ISSN 2286-4822
www.euacademic.org

EUROPEAN ACADEMIC RESEARCH
Vol. III, Issue 11/ February 2016

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

Security Issues in Cloud Computing - Overview

ARIANIT KRYPA
PhD Student
European University of Tirana, Albania
Dr. ANNI DASHO
Associate Professor
European University of Tirana, Albania
ARBËR KRYPA
MSc student
UBT College, Kosovo

Abstract:

Cloud Computing is the new trend in Information Technology in recent years. It has attracted many clients, organizations and businesses due to its advantages of scalability, throughput, easy and cheap access and on demand. Cloud has the potential to eliminate high-cost claims that come from the installation of the IT infrastructure. It provides flexible IT architecture through the internet. This will allow multiple increase capacity or capabilities of the existing and new software. In a cloud computing environment, data stay on a set of network resources, enabling the data to be accessed through virtual machines. Since these data centers can stay in every corner of the world beyond the reach and control of users, there are multi types of security and privacy challenges that must be understood and taken care off. There are various issues that need to be addressed in relation to security and privacy in a cloud environment. This paper aims to summarize the various security issues, such as trust, encryption, identification, confidentiality, data security, ethical issues, cloud vulnerabilities and allocation of resources are shown along with the endeavors made on how to pass these issues.

Key words: Cloud computing, data security, trust, security issues, risks

1. INTRODUCTION

With advancements in technology, information technology infrastructure has completely changed. In the past, organizations or businesses have decided expensive infrastructure to do their daily chores and storage of data. Certainly the data are stored on one or more servers and it has been very costly. There is no doubt that Cloud Computing offers wonderful services with features like flexibility, reliability, data storage, without limitation, fast processing power and foremost cost-free. But security issues are still controversial including: the lack of trust, internal risk malicious, failing cloud services etc.

Cloud computing has emerged around 2008 as a new model of computer distribution in order to achieve profitability. Cloud environments mix virtual techniques in order to provide an efficient route for delivery of resources to the minute. This allows the establishment of a business model pay-for-use, which means the client chooses specifically any source (e.g. Memory, CPU, platform, loads of equipment, etc.) that they require, reducing costs and paying only for it is registered. This paper describes the various security issues of cloud computing, cloud technology base which in itself presents a security risk, security and threats challenges of cloud computing.

1.1. Overview

Cloud computing as a service means the use of information technology resources such as technological equipment (hardware) and software. This type of service is already familiar to us because we are a service user such as email, access to social networks, uploading photos or other data in services like Dropbox or Google Drive, etc.

Cloud computing is defined by the National Institute of Standards and Technology (Mell, P., & Grance, T. 2009) as "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.”

Cloud Computing gives a developed paradigm in terms of on-demand (provisioning) of computing infrastructure. That paradigm converts the location of the physical infrastructure to the network to cut off some costs that are associated with the management of software and hardware resources (Brian, H., et al 2008).

Characteristics of cloud computing include: service on-demand, broad-network access, resource gathering, rapid elasticity and regular service. Requests on-demand means that customers, who are different organizations or companies, can request and manage their resources. Access to the extensive network that allows the services to be provided on the internet or private networks. Resources collected means that clients can extract their data, usually in data centers that are remote. These services can be expanded and scaled differently and regular use of these services billed to customers accordingly and based on requirements.

1.2 Delivery models

Cloud computing can be classified based on services provided and models of distribution. According to different types of services provided, cloud computing can be categorized according to the three types of delivery models (A AlZain and et.al. 2012) (You P., et. Al. 2012):

- **Infrastructure as a Service (IAAS):** Consumers are allocated computing resources in order to run virtual machines that consist of operating systems and applications that are provided as an on-demand service. The best example of IAAS is Amazon.com’s Elastic Compute Cloud (EC2) service. The requirements of security beyond the basic infrastructure are carried out mainly by the cloud consumer.

- Platform as a service (PAAS): Cloud consumers are allowed to write applications that run on the service provider's environment. It is a model of service delivery where the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Google Apps engine is an example of PAAS. The requirements of security are split between the cloud provider and the cloud consumer.

