International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(3): 1-17
The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)

Assessing Database and Network Threats in Traditional and Cloud Computing

Katerina Lourida[1], Antonis Mouhtaropoulos[2], Alex Vakaloudis[3]

[1] Informatics Department
DEI College
Thessaloniki, Greece
katerina.lourida@gmail.com

[2] Department of Computer Science,
University of Warwick,
Coventry, UK
a.mouhtaropoulos@warwick.ac.uk

[3] NIMBUS Centre
Cork Institute of Technology
Cork, Ireland
avakaloudis@hotmail.com

ABSTRACT

Cloud Computing is currently one of the most widely-spoken terms in IT. While it offers a range of technological and financial benefits, its wide acceptance by organizations is not yet wide spread. Security concerns are a main reason for this and this paper studies the data and network threats posed in both traditional and cloud paradigms in an effort to assert in which areas cloud computing addresses security issues and where it does introduce new ones. This evaluation is based on Microsoft's STRIDE threat model and discusses the stakeholders, the impact and recommendations for tackling each threat.

KEYWORDS

Cloud computing, STRIDE, security evaluation, security threats, web security, threat assessment

1 INTRODUCTION

Security has been a significant activity of the society from the early ages but today the issues around security have developed and become even more complicated. Even more, the nature of data and information has radically changed, as today we are dealing with information on a digital form rather than written on paper information. A few decades ago papers were locked in office cabinets with a key and were considered safe and secure to unauthorized access. Nowadays the case is different as digital data cannot be so easily handled and controlled. Due to this transformation of information, the notion of security has also been redefined and constantly modernized to line with new security needs and requirements. What is more, the way communication has been evolved today makes things even more complicated. Bearing in mind the invasive manner that the World Wide Web has brought in everyday life perplexes the way information is being transmitted. Information security thus, is crucial not only to individuals but in business also. Business today is more depended on information and thus on information systems while the growth of e-commerce has made security a mandatory task to all businesses no matter their size. Furthermore, the expansion of the boundaries of an organization makes the need of security even more compulsory as there is more in stake than securing data on premises. From all of the above, it can clearly be concluded that information security has become a business issue, which no organization can neglect.

Cloud computing is considered to be a revolution in the computing industry and large organizations are already implementing and providing such services. Cloud computing is innovating as it offers services such as data storage,

applications, servers and more from online resources. This can benefit individuals and enterprises as it enables users to access applications from anywhere without having to install them, while the expenditure on hardware and software is significantly reduced and therefore more cost effective.

Security can be an issue in cloud computing especially when dealing with sensitive data stored in databases [1]. Users are significantly dependant on the providers of such services in order to maintain data privacy and accessibility. Thus, security can be exceptionally challenging in cloud computing as it may affect quality, efficiency and success of the services.

Today, the "cloud computing" term is not only used by IT professionals, but by the business society and individuals as well. The term refers to a computing paradigm, which apparently has come to stay. It is considered evolutionary as it can affect all aspects of life as it can fulfil from simple tasks like email services, to even more demanding ones such as governmental services, health services and more. Cloud computing has already managed to benefit developing nations like India, South America and Africa, while facilitating access to highly advanced technological hardware and software. In India, the Apparel Export Promotion Council developed a cloud platform to offer services to more than 11000 members. Steve Bratt, the CEO of Non Profit World Wide Web Foundation has stated that *"*It has the potential to level the playing field because it breaks down barriers to entry" and "It's a catalyst for a wave of innovation and change in developing nations [2].

However, the European Commission acknowledges that "Cloud technologies and models have not yet received their full potential" [3] identifying this way how promising this field can be but at the same time recognizing the gaps that need to be filled in order to achieve full potential. The European Commission identifies technological and non-technological gaps. The technological gaps include issues about security and data handling which is considered a core task of cloud security.

According to [4], nearly one third of the organizations are thinking about moving their services to the cloud. However, some organizations show reluctance and uncertainty on migrating to a cloud environment. One of the most significant issues they have is the security drawbacks that cloud computing brings together which is an issue that will be examined in this report.

In [5] cloud security concerns are classified in three categories namely, traditional security, availability and third party data control and the same work concludes that current controls are not adequate to secure data storage so they should be enhanced and improved. The fact that cloud computing utilized different types of service models (IaaS, PaaS, SaaS) makes it even more complex in security terms. In [6] cloud security is examined in each service model and proposes that each model should be placed to a different security level. On the other hand, Cloud Security Alliance [7] uses a taxonomy of fifteen security domains to reflect on cloud security. In the research report of [8] four point criteria are proposed for a vulnerability to be defined as cloud specific and concludes that several risks should be considered before moving to

the cloud and the responsibility of mitigating these risks belongs to both client and provider. In the research conducted by [9] the findings conclude the significance of security in cloud environment and the aim of the paper is to help users to identify threats related to the use of cloud services.

