MITIGATING SECURITY AND PRIVACY RISKS IN THE CLOUD

Laith Hamasha

IT Auditor – Central Bank of Jordan School of Engineering and Computing Sciences

New York Institute of Technology Amman, Jordan

Raed Abu Zitar, Professor

College of Information Technology American University of Madaba Jordan

Farid Alzboun, Assistant Professor

Collage of information Technology, Ajloun National University

Abstract:

Within the fast growing era of the internet and distributed systems, a need presented itself to establish a virtual platform where you can perform all your tasks and computations without incurring all the costs associated with building an infrastructure, maintaining it and at the end having to upgrade it in order not to lose your competitive advantage. That need was translated into a scheme called "Cloud Computing".

As the case with any cut of the edge technology, there are people who support the trend and others who oppose it; usually for good reasons. The main concern for adopting cloud computing in a wide scale implementation is the security and privacy issues that can be viewed as residual risks associated with the cloud.

In this research paper, we are going to present these security and privacy setbacks and explain how they can tremendously affect the shift to the cloud computing scheme. Another pillar in our research is how to mitigate these risks by addressing the cause/result of each one of them to hinder their ability to limit the scope of adoption for the cloud.

Keywords: Security, Privacy risks.

1. Introduction

Cloud computing is a relatively new concept that aims at reducing the costs associated with building a computer infrastructure; software, hardware, databases and data centers. Basically, cloud computing is leasing customizable computer resources to customers, thus enabling them to perform all their desired tasks without any understanding of the infrastructure or concern for availability and maintenance. These resources can be software (Operating systems, utilities and programming languages), hardware (servers, storage devices), services (HR systems, Public relations services, and payroll) and databases (Oracle, Microsoft SQL).

Different disciplines can benefit from the virtualization that is offered by the cloud. Formidable efforts to build and maintain a computer infrastructure is facilitated to the point where anyone can benefit from it. For example, a school computer laboratory that has two hundred computer systems for the students to use for less than eight hours a day, will be more efficient if it was a virtualized environment where the school pay for the actual usage of resources, no more and no less.

However, in spite of all the benefits and facilities provided by the cloud, it also has a major security concern for the wide scale usage intended by its creators. Privacy risks associated with it are also a reason to minimize its applications and instill fear in the minds of business owners and governments.

The organization of the rest of this research is divided into: Section 3 describes major risks profound in the literature. Section 4 explains our mitigation mechanisms and the feasibility of applying them. Section 5 discusses how international standards and bodies are tackling the privacy and security issues of the cloud. In Section 6 we outline a risk assessment scenario using threat modeling technique taken into business transition to the cloud. Section 7 presents our future work to address the issues of the cloud computing. In section 8 we conclude and finally section 9 outlines the resources we cited.

2. Major Risks

Cloud computing security is a hot topic for research, its freshness, interestingness and recognition created an appeal for researches to pursue this topic in specific. Many security concerns evolved while weighing the benefits of using cloud computing over local resources. Below are the major risks introduced by the cloud are:

3.1 Data Storage:

Data is stored in the cloud in shared mediums that can be distributed all over the world depending on the geographical breadth of the CSP Cloud Service Provider.

In order to start utilizing the cloud resources fully, enterprises need to transfer their data to be stored over the cloud, therefore granting the CSP an implicit trust for their data. CSP on the other hand, should take proper measurements to protect the data stored in its premises through encryption, access control and data backup. [1]

3.2 Legal and Regulatory Risks:

Although data and its computations are residing at the CSP premises but the question to be asked is whether the protection of this data is the responsibility of the service provider, business owner or joined between both parties?

On the other hand, are the geographical location and the dissemination of the data over various locations? For example, if the data is stored in the CSP headquarters in Rome - Italy and the business owner resides at Allahabad in India. The CSP is governed by the rules and regulations of Italy however the business owner is not, he is governed by the regulations of India. In the case of a dispute between both ends, which laws and procedures are to be applied?

Looking at the subject from a different angle is when the cloud is used by cybercriminals to perform illegal activities or to host inappropriate material, such as: botnet C&C and child pornography respectively. A periodic review of businesses conducted through the cloud is essential to prevent cybercrime.

3.3 Privacy and Confidentiality:

Knowing the fact that multiple clients share the same computing resources in a virtualized manner; virtual machines working in harmony and are granted a fair amount of resources, can the CSP guarantee that these virtual machines are fully isolated. A group of researchers experiment the latter and gave evidence that sensitive data is not safe and can be extracted which implies privacy is not maintained using this mechanism. [2]

The service provider should guarantee also that proper access control rules are applied to the data. Enterprise employees have different levels of access control levels (privileges), which are usually depending on the security principle of “the least privilege”. In this scenario cloud operators should provide guarantees that they can adhere to these rules thus providing employees with limited access to the data according to their level of trust.

3.4 Availability:

CSP must provide redundancy in their architecture design. Congestion of the network due to the number of clients working at the same time should not present an issue; at least it should be seamless to the customer.

3.5 Integrity:

The delay in the processing of transactions can affect data integrity severely. Usually data records are accessed and updated by multiple users simultaneously. As a result, the cloud shall be vigilant to this issue and address it carefully.

3.6 Computationally feasible:

Many users prefer to utilize the cloud for its reasonable priced unlimited computational resources compared to expensive local resources. The cloud should preserve this assumption by allocating more resources to computation and providing results rapidly to maintain its competitive advantage.

