figure 2 - Cloud Provider Risk Categories and Subcategories [Latif14]

In figure 2 we can see the five main areas of concern for a cloud service provider when it comes to security. The bullet points next to each category further narrows down a subcategory that could cause security issues to a CSP. Let us compare this to the security challenges facing the typical CSC, illustrated in figure 3.

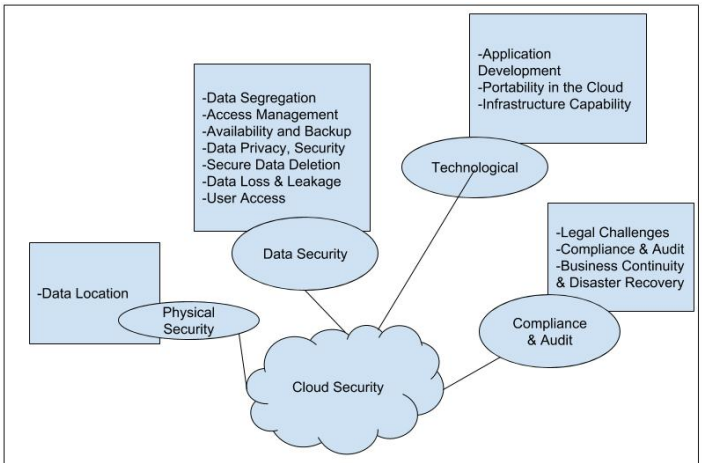

Figure 3 - Cloud Customer Risk Categories and Subcategories [Latif14]

Figure 3 similarly outlines the risk categories and subcategories facing CSCs. Comparing, we can see that organizational risks are solely borne by CSPs. This is because in a cloud computing service, the infrastructure is always provided by the CSP. We can also see that both CSPs and CSCs are bound by the same considerations when it comes to compliance and audit while regarding data security, technological security and physical security, the specific concerns a CSC may have would be different from what a CSP would have. This is mainly as a result of the different levels of control they have regarding each area, as discussed in section 2. Let us now look more closely at the data security issues that need to be taken into consideration.

Having given an outline of the basic security considerations present in this subsection, we will look at the considerations that have to be made for data in the next subsection.

3.2 Data Security Considerations

At the heart of all computing is arguably the processing of data into meaningful information. As such, when the processing and storage of such data is outsourced to infrastructure owned and maintained by a third party, this leads to a host of issues to consider when securing said data. These issues are especially more pronounced in the public cloud, since multiple parties, some of which could be malicious, have to share this aforementioned infrastructure.

Data Security Properties

As mentioned earlier there are some properties we need to ensure with data when utilising the cloud:

A. Privacy

Privacy is one of the more important issues to deal with in the cloud and in network security in general. Privacy ensures that the personal information and identity of a CSC are not revealed to unauthorized users. This property is most important to the CSC, especially when they deal with sensitive data.

B. Confidentiality

This is related to data privacy since this is the property ensuring that the data that belongs to a CSC is not revealed to any unauthorized parties. In public clouds, the CSP is mainly responsible for securing the CSC's data.This is particularly difficult due to multi tenancy, since multiple customers have access to the same hardware that a CSC stores its data. Some providers use job scheduling and resource

management, but most providers employ virtualization to maximize the use of hardware [Latif14] . These two methods allow attackers to have full access to the host and cross- VM side channel attacks to extract information from a target VM on the same machine.

C. Integrity

The integrity of data refers to the confidence that the data stored in the cloud is not altered in any way by unauthorized parties when it's being retrieved, i.e. you get out what you put in. To ensure this, CSPs must make sure that no third party has access to data in transit or data in storage. Only authorized CSCs should be able to change their data.

D. Availability

This property ensures that the CSC has access to their data, and are not denied access erroneously or due to malicious attacks by any entity. Attacks like denial-of-service are typically used to deny availability of data.