Given the aforementioned differences between security in cloud computing to security in conventional computing, this paper is intended to:

- **a)** Give an overview of the information security background
- **b)** Evaluate cloud computing security characteristics
- **c)** Assess the risk assessment process in the cloud.
- **d)** Conduct a threat assessment analysis in cloud computing in order to understand the variability between the traditional and cloud computing background.

This paper is structured into five sections. The current section introduced the reader to the concept of cloud computing and cloud security concepts. The next section (section 2) defines cloud computing characteristics and categorizes it according to service and organizational needs. Section 3 identifies all cloud computing related threats, which are then mapped according to Microsoft's STRIDE Threat Model. In section 4, we present the results of a threat assessment analysis, where threats are classified into eight different categories. In this section each threat type is assessed based on attacks, impacts, stakeholders, and recommendations. The last section (section 5) concludes the paper and proposes areas for further research.

2 CLOUD COMPUTING OVERVIEW

Cloud computing is defined [10] by the following five characteristics:
a) on demand self service, which focuses on the fact that cloud clients can access resources from the cloud whenever these are required without the need to interact with a human,
b) broad network access, which refers to the network based mode of cloud computing and that client's cloud resources are accessible from any standardized platform such as smart phones, tables, personal computers etc.,
c) resource pooling, which refers to the multi-tenant model of the cloud in a sense that the provider offers resources to multiple clients at the same time and that the same resources can be shared simultaneously to multiple users,
d) rapid Elasticity reflects to the capability of cloud clients to utilize resources from the resource pool in the cloud when they require them and to release them back to the pool when they no further need them,
e) measured service refers to the fact that the cloud provider charges services as per usage metrics.

Cloud computing can also be categorized according to their service model. There are three basic service models:

- Infrastructure as a Service (IaaS),
- Platform as a Service (PaaS),
- and Software as a Service (SaaS);

each one of the above models has its own approach and characteristics. Depending on the needs of the client the appropriate model is selected and implemented. The categorization of cloud computing models is currently a

topic of considerate analysis [1][3] as each of the three models listed above, commonly contains a number of subsets.

Infrastructure-as- a-Service (IaaS) or Hardware-as-a-Service

This model is commonly used by system managers or IT architects that have greater needs in hardware and physical machines in order to be able to meet growing needs of their applications. IaaS model provides the client with the entire infrastructure and computing power for their business needs. The client rents the physical resources from the IaaS provider and maintains control of applications, storage, middleware and operating systems. This model involves two subsets: the Network-as-a-Service (NaaS) and the Storage-as-a-Service (STaaS). Both of the subsets are part of the lower levels of the cloud service.

Platform-as-a-Service (PaaS)

The model is usually the choice of developers and it facilitates them to deploy their applications on the provider's platform. PaaS provides the client with an application-hosting environment (e.g. Windows, Android, Linux and more) while the developer rents some software, hardware and infrastructure in order to run his own applications and data. This model includes the Backend-as-a-Service (BaaS) model, the Database-as-a-Service (DBaaS), and the Integration-Platform-as-a-Service (IPaaS). These subsets involve databases, mobile application developments, and platforms.

Software-as-a-Service (SaaS)

This model is used on our everyday life and usually is accessed via a web browser. The consumer purchases their access to applications and services that the cloud has to offer. The SaaS model removes any concerns of the client for servers, storage, and networks. By the use of an Internet connection and a web browser or program interface the client can log in to the cloud and access various services offered by the provider. The client has no control of any of the underlying infrastructure of the applications while the provider has total control of middleware, operating systems and hardware [10] [11].
This model includes the Data-as-a-Service (DaaS), the Integrated-Development-Environment-as-a-Service (IDEaaS), and the API-as-a-Service. All of the above sub models involve services of higher levels in the application stack.

Even though the basic threefold categorization is detailed above, some of the subsets do not lay in a single category but can fall into two categories. Such subsets are the following: a) Security-as-a-Service (SECaaS), both a PaaS and a SaaS component, b) Desktop-as-a-Service (DTaaS), both an IaaS and a SaaS component, and the 3) Test-Environment-as-a-Service (TEaaS), both an IaaS and a PaaS component

Additionally, cloud computing is categorized into four deployment models [7], where according to the organization's needs the appropriate model can be selected:

Private Cloud

The cloud infrastructure is used only by a single and specific organization thus client dedicated. It can be managed or owned by the organization or by a third party, on or off premises.