- Software as a service (SAAS): Cloud consumers are provided with various software applications that run over the internet. Google Docs programs are an example of SAAS. The requirements of security are carried out mainly by the cloud provider

In other words, the cloud computing is an assortment of PaaS, SaaS and IaaS. The employees working for an organization can be users or providers of cloud computing services in accordance with the organizational scope and the control over the IT environment (Y. Chen, V. Paxson, R. H. Katz 2010).

1.2.1 Infrastructure as a Service (IaaS)

IaaS is a single holder cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with collocation services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a collocation service (Brodkin. 2008). IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but out of the box IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host (Kuyoro and et.al 2011).

1.2.2 Platform-as-a-Service (PaaS)

PaaS is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. Platform as a service cloud layer works like IaaS but it provides an additional level of 'rented' functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental (Kuyoro and et.al 2011).

1.2.3 Software-as-a-Service (SaaS)

SaaS is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost. The architecture of SaaS-based applications is specifically designed to support many concurrent users (multitenancy) at once. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet (S. Subashini and V. Kavitha 2010).

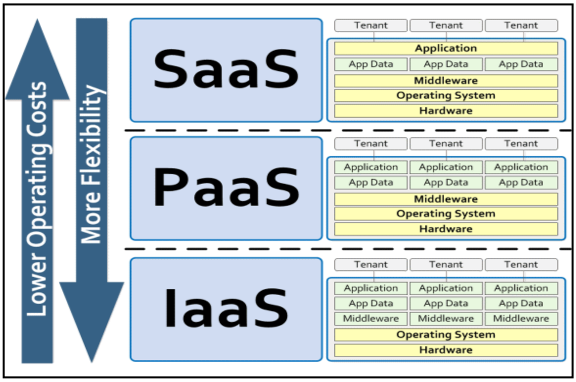


Figure 1: Cloud computing service delivery models (Jesus 2012)

2. CLOUD DEPLOYMENT MODELS

2.1 Public Cloud:

A cloud infrastructure is provided to many customers and is managed by a third party (Grossman 2009).

The infrastructure behind a public cloud is, in general, owned by a cloud provider. A public cloud houses many services from different customers, therefore being accessed from multiple locations by multiple tenants. Web interfaces are commonly used to access the services. This model is based on a pay-per-use business approach and is typically low cost, supplying highly scalable services. The resources of the cloud are located at an off-site location, which turns this model into less secure and more risky than other deployment models, because the service delivery models can be subjected to malicious activities. In this case, Service Level Agreements (SLAs) between customers and providers must be well detailed and analyzed (Fernandes and et.al. 2014).

2.2 Private Cloud:

Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider (Grossman 2009).

This uses the concept of virtualization of machines, and is a proprietary network. A private cloud has a proprietary infrastructure and may be placed within the internal data center of an organization, usually behind a firewall. Thus, the management and security responsibilities are much easier to carry out and identify, which may be in charge of the organization itself or of a third party. In contrast, private clouds encompass big budgets and require highly skilled IT technicians to manage them and improve security, control, compliance, resiliency, and transparency. Off-premises private clouds are expected to grow in 2013, so as to overcome sharing issues and compliance requirements (Fernandes and et.al. 2014).

2.3 Community cloud:

Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider. The community cloud deployment model is the one that is controlled and shared by multiple organizations. Usually, the cloud is setup to support a common interest among the several owners. It may be managed by the owners committee or a third-party organization and may be placed at an on-site or off-site location. The members of the community can freely access the data in the cloud. The community cloud eliminates the security risks of public clouds and the costs of private clouds (Fernandes and et.al. 2014).