Data Stages

The flow of data through a cloud goes through various distinct stages, with each stage requiring one or more of the previous properties to be maintained. These stages are as follows [Bhadauria12] :

A. Data-in-transit

This is when data is in the process of being transmitted either to the cloud infrastructure or to the computing device used by the CSC. Here, data is most at risk of being intercepted, hence violating confidentiality. Encryption is generally used here to prevent this, along with other methods we shall detail later.

B. Data-at-rest

This is when data has been stored in the cloud infrastructure. The main issue with this stage for the CSC is their loss of control over the data. The onus of defending against attacks at this stage hence fall on the CSP. They have to ensure that all 4 of the data security properties outlined are upheld at this stage.

C. Data-in-use

This is when data is being processed into information. Here, the issues might lie with the corruption of data while it is being processed. In order to prevent this the integrity of data going into a process must be ensured using any one of the applicable methods we will discuss later

In addition to these three stages, the data left out in case of data transfer or data removal also needs to be considered, since it can cause severe security issues in the case of public cloud offerings since a CSC may end up gaining access to sections of data not properly deleted from a prior CSC.

Now that we have looked at the various issues that need to be guarded against in cloud computing, we can see that by far the largest and most complex area is that of data security. We shall hence focus slightly more on the methods used in industry to preserve data security, and give an overview of the more straightforward techniques used in the other risk areas.

4. Methods to Ensure Security in the Cloud

Having now outlined the various risks faced when using clouds, we can now take a look at the methods industry has developed to deal with these issues. In this section we will focus on the methods used to ensure all the various forms of data security, and also take a brief look at the strategies employed to solve the other secondary issues.

4.1 Countermeasures for Security Risks

In section 3 we outlined a number of areas where security exploits could target. In this subsection, we give a cursory overview of various techniques used in industry to secure select issues in these problem areas.

Organizational Security Risks [Jain14]

Malicious Insiders - The risk of having malicious personnel in a CSPs staff can be mitigated by putting strict legal constraints in contracts when hiring personnel. A comprehensive assessment of the CSP by a third party, as well as a robust security breach notification process will also go a long way to preventing this.

Physical Security Risks

Physical Breach - The risk of intruders gaining physical access to devices used in the provision of cloud services can be reduced by having strong physical security deterrents in place such as armed guards, keycard access and biometric scans to restrict access to sensitive locations in the data center.

Technological Security Risks

Virtualized defence and reputation based trust management - CSP could use the following structure: a hierarchy of DHT-based overlay networks, with specific tasks to be performed by each layer. The lowest layer deals with reputation aggregation and probing colluders. The highest layer deals with various attacks [Bhadauria12] . Reputation aggregation here is related to utilizing various sources to verify certain connections, and probing colluders refers to checking if any sources are associated with known malignant parties.

Secure virtualization - CSP can use an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware. Behaviour of cloud components can also be monitored by logging and periodic checking of executable system files.

Trust model for interoperability and security - There should be separate domains for providers and users, each with a special trust agent. A trust agent is an independent party that collects security information used to verify an endpoint [Wiki1] . There should also be different trust strategies for service providers and customers.

Compliance and Audit Risks

This area primarily deals with legal issues and as such, both CSPs and CSCs need to understand legal and regulatory obligations and ensure that any contracts made meet these obligations The CSP should also ensure that its discovery capabilities do not compromise security and privacy of data [Jain14] .

Having seen some methods used to prevent lapses in security from the other four areas, in the next subsection

we will look at some of the primary techniques used for ensuring data security.