Public Cloud

The infrastructure of the cloud is shared to the public or to a business group and can be owned by an organization or a

third party on the premises of the cloud provider.

Community Cloud
The infrastructure of the cloud is shared between several organizations, which may have similar scopes, missions or compliance requirements and it can be owned by an organization or a third party, on or off premises.

Hybrid Cloud
The infrastructure of this model is a combination of two or more of the public/private/community clouds, which work together as an entity in order to enable data portability.

3 CLOUD RISK ASSESSMENT PROCESS

The identification and evaluation of all risks is a critical task within the implementation of the appropriate information security framework by an organization. A risk is composed of a threat, a probability and an impact [12]. Risks are in various forms and not all risks are likely to exist in all IT systems or businesses. Each system has its own risks, and thus it is important to have a clear scheme of the business and risks involved to the specific system before applying any security controls. No matter the categorization, risks may overlap each other due to the nature of business today and the IT involvement. There are different types of risks: a) organizational, b) technological, and c) legal. Following, figure 1 depicts a representation and taxonomy of risks.

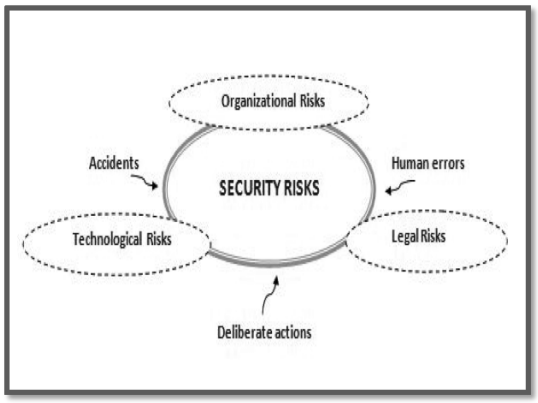

Figure 1. Security Risks

a) Organizational Risks: Organizational risks include risks that may compromise the security of a business structure. Examples: Loss of reputation, loss of share value.
b) Technological Risks: Risks of this type comprise failures or losses, which are associated with the use of technological services such as design, engineering, processes, and procedures.
c) Legal risks: With the term of legal risks we include all issues that may occur in an organization due to legislations and regulations. For example, countries have different legislations for data privacy and this can lead to discrepancies.

What is more, damages caused by human errors or accidents (e.g. nature disasters), which are unintentional, are also considered as a risk while deliberate and intentional actions from entities yearning to harm a business or IT system have a great share today (e.g. criminals, hackers).

On the other hand, there are three main categories of threats [13]: a) Network threats refer to attacks on the network system. Attacks of this type are spoofing, sniffing, denial of service. b) Application threats which refer to

attacks on the application layer. Such attacks include SQL injection, buffer overflows, cross-site scripting and more c) Host threats which refer to attacks on the software of a system. Such attacks include malware (viruses, Trojan, worms), port scanning, and Denial of Service (DoS).

3.2 The STRIDE Threat Model

Various threat models have been designed and proposed in order to help clarify and categorize threats. A widely used threat model is Microsoft's STRIDE [13,14].

STRIDE is used in order to classify threats in the following six categories: Spoofing, Tampering, Repudiation, Information Disclosure, denial of service and elevation of privilege. The model also suggests some countermeasures in each category, which can be applied to mitigate the threats. Today, STRIDE is considered as a broad threat model and can be used to provide a wider and a more general idea of how threats can be identified.

The model depicted in Table 1 classifies threats according to the STRIDE model along with the countermeasures proposed. However, for the purposes of cloud computing the responsible party for applying countermeasures should be identified. The responsibility differs in the services, IaaS, PaaS and SaaS due to the fact that IaaS provides Infrastructure alone, PaaS the platform while SaaS provides software solutions as well. According to the following threat model, in the IaaS service the provider is responsible only providing availability of services while a shared responsibility is depicted in authorization techniques. However, in PaaS things are different as everything is a shared responsibility between cloud provider and cloud client. Still, the cloud client is responsible for not disclosing any information such as passwords while the prevention of DoS still remains a cloud provider responsibility. On the other hand, in SaaS the only difference between SaaS and PaaS is the fact that the cloud provider is the only responsible for applying authorization techniques to prevent the escalation of privileges.