2.4 Hybrid Cloud:

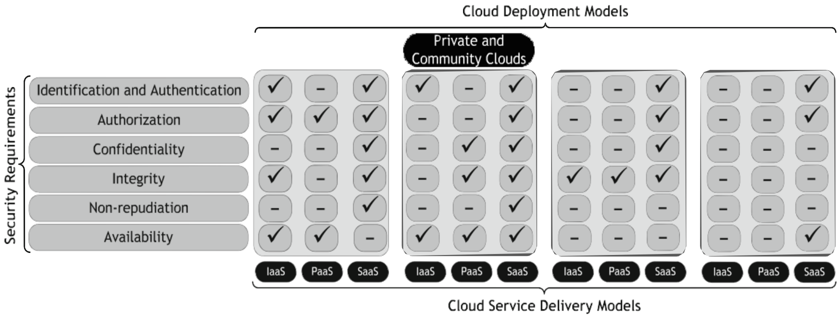
A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other.

A hybrid cloud is a mixture of two or more other cloud deployment models that are centrally managed and circumscribed by a secure network. It is traditionally seen as a mixture of private and public clouds, bringing together the advantages of each one and overcoming their obstacles. It allows multiple, but limited, and well-defined entities to access the cloud via the Internet in a more secure manner than public clouds. It also enables data and application portability. This model is managed by both the organization and a third-party entity and is placed in both on-site and off-site locations (A AlZain and et.al. 2012).

2.5 Virtual private cloud

According to Fernandes et.al. (2014), this last model is mentioned by less sources, and it consists on using Virtual

Private Network (VPN) connectivity to create virtual private or semi-private clouds, resorting to secure pipes supplied by VPN technology and by assigning isolated resources to customers. A VPC seats on top of any model previously described, likewise a VPN that is built upon other networks. Hence, a VPC is a particular case of private cloud existing within any other. This model allows entities to use cloud services without worrying about operating in shared or public environments (Jackson 2010). An example of this model is Amazon *VPC* (Amazon n.d.).



				Private and Community Clouds								
	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS
Identification and Authentication	✓	-	✓	✓	-	✓	-	-	✓	-	-	✓
Authorization	✓	✓	✓	-	-	✓	-	-	✓	-	-	✓
Confidentiality	-	-	✓	-	✓	✓	-	-	✓	-	-	-
Integrity	✓	-	✓	-	✓	✓	✓	✓	✓	-	-	-
Non-repudiation	-	-	✓	-	-	✓	-	-	-	-	-	-
Availability	✓	✓	-	✓	✓	✓	-	-	-	-	-	✓

Figure 2. Security requirements per cloud service delivery model and for the public, private and community, hybrid and VPC deployment models, as established by (Ramgovind S, Et. al. 2010). A check mark (√) means an obligatory requirement in the combination of a specific service delivery model with the underlying deployment model, whereas a dash (-) means optional.

3. CLOUD DEPLOYMENT AND SERVICE DELIVERY MODELS SECURITY REQUIREMENTS

Before choosing a model, businesses should conduct strategic evaluation of each of them. In fig. 2 are summarized six security requirements: identification and authentication, authorization, confidentiality, integrity, non-repudiation and availability. As can be seen on the figure, authorization requirements on IaaS, PaaS and SaaS models on public clouds are mandatory to prevent unauthorized access to assets. The hybrid model requires less properties than the public and private models as it is more secure. Amongst the public, private and community and hybrid deployment models, integrity is a much desired requirement, pointing out the interest in checking data correctness and if it was tampered with or corrupted. In the SaaS model is the majority of the requirements, while the VPC is a less stringent model because a specific part of the cloud is allocated to one customer in an isolated manner.

4. CLOUD COMPUTING CHALLENGES

Moving towards cloud computing seems to be promising but is has to overcome different challenges. Security is a critical issue that worries those considering an external outsource to hold their data and processes (Zissis & Lekkas, 2012).

What Is Security? A "secure" cloud is one that addresses the following information security principles: confidentiality, integrity, availability, identity, authentication, authorization, and auditing. The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC (Kuyoro and et.al 2011), the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are: security, costing model, charging model, Service Level Agreement (SLA), what to migrate and cloud interoperability issue.

5. LITERATURE REVIEW

The security state has been and currently is widely discussed in both the industry and the academia. Several international conferences have focused on this subject alone and several surveys on this area of knowledge have also been published.