4.2 Methods to ensure Data security

There are several methods used to ensure the various properties of data are secure. Here we look at authentication and encryption techniques and present a cursory comparison of these techniques:

Authentication in the Cloud

Since cloud computing is associated with having users' sensitive data stored both with a CPC and a CSP, identity and access management (IAM), a form of access control, is very crucial [Ahmed14] . Authentication for the CPC can be done either by the CSP or outsourced to third party specialists. Some methods for authentication include the identity-based hierarchical model for cloud computing (IBHMCC) and the SSH Authentication Protocol (SAP)[Spoorthy14] . This is used mainly to protect data privacy and confidentiality. IAM ensures regulatory compliance by managing the major security concerns - authentication, automated provisioning and authorization services. Other underlying technologies used for authentication, authorization and access control services are OpenID, OAuth, SAML, XACML[Ahmed14] .The trusted computing group's (TCG's) IF-MAP standard further allows for real-time communication between a cloud service provider and the customer about authorized users and other security issues [Sen13] .

Encryption techniques in the cloud

For securing data both at rest and in transit, cryptographic encryption mechanisms are certainly the best options. In transit, homomorphic encryption is one such mechanism. This involves processing on an encryption domain as described in [Ukil13] . Other methods such as searchable encryption [Agudo11] are also employed, so that data does not need to be decrypted to be accessed unlike with hommoorphic encryption. Sample encryption algorithms used include:

Caesar Cipher : It is a classical substitution cipher. A simple example of such a cipher replaces the letter of alphabet with a letter that is 3 paces ahead of it, for example "ZULU" will be converted into "CXOX". There are only 25 possible key options and as such this cipher can easily be brute forced [Krishna11] . It is no longer used in serious applications. Other similarly outdated classical ciphers are the Vigenere Cipher and the Playfair Cipher, also described in [Krishna11] .

S-DES - Simplified Data Encryption Standard has a process of key generation where instead of using a key as is for encryption and decryption, the key generation process of S-DES generates 2 sub keys after processing the initial 10 bit input [Krishna11] . The two sub keys are generated at both the transmission and receiving ends. With the inclusion of initial permutation and expansion permutations the security is substantial when compared with the classical techniques, S-DES gives some structure and formation to encryption techniques with step to step procedures for both encryption and decryption. It is not quite as widely used anymore since computing power has caught up with breaking it.

RSA - A cryptographic algorithm whose encryption key is public and differs from the decryption key which is kept secret [Soofi14] . RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, the creators of the algorithm. This algorithm is based on the fact that finding the factors of an integer is hard. It is one of the more commonly used encryption algorithms nowadays.

Secure Socket Layer (SSL) 128 bit encryption - it is a commonly-used protocol for managing the security of a message transmission on the Internet and it uses public and private key encryption system [Soofi14] .

5. Summary

From this paper, we have gained a decent understanding of cloud computing and what it entails. Building on that understanding we proceeded to outline and examine the various security issues that emerge as a result of the structures used in the development of various cloud computing solutions. We have realized that the bulk of issues occur in public clouds and relate to the security of the data that CSCs transmit to CSPs and vice versa. We then undertook a brief examination of some methods utilized by industry to combat the various security issues faced.

6. References

[Latif14] Latif, R., Abbas, H., Assar, S., Ali, Q., "Cloud computing risk assessment: a systematic literature review", Future Information Technology, pp. 285-295, Springer, Berlin, Germany, 2014., URL: http://www.researchgate.net/profile/Haider_Abbas8/publication/259221049_Cloud_Computing_Risk_Assessment_A_Systematic_Literature_Review/links/0a85e53328b478e2cb000000.pdf

[ASD12] Australian Government Cyber Security Operations Center, "Cloud Computing Security Considerations", September 2012, URL: http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_Considerations.pdf

[Jansen11] Jansen, W., Grance, T., "Guidelines on security and privacy in public cloud computing." NIST Special Publication 800-144, December 2011, URL: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[Ziao13] Xiao, Z., Xiao, Y., "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843-859, 2013, URL: http://mbanat.net/Security%20and%20Privacy%20in%20Cloud%20Computing.pdf