Table 1. Cloud Threat Model

Threat	Countermeasure	Responsible in IaaS	Responsible in PaaS	Responsible in SaaS
Spoofing	Authentication techniques	Cloud Client	Cloud Provider Cloud Client	Cloud Provider Cloud Client
Tampering	Digital Signatures	Cloud Client	Cloud Provider Cloud Client	Cloud Provider Cloud Client
Repudiation	Auditing	Cloud Client	Cloud Provider Cloud Client	Cloud Provider Cloud Client
Information disclosure	Encryption	Cloud Client	Cloud Client	Cloud Client
Denial of Service (DoS)	Monitoring Provisioning	Cloud Provider	Cloud provider	Cloud provider
Elevation of privilege	Authorization	Cloud Provider Cloud Client	Cloud Provider Cloud Client	Cloud provider

4 THREAT ASSESSMENTS

In order to be able to understand in what extent security is changed or transformed in a cloud computing setting and how threats and attacks are perceived in a virtualized environment, a comparison between various threats in traditional and cloud computing is being held. Thus, the following threats are analyzed: a) Data threats, b) Physical threats, c) Interface threats, d) Authentication threats. These four types of threats (Table 2) are more traditionally oriented. The next four types (Table 3), which can be considered more as cloud specific threats e) Cloud power threats, f) Virtualization threats, g) Outage.

4.1 Data Threats

Attacks: Nowadays, more and more businesses are dependent on digital information and thus it is of great significance to appropriately control, store and backup data. The threat of data loss or integrity loss is present in traditional computing today more than ever and that is why organizations today invest a lot of its security budget to apply adequate controls for data storage and management. Known attacks that compromise the data lifecycle includes cracking authentication credentials, SQL injections, privilege escalation or exploiting unpatched database vulnerabilities, human errors, and loss of encryption keys. The same threats seem to appear in the cloud environment. However, it seems that the cloud increases this threat as the amount of data transmitted and need to be managed also increases.

The nature of communication in the cloud, which uses the Internet as the medium, can in fact widen the risk of data loss or leakage. Therefore, cloud environment should be enhanced with stronger authentication and encryption

Table 2. Traditional Threats Classification

	Attacks	Impact	Stakeholder	Recommendations
Data	SQL injection Unpatched databases Loss of encryption key Privilege escalation Malicious insiders	Confidentiality Integrity	Cloud provider IaaS PaaS SaaS Cloud client	Strong encryption algorithms Regular backup strategies Access Controls Strong key management Regular patching
Physical	Nature disasters Malicious insiders	Confidentiality Integrity Availability	Cloud provider IaaS PaaS SaaS	Recovery planning Access control in buildings Backup strategies
Interface	Malicious attack on low-level security applications Malicious attack on insecure browsers	Confidentiality Integrity Availability	Cloud provider IaaS PaaS SaaS Cloud client	Strong authentication Access Controls Encryption methods
Authentication	Phishing Human accidents Social engineering Key loggers Eavesdroppers Malicious code Man-in-the middle	Confidentiality Integrity Availability	Cloud provider IaaS PaaS SaaS Cloud client	Strong authentication Security policies Monitoring Auditing logs Encryption methods Firewalls Intrusion Detection system Antivirus Client awareness

techniques, backup techniques while clients should be appropriately aware of the issue to avoid leaks of IT credentials or social engineering type of attacks. The impact of data leakage or data loss could be disastrous for an organization as it may depend heavily on the privacy of sensitive data.

It is important to mention at this point that the threat of loss of data confidentiality is not the same in all cloud models. In IaaS customers create infrastructure in the cloud thus reducing the threat, whereas in PaaS customers make use of Web and Mail Servers in the cloud, which increases the threat as the control of data is limited. In SaaS the security of data lies on the cloud provider.

An additional security concern that the nature of cloud paradigm seems to produce, in terms of data control is the fact that because of the lack of visibility things are more complicated. In the majority of traditional computing the users have the data storage hardware and databases on their own premises. It is their responsibility to adequately secure data from unauthorized access or damage and to follow regular backup methodologies. Nevertheless, when it comes to cloud computing the data are stored and managed by the provider who is considered to the organization a third party. Thus, this may cause insecurity to the client, as he has no control on its own data.

Furthermore, the risk of data exposure or damage is present, as the client unlike traditional IT departments, has no knowledge or interference on the personnel who will be managing their data. If for any reason data is exposed from malicious insiders in the cloud provider, the impact on the client could be devastating not only in terms of financial or reputation loss but on the legal aspect as well bearing in mind that the majority of large organizations need to comply with privacy laws. Thus, sensitive data could be vulnerable to an adversary if appropriate measures are not taken.