Zhou, et.al. (2010) elaborated a survey on the security and privacy concerns of many cloud computing providers. Security and privacy were discussed individually. While the first was studied with focus on availability, confidentiality, integrity, control and auditing characteristics, the second was discussed by listing out-of-date privacy acts. In addition, a few problems related with multi-location storage were also discussed.

According to (Chang and Lai 2012), due to the fact that cloud computing uses the internet, all the security issues related to the internet can occur. This includes fraud and attacks from hackers. These hackers can easily hijack a customer's or user's account. Once this account information has been hijacked they can easily manipulate and steal confidential data of the user. It is the responsibility of the Cloud Service provider to prevent hackers from accessing this confidential user information.

Sensitive data are also not as secure as it would've been if it was physically stored. When data is in the cloud anyone can access it. The Cloud does not differentiate between sensitive data and common data, which means it will enable anyone to access those sensitive data. Which means the data integrity is compromised? The responsibility of ensuring the data integrity becomes the concern of the Cloud service provider (Chen and Chang 2010).

Several solutions were proposed for the security and privacy concerns, of which one was to encrypt the data that was to be uploaded into the cloud. This will however have an effect on the processing requirements on the user end it is also a very complex task to process data in an encrypted format. Encrypting the data will also be very impractical because if your need to search for information through encrypted data it will be increase the computing time required. Cloud service providers are reluctant to change their service to a safer solution, due to the additional processing and memory requirements that will be required to provide a more encrypted solution. Organizations are fully accountable for their own assets with the cloud solution it will be the data that is outsourced to Cloud providers. It is the organizations responsibility to secure the devices that accesses the cloud data. It is the responsibility of the organization to prevent client-side threats such as Web browser vulnerabilities, theft of authentication credentials, virus attacks or data theft (Zissis and Lekkas 2012).

The view of Zissis and Lekkas (2012), are that the assignment of responsibilities is less clear for the data and software that physically reside on the Cloud service provider's site and infrastructure. The cloud model plays an important role in this case; there is a general rule that states that the party that manages and controls an asset is also responsible for providing the suitable security controls to protect it. The Cloud service provider manages and controls the physical infrastructure of the cloud environment. The Infrastructure comprises of the servers, network, human resources and site services. It will be the responsibility of the service provider to ensure suitable infrastructure controls are in place. This will include physical site security, network firewalls and employee training.

The security landscape concerning clouds is wide and the previous works focus on specific areas, paying less attention to the role that clouds play in IT and cyber security, though favoring sometimes the depth of the technical description of the solutions to the problems.

6. SECURITY ISSUES

6.1 Understanding Risks to Cloud Computing

A major concern with cloud computing is that the cloud provider offers the resources in the cloud, that is, the software, platform and infrastructure to the user (cloud consumer). In addition, user data information also resides with the cloud provider. The risk with this type of service is that user information could be abused, stolen, unlawfully distributed, compromised or harmed. There is no guarantee that user's information data could not be sold to its competitor. Unfortunately, this particular risk applies to all the three types of cloud delivery models. Other risks to cloud computing also exist, and range from privacy, data protection, ownership, location and lack of reliable audit standard to data security procedure of most pioneer cloud providers, such as Google, Amazon, etc. According to Rick Gordon of Civitas Group (Gellman 2009), a concern with regard to cloud providers, especially Google Apps includes the lack of reliable security audit standard, data lock-in and Google's opacity regarding its internal data security procedures.

6.2 Trust Issues

Trust in both the traditional IT services and cloud computing must be earned. Trust is a major issue with cloud computing irrespective of the cloud model being deployed. Nevertheless, the cloud like traditional IT services can be secured, protected and dependable. It is believed that the cloud offers security advantages. For example, intruders do not have access to the source code and providers often work hard to provide clean, unbreakable barriers between the customers (Cohen 2009).