[Bhadauria12] Bhadauria, Rohit, Sanyal, Sugata, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", Intl. Journal of Computer Applications, Vol. 47, No. 18, pp. 47-66., Foundation of Computer Science, New York, USA, URL: http://arxiv.org/pdf/1204.0764.pdf

[Dahbur11] Dahbur, K., Mohammad, B., "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing.", Int Conference on Intelligent Semantic Web-Services and Applications, 2011, URL: http://www.jisajournal.com/content/4/1/5

[Ahmed14] Ahmed, M., Hossain, A., "Cloud computing and security issues in the cloud", IJNSA, Vol.6, No.1, January 2014., URL: http://airccse.org/journal/nsa/6114nsa03.pdf

[Spoorthy14] Spoorthy, V., Mamatha, M., Kumar, S., "A Survey on Data Storage and Security in Cloud Computing", IJCSMC, Vol. 3, Issue. 6, June 2014, pp.306 - 313., URL: http://www.ijcsmc.com/docs/papers/June2014/V3I6201444.pdf

[Sen13] Sen, Jaydip - "Security and Privacy Issues in Cloud Computing", Innovation Labs, Tata Consultancy Services Ltd., Kolkata, India. 2013, URL: http://arxiv.org/pdf/1303.4814.pdf

[Ukil13] Ukil, A., Jana, D., Sarkar A., "A security framework in cloud computing infrastructure", IJNSA, Vol.5, No.5, September 2013,pp 11-24., URL: http://airccse.org/journal/nsa/5513nsa02.pdf

[Agudo11] Agudo, Isaac, Nunez, David, Giammatteo, Gabriele, Rizomiliotis, P., Lambrinoudakis, Costas, "Cryptography Goes to the Cloud", Secure and Trust Computing, Data Management,

and Applications, pp. 190-197. Springer Berlin Heidelberg, 2011., URL: http://www.eng.it/ricerca/file/2011%20Crypto_STAVE.pdf

[Krishna11] Krishna, Vamsee, Yarlagadda, Ramanujam, Sriram, "Data Security in Cloud Computing", Journal of Computer and Mathematical Sciences, Vol.2 (1), pp 15-23, 2011., URL: http://compmath-journal.org/dnload/VAMSEE-KRISHNA-YARLAGADDA-and-SRIRAM-RAMANUJAM/CMJV02I01P0015.pdf

[CSA11] Cloud Security Alliance, "Security Guidance for Critical areas focus in Cloud Computing v3.0", 2011, URL: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[Jain14] Jain, Raj, "Network Access Control and Cloud Security", CSE 571s, Washington University in Saint Louis, URL: http://www.cse.wustl.edu/~jain/cse571-14/ftp/l_16nac.pdf

[Wiki1] "Network Admission Control.", Wikipedia: The Free Encyclopedia. Wikimedia Foundation., URL: https://en.wikipedia.org/wiki/Network_Admission_Control

[Soofi14] Soofi, Amin, Khan, M., Fazal-e-Amin, "Encryption Techniques for Cloud Data Confidentiality", International Journal of Grid Distribution Computing, Vol.7, No.4, pp.11-20 2014. URL: http://www.sersc.org/journals/IJGDC/vol7_no4/2.pdf

7. List of Acronyms

- CSC - Cloud Service Customer/Consumer
- CSP - Cloud Service Provider
- DES - Data Encryption Standard
- DHT - Distributed Hash Table
- IaaS - Infrastructure as a Service
- IBHMCC - Identity-based hierarchical model for cloud computing
- IT - Information Technology
- NIST - National Institute of Standards and Technology
- PaaS - Platform as a Service
- SaaS - Software as a Service
- SAP - SSH Authentication Protocol
- SLA - Service Level Agreement
- SSH - Secure Shell
- VM - Virtual Machine

Last modified on November 30, 2015
This and other papers on recent advances in networking are available online at http://www.cse.wustl.edu/~jain/cse570-15/index.html
Back to Raj Jain's Home Page