Auditing techniques are easier to be implemented on an organization's own premises rather than on the cloud due to the architecture complexity. Especially when bearing in mind that auditing is a requirement for compliance with legal regulations laws, the issue is bigger than someone would assume. In response, some guidelines have emerged in order to help auditors on how to assess cloud services, SAS 70 (Statement on Auditing Standards**)** [15] being one of the most widespread, while SOX (Sarbanes-Oxley Act) and HIPAA (Health Insurance Portability and Accountability Act**)** are also gaining grounds for cloud auditing assistance [5].

The assurance that data is being stored and managed securely falls to the trust that the provider applies appropriate measures for the issue [16] . It is important for the client to know beforehand how the cloud provider deals with this issue and appropriate legal agreements should reflect on the matter.

Finally, the cloud data lock-in can also be considered as security issue. The issue emerges the instant a client wishes to change cloud provider or even when a cloud provider decides to cease operation. What really happens to their data, how are they transported to the other provider and how sure is the client that the initial cloud provider erases all data and not use them adversely against them are some of the questions that arise when dealing with data security. Obviously such matters do not apply in the traditional data management as organization own, control and manage their data on premises. However, this can be of an additional burden to the conventional organization, as they need to invest more on database servers, data storage machines and security controls for keeping data safe. On the other hand, when data is handled in the cloud, less data is stored on the premises of the client and thus there is less concern for data loss.

Stakeholders: The matter is an issue for both cloud providers and clients. All three-service models are affected: IaaS, PaaS, SaaS.

Impact: The impact is severe in confidentiality and integrity of data. Especially if realizing that most businesses which have to manage personal data need to comply with privacy laws and regulations. Thus any data compromise can have legal implications as well.

Recommendations: Strong encryption algorithms should be applied during transmission and storage of data. Backup strategies are significant and should be adopted by cloud providers. Moreover, strong key management, access controls

are also suggested for dealing with threats of this kind.

4.2 Physical Threats

Attacks: Physical threats are certainly met in both conventional computing and cloud environment. As physical threats we refer to the occasion in which assets of an organization are damaged due to human accidents, malicious attacks or physical disasters. Types of physical attack range from a laptop theft, a window left open on the server building on a rainy day, to an earthquake or fire burst.

As far as traditional computing is concerned, most of the physical machines are located on its own premises and thus if no appropriate security measures are taken then hardware and machines can be damaged. An appropriate security policy and risk assessment would probably minimize such risks. The same concerns however trouble the cloud environment. The locations in which the infrastructure and servers are held should also be protected by all kind of physical risks. The main difference though is that in the cloud environment, the cloud provider can have more powerful barriers and controls to protect assets compared to the smaller organization that needs to invest capital on additional controls for physical threats. Nevertheless, if a physical attack is detected on the cloud and disaster planning is not efficiently in place then the impact could be huge and catastrophic for a great number of the cloud's clients.

Stakeholders: Attacks of this kind affect mainly cloud providers. All three models of service are affected.

Impact: The attack can affect all three principles of security, confidentiality, integrity and availability as physical machines can be stolen or damaged.

Recommendations: In response, cloud providers can design the physical architecture of their buildings where equipment is held, in such a way that they are of great physical distance from each other and thus damages which could expand are limited to a single point. Needless to point out, that backup methodologies used in cloud services should be regular and prompt in order to mitigate the risks and impacts if such an attack is detected.

4.3 Interface Threats

Attacks: The security of interfaces and application is an issue relevant both to traditional and cloud environment computing. In traditional systems the security policy should ensure that authentication and access controls are implemented in an adequate level of security. Interfaces and applications should be monitored to detect any discrepancies while encryption techniques should be applied upon request transmissions. The difference in cloud systems is the fact that the various layers of applications make monitoring and provisioning more complex. From a traditional point of view, current browser-based authentication protocols are insecure for cloud environment [9].

In a cloud environment, as organizations rely on cloud services to provide services and solutions to third party entities, the process is even more risky since credentials may be provided to a third party. A cycle is constructed by a

different organization, which may be using the same credentials and same services and it is especially difficult to ensure that authentication permissions are not violated and that monitoring of various interfaces is efficient.

Stakeholders: This is an issue for both cloud providers and clients. The client should understand how the cloud environment is organized. The attacker can gain access from the client's application or interface thus finding a path to the infrastructure of the provider. The security issue to the interface is present in all three-cloud models as they all use an interface in order to access the cloud services.

Impact: Comparing, both traditional and cloud systems have security issues with the authentication and access control to a service via an interface. However, the impact in virtualization environment is more severe as it can affect confidentiality, integrity and availability at all levels. It can affect databases and services in the cloud, while co-tenants can also be influenced by this type of attacks.