However, this requires conscientious effort from both cloud providers and users; in addition, cloud providers must be transparent about their security policies, audit practices, data backup procedures and certification/accreditation. Once users are comfortable with a particular provider's practices, together with the service level agreement (SLA) agreed upon, they are more willing to do business. However, cloud users must be open-minded and must not whole-heartedly trust a provider just because of the written-down service offerings, without carrying out appropriate due diligence on the provider and where certain policies are not explicit, they should ensure that missing policies are included in the service contract. By understanding the different trust boundaries, each cloud computing model assists users when making decision as to which cloud model they can adopt or deploy. For example, with infrastructure cloud computing, a great trust relationship is created because user data backup is possible and applicable, where copies of a user's data are backed up. Similarly, there is a possibility for the user to create and configure additional and customized access controls to protect its data. This level of trust is not possible with software cloud computing, for instance (Cyril 2010).

Software security is, and has been for a while, a vital topic regarding computer systems. Nowadays, security measures might be hard to enforce because common software usually has thousands or millions of lines of code. To make it worse, that software can be written by several people with different programming skills and ideals. Even if all follow a set of pre-specified metrics to develop the software, a single bug can pose a critical problem. In critical and real-time systems, like the ones in airplanes, it is imperative to have fully-reliable software that has passed rigorous software tests so that it does not fail because people lives are at stake in this case. Data, after an extract process, can be transformed into information. A business secret stored in a digital file is, therefore, a high value piece of information. Although there are no lives at stake here, the enterprise revenue can be. Thus, cloud SaaS systems should ensure no data leakage by means of software faults. In spite of being in a more tightly managed environment, software is no more secure simply by virtue of being in a virtualized environment (Pearce, Zeadally and Hunt 2013).

6.3 Data Security

Data seeking is done extremely by many cloud consumers, which can give rise to serious security concerns in cloud environment. There is a critical need to securely store, manage, share and observe enormous amounts of data. It's very important that cloud should be secured enough to maintain the security of data. Exact physical localization of user data in virtual cloud atmosphere is among some of the prime challenges in cloud computing. The major security challenge with clouds is that the owner of the data may not have complete knowledge of where their data are stored (Biswasl and Majumder 2013). Data security involves encrypting the data as well as ensuring that suitable policies are imposed for sharing those data. There are numerous security issues for cloud computing. Some of the major data security issues are (A AlZain and et.al. 2012):

-**Data Integrity**: It is very essential to maintain the integrity of data. The stored data in the cloud storage may suffer from enormous damage occurring during the transition operations from or to the cloud storage provider. The risk of attacks from both inside and outside the cloud provider exists and should be considered.

-**Data Intrusion**: Data Intrusion is another security risk that may occur with a cloud provider. If any intruder can gain access to the account password, then he/she will be able to do any kind of unwanted changes to the account's private documents. Undesirable alteration of user data may commence due to intrusion.

-**Service availability**: Service availability is another major concern in cloud services. It is mentioned in some cloud providers licensing agreement, that the service may be unavailable anytime due to some unforeseen reason. If all the valuable business documents are stored on the cloud and the cloud suddenly goes down, will it be coming back up with all of our important documents intact? It is also important to know whether the company with whom user is storing his vital information is financially steady and will not suddenly vanish taking all of the valuable information with it.

-Confidentiality: Confidentiality of data is another security issue associated with cloud computing. The data should be kept secured and should not be exposed to anyone at any cost. The users do not want their confidential data to be disclosed to any service provider. But it is not always possible to encrypt the data before storing it in cloud.
-Non- Repudiation: Non-repudiation is a major concern for data security. It guarantees the transmission of message between parties and gives the assurance that someone cannot deny something. Non-repudiation is often used for signatures, digital contracts, and email messages. It ensures that a party cannot deny the genuineness of their signature on a document or the sending of a message that they originated.