Recommendations: In order to mitigate risks strong authentication and access controls are suggested in both providers and clients.

4.4 Authentication Threats

Attacks: Authentication techniques are core security tasks in organizations no matter if we are referring to cloud or traditional computing environments. The risk remains the same in both paradigms and the main difference is focused on the impact a successful attack may have. Due to the fact that cloud environment uses multi-tenant architecture, successful attacks such as phishing, malware and software vulnerabilities exploitation may compromise multiple services and clients. On the other hand, in traditional computing environment such a compromise is restricted to the organization assets. It is worth mentioning at this point, that because cloud providers have the computational power with advanced technological hardware and professionals with high technical skills, it is easier for them to apply strong encryption and access control techniques.

Therefore, in comparison both traditional and cloud services suffer from authentication threats however it is the nature of their architecture that makes cloud services more vulnerable in case of a compromise. However, the cloud overmatches traditional systems in prevention and detection techniques due to their large computational power.

Stakeholders: The matter is an issue for both cloud providers and clients. Especially in the cloud providers, an authentication compromise could affect multiple clients due the multi-tenancy level of services. All three-service models are affected: IaaS, PaaS, SaaS.

Impact: The attack can affect all three principles of security, confidentiality, integrity and availability. An attacker can gain unauthorized access to a resource and damage the whole provider's infrastructure and services.

Recommendations: In order to mitigate risks, strong authentication and access controls are suggested in both providers and clients. However, it is crucial to adopt appropriate training programs in

order to make clients aware of the different security aspects and how they can protect their assets. Security policies should be clear and communicated to everyone involved.

4.5 Virtualization Threats

Attacks: Unlike traditional computing, cloud services highly depend on the virtualization paradigm. The benefits of virtualization however, come with security concerns due to virtual machine attacks. Cloud environments make use of hypervisors [17] as in IaaS infrastructure is provided which however does not ensure isolation in its components.

Stakeholders: Attacks of this kind affect mainly cloud providers. Because of the multi tenant architecture of the cloud, a compromise on the hypervisor could affect more than one tenant on the same platform. IaaS models are mostly affected.

Impact: Hypervisors on their turn have their own vulnerabilities, which can give attackers privileges in terms of security control levels, on the shared platform of the cloud environment.

Recommendations: It is strongly advised for cloud providers to implement monitoring, firewalls, regular patching, scanning and compartmentalization [7].

4.6 Cloud Power Threats

Attacks: The denial of service attack is considered one of the most common attacks on computer systems and IT environments. The DoS attack in traditional systems focuses mainly on making a resource unavailable to other legitimate entities. DoS attacks are typical and widespread in traditional computing and the use of firewalls and intrusion detection systems can be applied to control such attacks. However, the question that remains is how a DoS attack is different in a cloud environment.

In terms of Cloud computing a DoS attack is still considered possible in services provided. It could be easily assumed that it is easier to recover from a DoS attack in the Cloud paradigm due the continuous provision of resources which is typically implemented by the cloud provider. However, the impact of a DoS attack, which is not treated appropriately, may be more catastrophic than the impact a DoS attack may have on a traditional computing system. A DoS attack in the cloud environment is launched similarly to the typical DoS attack, yet the attacker may select a client's cloud application which consumes large amount of resources and by using low-bandwidth attacks he can take down cloud services. DoS attacks in cloud environment are more sophisticated as the focus on application infrastructure. At this point it should be reflected that one of the main characteristics of cloud computing is resource pooling, meaning that resources are not dedicated to one client but a service is available to multiple clients. Therefore, a denial of service attack may affect services for multiple customers who are hosted on the same platform. This indeed may cripple the cloud services and multiple organizations while at the same time revoking the unique feature of cloud computing, resource pooling. Such types of attacks are closely related to a cloud specific threat proposed by the Cloud Security

Table 3. Cloud Specific Threats

	Attacks	**Impact**	**Stakeholder**	**Recommendations**
Virtualization	Hypervisor vulnerabilities	Confidentiality Integrity Availability	Cloud provider IaaS	Monitoring Firewalls Regular patching Scanning Compartmentalization
Cloud power	DoS Malware Malicious insiders	Availability	Cloud provider IaaS PaaS	Strict registration process Monitoring network traffic Intrusion detection system Firewalls Antivirus
Downtime	Network failures Hardware failures Power failures Software failures	Availability	Cloud provider IaaS PaaS SaaS	Recovery planning Backup strategies

Alliance labelled as "the abuse and nefarious use of cloud computing" [7].