7. ETHICAL ISSUES IN CLOUD COMPUTING

Cloud computing is based on a paradigm shift with profound implications for computing ethics. The main elements of this shift are: (a) the control is relinquished to third-party services; (b) the data is stored on multiple sites administered by several organizations; and (c) multiple services interoperate across the network. Unauthorized access, data corruption, infrastructure failure, and service unavailability are some of the risks related to relinquishing the control to third-party services; moreover, whenever a problem occurs, it is difficult to identify the source and the entity causing it. Systems can span the boundaries of, multiple organizations and cross security borders, a process called "deperimeterization". As a result of deperimeterization, "not only the border of the organization's IT infrastructure blurs, also the border of the accountability becomes less clear" (Timmermans, et al. 2010).

8. CLOUD VULNERABILITIES

The question of what can be done proactively about ethics of cloud computing does not have easy answers; many undesirable phenomena in cloud computing will only appear in time. However, the need for rules and regulations for the governance of cloud computing is obvious. The term governance means the manner in which something is governed or regulated, the method of management or the system of regulations. Explicit attention to ethics must be paid by governmental organizations providing research funding for cloud computing, private companies are less constrained by ethics oversight and governance arrangements are more conducive to profit generation.

Accountability is a necessary ingredient of cloud computing; adequate information about how data is handled within the cloud and about allocation of responsibility are key elements for enforcing ethics rules in cloud computing. Recorded evidence allows us to assign responsibility; but there can be tension between privacy and accountability, and it is important to establish what is being recorded and who has access to the records.

Unwanted dependency on a cloud service provider, the so-called vendor lock-in, is a serious concern, and the current standardization efforts at NIST attempt to address this problem. Another concern for users is a future with only a handful of companies that dominate the market and dictate prices and policies (Marinescu 2013).

9. CONCLUSION

Today we have many new technologies emerging at a rapid rate, each with the potential of making human's lives easier. Cloud computing technology is one of them. The revolution of cloud has provided opportunities for research in all aspects.

However, we must understand the challenges and security using these technologies. Cloud computing is no exception. We presented the five essential characteristics of cloud computing, cloud service models, and cloud deployment models. In this paper, security issues and challenges are highlighted. Data security and major issues are presented. Security in a cloud environment requires a systemic point of view, from which security will be constructed on trust, mitigating protection to a trusted third party.

REFERENCES

A AlZain, M, and et.al. 2012. "Cloud Computing Security: From Single to Multi-Clouds." *45th Hawaii International Conference on System Sciences (HICSS).* 5490-5499.

Amazon. n.d. *Amazon: Amazon Virtual Private Cloud (Amazon VPC).* Accessed 10 20, 2015. http://aws.amazon.com/vpc/.

Biswasl, Satarupa, and Abhishek Majumder. 2013. "A survey on data security in cloud computing: Issues and mitigation techniques." *International Journal of Research in Engineering and Technology* (IJRET) (02). http://www.ijret.org.

Brian, H., et al. 2008. "Cloud computing. Communications of the ACM." 9-11.

Brodkin., J. 2008. "Gartner: Seven cloud-computing security risks." *Infoworld* http://www.infoworld.com/article/2652198/security/gartner--seven-cloud-computing-security-risks.html. Accessed 10 21, 2015.

Chang, and W Lai. 2012. "The impact of cloud computing Technology on legal infrastructure within internet-focusing on the protection of information privacy."

Chen, and A Chang. 2010. "Information Security Issues of Enterprises adopting the application of Cloud computing."

Cohen, Reuven. 2009. "Lightning knocks out amazon's compute cloud." *@CloudExpo: Blog Post.* 06 11. Accessed 10 15, 2015. http://cloudcomputing.sys-con.com/node/998582.

Cyril, O. 2010. "Security Issues to Cloud Computing." In *Cloud Computing. Principles, Systems and Applications*, by L. Gillam, A. Nick, pp 271-279. Springer.

Fernandes, Diogo A B, and et.al. 2014. "Security Issues in Cloud Environments - A Survey." *International Journal of Information Security (IJIS)* 113-170. doi:10.1007/s10207-013-0208-7.

Gellman, Robert. 2009. *Privacy in the clouds: risks to privacy and confidentiality from cloud computing.* World Privacy Forum. 2 23. Accessed 11 10, 2015. http://www.worldprivacyforum.org/www/wprivacyforum/pdf/WPF_Cloud_Privacy_Report.pdf.

Grossman, R. L. 2009. "The Case for Cloud Computing." *IT Professional vol 11 (2), ISSN: 1520-9202,* pp. 23-27,. doi:10.1109/MITP.2009.40.

Jackson, C. 2010. "8 Cloud Security Concepts You Should Know." *Network World.*

Jesus, Jose de. 2012. "Navigating the IBM cloud, part 1: A primer on cloud Technologies." *IBM Middleware Technical Journal for Developers.* Accessed 10 21, 2015. http://www.ibm.com/developerworks/websphere/techjournal/1206_dejesus/1206_dejesus.html.

Kuyoro, S.O, and et.al. 2011. "Cloud Computing Security Issues and Challenges." *International Journal of Computer Networks (IJCN), Volume (3) : Issue (5).* 247-253.

Marinescu, Dan. 2013. "Cloud Vulnerabilities." In *Cloud Computing. theory and practice.*, by Dan Marinescu, pp 1-19. doi:doi:10.1016/B978-0-12-404627-6.00001-4.

Mell, P., & Grance, T. 2009. *The NIST definition of cloud computing.* National Institute of Standards and Technology, Information Technology Laboratory, U.S. Department of Commerce. Accessed 11 10, 2015.

http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Pearce, M, S Zeadally, and R Hunt. 2013. "Virtualization: Issues, Security Threats, and Solutions." *ACM Comput. Surv.45 (2),*. doi:DOI 10.1145/2431211.

Ramgovind S, Et. al. 2010. "The management of security in cloud computing." *Information Security for South Africa* pp.1-7. doi:10.1109/ISSA.2010.5588290.

S. Subashini and V. Kavitha. 2010. "A survey on security issues in service delivery models of cloud computing." *J Network Comput Appl.* doi:10.1016/j.jnca.2010.07.006.

Timmermans, J, V Ikonen, B Stahl, and E Bozdag. 2010. "The ethics of cloud computing. A conceptual review." *Proc IEEE 2nd Int. Conf. on Cloud Computing Technology and Science.* 614–620.

Y. Chen, V. Paxson, R. H. Katz. 2010. *What's New about Cloud Computing Security?* Technical Report No. UCB/EECS-2010-5,, Electrical Engineering and Computer Sciences University of California at Berkeley.

You P., et. Al. 2012. "Security Issues and Solutions in Cloud Computing." *Proc. of 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW)* . 573-577.

Zhou, M., et.al. 2010. "Security and Privacy in Cloud Computing: A Survey." *6th Int. Conf. on Semantics Knowledge and Grid.* Washington, D.C., USA: IEEE Computer Society,. pp. 105.

Zissis, D, and D. Lekkas. 2012. "Addressing cloud computing security issues." *Future Generation Computer Systems* 28. doi:http://dx.doi.org/10.1016/j.future.2010.12.006.

ABOUT THE AUTHORS:

ARIANIT KRYPA has graduated the Faculty of Education – Technology & Informatics in 2010 and economic Master degree in 2013. He is PhD candidate at Faculty of Economics – Management Information Systems in European University of Tirana (UET). Founder and owner of "Design Kibernetika" a computer shop in Kosova where the main work is presenting the new technology. His work in PhD thesis is focused on adoption of cloud services from SME's with their implication in economic growth of Kosova.

DR. ANNI DASHO is working as an Associate Professor and Executive Director of IT solution center at European University of Tirana, Albania. Has a vast background of working experience in different areas in Albania as a Lecture in different Faculties, as a Director of Projects in CEZ Albania for Dara Cleaning etc.

ARBËR KRYPA has graduated at the Faculty of Electrical and Computer Engineering, Department of Telecommunications in 2011. He is MSc candidate at UBT College, Department of Computer Science and Engineering. His work in master thesis is focused on adoption of cloud services in higher education institutions. Arbër works at the University of Gjakova as electronic systems and computer network administrator.