Stakeholders: This threat mainly affects IaaS and PaaS models as the attacker can launch an attack on a cloud application layer. The fact that cloud providers offer great computer power and resources easily accessible by a credit card can be taken advantage of by hackers. Even more, the fact that anyone can register to use the cloud services for a trial period providing the attacker with the ability to access the cloud environment with the minimum of effort or anonymously. The adversary can thus use the platforms to perform not only DoS attacks but also any malware intrusions they require.

Impact: The main purpose and goal of the attacker remains the same, to disrupt the availability of a service, yet the impact of a DoS attack in a cloud environment can indeed be more disastrous as it can affect more than one client. The significance of this can be even more realized if we consider that various critical mission organizations may make use of cloud services.

Recommendations: Implement stronger registration processes and more sophisticated methodologies for monitoring client's network traffic. Concluding, DoS type attacks are possible both in traditional and cloud computing.

4.7 Outage and Downtime Threats

Attacks: In all types of infrastructure, even if we are talking about traditional, distributed or cloud environment, there is the likelihood of a downtime. This for example may be the result of the electricity going down, system failures, network failures and more.

Stakeholders: Attacks of this kind affect mainly cloud providers. All three models of service are affected.

Impact: Someone would imagine that organizations with extensive computational and financial power as a cloud provider could more easily and more efficiently protect assets from such threats. Still, the bigger the size and growth of the organization then the

Table 4. Threat Comparison (Traditional vs. Cloud Environment)

	Traditional	Cloud
Data Control	- Full control of data - Additional capital investment - Data management is the organization's responsibility.	- Limited control of data - Data spread to many data servers. Difficult to locate them. - Data Lock in
Data Loss	- All data can be compromised, as data are stored on premises. - Additional capital investment	- All data transmission is done through the Internet thus making loss of data more probable. - Strong encryption techniques can be provided.
Data exposure	- More easily managed as access to data is monitored and controlled. - Additional capital investment	- No control on who can access the data. Need to trust the provider. - Legal agreements between clients and providers are essential. - Strong authentication can be provided
Network	-Full control of network infrastructure -Limited dependency on global outages	-Impact can be severe -Need for redundancy infrastructure
Physical	- Additional capital investment - Costly to recover - Regular backups needed	- Impact can be severe - Need for physical architecture to build storage and server rooms in distance from each other. - Regular backups needed
Interface Application	- Easier to monitor - Easier to train personnel for awareness.	- Difficult to control due to multi-tenancy and resource pooling characteristics. - Impacts can be severe due to shared platform. - Current browser authentication protocols are insecure. - Issue for both clients and cloud providers.
Development Environment	- Easier to monitor - Easier to train personnel on use	-No control on source code accessibility -Exposure to security bugs on the IDE
Authentication	- Breach remains on premises. - More controllable - Additional capital investment.	- Multiple clients affected by the shared services. - Strong authentication and access controls can be provided.
Virtualization	- On premises environment. - Not affected by virtual machine vulnerabilities.	- Hypervisor vulnerabilities can affect multiple tenants of the shared platform.
Cloud power	- DoS attack : - Disrupt services - Limited to single point of attack. - Additional capital investment	- DoS attack: Disrupt services - More sophisticated attacks. - Abuse of cloud power - Multiple organizations affected due to multi-tenancy characteristic. - Impacts can be severe due to shared platform. - Complex to provision but computational power and high technical skills of personnel simplifies it.
Downtime	- Backup techniques required - Disaster planning required	- Backup techniques required - Disaster planning required - Can affect third party services

bigger the impacts and losses are on such an occasion.

Recommendations: The complete elimination of downtime is impossible for any organization which may design and implement policies for preventing

such incidents while recovery plans should be provisioned for immediate launch in such occasions.
Based on the previous analysis on the different threats met in cloud and traditional computing the following table (Table 4) can be derived which depicts all of the differences. Data can be expanded in data control, data loss and data exposure as data is significant in all terms and can be interpreted variously.

5 CONCLUSIONS

Computing is constantly advancing to new forms and structures in order to provide even more ways of dealing with everyday or more demanding tasks. ICTs are moving towards cloud computing solutions even though there is still reluctance from various organizations mainly due to security issues. However, the vulnerabilities of cloud computing and as far as security is related are yet to be fully explored. As more information technologies engage to cloud environments the background will be more clarified. Due to the nature of cloud computing and its unique characteristics some security vulnerabilities can emerge which are not considered as an issue when dealing with traditional computing or they are transformed acquiring a different structure.

In traditional security, policies and controls can be more easily applied as all assets are known, risks can be more clearly identified and thus more controllable measures can be adopted to mitigate the risks. When it comes to cloud services however, things are different. Surely threats and attacks concerning traditional systems are also applicable in the cloud environment; but are there any other concerns regarding security when interacting with the cloud? For this purpose, the use of a cloud threat model might prove to be helpful.

There is no right answer whether traditional computing or cloud computing is better in terms of security. Certainly, cloud computing is still in the process of evolvement and the security issues are yet to be fully identified, explored and tackled. Some may even state that overall the benefits of cloud computing outweigh any issues which may arise concerning security depending naturally on the case. In general, traditional IT systems are more easily controllable due to the fact that all components of the system are broken down to a specific perimeter in the organization and thus more easily managed and decide upon security controls required. On the other hand, computational power in traditional systems is limited with the exception of large organizations with exceptional capital and who can invest a lot on security departments.

In cloud environments, most components (network infrastructure, data storage, servers) depending on the cloud model, are managed by the provider, which adds transparency. This can have both a positive and a negative aspect as smaller organizations can invest less on security controls and thus manage

security more efficiently. However, the lack of visibility brings a sense of uncertainty if appropriate security measures are deployed on behalf of the cloud provider. Clouds are complex and developed for a general use and each organization has its own security requirements making it imperative for an organization to invest on professionals with advanced technical skills in order to deploy the cloud architecture according to the organization's needs.

6 REFERENCES

[1] Jouini M., Aissa A. Ben, Ben L., Rabai A., and Mili A., 2012, "Towards quantitative measures of Information Security : A Cloud Computing case study", International Journal of Cyber-Security and Digital Forensics, **1**(3), pp. 248–262.

[2] Greengard S., 2010, "Cloud computing and developing nations," Communications of the ACM, **53**(5), pp. 18–20.

[3] Schubert L. The future of cloud computing [Internet]. 2010. Available from: http://cordis.europa.eu/fp7/ict/ssai/docs/executivesummary-forweb_en.pdf

[4] Gartner, "Gartner Says Nearly One Third of Organizations Use or Plan to Use Cloud Offerings to Augment Business Intelligence Capabilities." [Internet] Available from: http://www.gartner.com/newsroom/id/1903814

[5] Chow R., Golle P., Jakobsson M., Shi E., Staddon J., Masuoka R., and Molina J., 2009, "Controlling data in the cloud: outsourcing computation without outsourcing control," Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, pp. 85–90.

[6] Subashini S., and Kavitha V., 2011, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, **34**(1), pp. 1–11.

[7] Cloud Security Alliance, 2010, "Top threats to Cloud Computing v.1.0." [Internet] Available from: https://cloudsecurityalliance.org/topthreats/

[8] Dahbur K., Mohammad B., and Tarakji A. B., 2011, "A survey of risks, threats and vulnerabilities in cloud computing," Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, ACM, p. 12.

[9] Jensen M., Schwenk J., Gruschka N., and Iacono L. Lo, 2009, "On technical security issues in cloud computing," Cloud Computing, 2009. CLOUD'09. IEEE International Conference on, IEEE, pp. 109–116.

[10] Mell P., and Grance T., "The NIST Definition of Cloud Computing (Draft) Recommendations of the National Institute of Standards and Technology," **145** (6), pp. 1-7.

[11] Orlando D., 2011, "Cloud Computing Service Models." [Internet] Available from: http://www.ibm.com/developerworks/cloud/library/cl-cloudservicemodels/?cmp=dw&cpb=dwcld&ct=dwnew&cr=dwnen&ccy=zz&csr=021011.

[12] Purser S., 2004, A Practical Guide to Managing Information Security (Artech House Technology Management Library), Artech House.

[13] Microsoft, 2003, "Microsoft pattern & practices." [Internet] Available from: http://msdn.microsoft.com/en-us/library/ff648641.aspx

[14] Gollmann D., 2005, Computer Security, John Wiley & Sons.

[15] SAS, "Statement on Auditing Standards (SAS) No. 70."

[16] Wireless Communications, Canedo E. D., Carvalho R. R. De, and Albuquerque O., 2012, "Trust Measurements Yeld Distributed Decision Support in Cloud Computing", International Journal of Cyber-Security and Digital Forensics **1**(2), pp. 140–151.

[17] Azab A.A., Ning P., Zhang X. 2011, "SICE: a hardware-level strongly isolated computing environment for x86 multi-core platforms." Proceedings of the 18th ACM Conference on Computer and Communications Security, ACM, pp. 375-388.