3.7 Proper usage metering:

One major setback for the cloud is the lack of a fair pricing scheme that properly calculates the cost of the customer's real usage. Since computer resources are shared among different clients, calculating the amount of usage based on the time spent as per Amazon's policy is not fair. Another model is Google's per CPU cycle metering which is not fair also comparing two clients using the same resource for different purposes; editing a document and calculating gross national product of a country.

Committing to each customer's service level agreement is another issue that should be addressed by the cloud to guarantee fairness and encourage users.

3.8 Internal and external attacks:

Despite the fact that CSPs are usually multi-billion dollar companies however that does not guarantee that they are bullet-proof. Rogue employee acts and internal disclosure of sensitive information are always a possibility which impede the adoption of the cloud scheme.

Another issue in this context is external DDOS attacks, which can be launched against the service provider resulting in significant loss of communication.

3.9 Abusing cloud's resources:

Overriding reserved quota for each customer in memory usage or computing power can be considered as an abuse for the cloud's resources. Resource sharing can be tempting to unethical users who are part of the cloud client base. Proving this act and as a result legally pursuing the beneficiary is a whole different matter.

3. Mitigation mechanisms and their feasibility

Following what we have discussed earlier, this section proposes solutions for the upstanding risks facing a widespread cloud adoption.

A primary solution for a CSP to meet customers' demands is to establish customized packages that suit every customer's need, after all that is the essence of cloud computing (Customizability). Since the whole concept is leasing computational resources on demand, this solution will be of great benefit.

Data storage risks can be addressed through encryption as we stated above. However, these encryption algorithms should maintain a level of feasibility that will not negatively affect the performance criterion; otherwise, customers will lose trust in the ability of the cloud to provide its services in the manner that was proposed.

Dedicated storage capacities have to be available for customers who demand that their data should be fully isolated from others.

The key to addressing most of the obstacles facing cloud computing is establishing a common understanding through signing a customer specific SLA that states the acceptable policy to be conducted by the CSP. This approach also will eliminate any disputes from arising in the future.

Access control levels can be determined by the enterprise, delegated to staff members who will be granted proper certificates from the CSP. Those delegators will be responsible for requesting specific privileges from the CSP for other employees. This mechanism will guarantee that access control is limited and per the enterprise policy.

In order to solve the legal and regulatory issues, we propose to establish a multi-continent institution that governs the usage of cloud resources for all CSPs and their clients all over the world.

Extracting security information is a very difficult mission when dealing with local resources. Now that the infrastructure is virtual and remote, this task will become nearly impossible.

A security framework that guarantees CIA for auditing, legal and regulatory purposes is proposed by [1]. Existing frameworks such as: NIST and Cloud Security Alliance are applicable to a certain extent. [3] On the contrary, the cloud needs a fresh perspective, a brand new framework that will govern its activities and act as an enabler for security professionals and auditing firms to perform their tasks without any difficulty.

The existence of such a framework will enforce the trend of switching businesses to the cloud and widening its base of customers.

4. International Standards

Cloud computing as a new trend has tremendous opportunities however it is faced by bigger challenges. International bodies worldwide adopted the research on governing the cloud and explaining its issues along with recommended solutions.

The World Privacy Forum (WPF) issued a document in the beginning of 2009 discussing risks to privacy and confidentiality in the cloud. It highlighted some issues that probably are driving institutions and organizations away from adopting the cloud. The document is filled with legal citations and references to laws applicable in the United States of America and related to this subject such as: the Privacy Act of 1974, HIPPA and the Patriot act. [4]

One major reason for not adopting the cloud according to this document is that some information cannot be legally shared. One example is the health records of the US citizens' which are legally privileged information protected by the law and the nature of the relation between a doctor and a patient is legally abiding which means that any expose of some or most of this information to the public can result in a very big law suit against the company which can be easily won.

As discussed earlier, it is not clear which set of laws and regulations are applicable for the CSP, most argue that applicable laws are the local laws where the physical machine storing the data is residing, while others disagree and state that laws governing the mother company should be applied no matter where physical machines are kept.

On the other hand, tackling the issue of privacy is tricky. No matter how secure the CSP environment is, sometimes it is legally forced to expose private information to law enforcement agents based on a warrant issued by the court of law. This case is applicable where illegal materials are stored in the cloud; child pornography for instance is a crime punishable not by the civil law even if it was a corporation dispute but it is transferred to criminal court governed by the criminal law according to US laws.

Another case is where there is an embezzlement case and the sole way to find the criminal is by exposing his private financial records stored in his bank's cloud space, this kind of cases hinder the privacy in the cloud severely and therefore instill a negative notion into the minds of company's stakeholders.

A solution to this dilemma is by forming a profound risk assessment methodology applied to determine which category of information is suitable for storage in the cloud [4].

The document argues that extremely sensitive information like trade secrets or military specifications are not suitable for storage in the cloud, and the reason for that is the extraction of information from a third party is much easier than getting the same kind of information from the creator.

Other privacy issues like breaking the agreement signed by parties protecting information from the CSP side is hard to monitor, even bankruptcy of the CSP can expose sensitive information to the public.

Moreover, auditing requirements of customers may be an obstacle for the CSP. Customers need to acquire auditing information and maintain data integrity to adhere to the auditing requirements forced upon it by governing agencies, this kind of commitment is difficult to maintain in the cloud from the CSP perspective.

Answers to all these issues as given in the document are summarized by the following [4]:

- Creating better policies and procedures by the CSP will eliminate most of the aforementioned threats.
- Changes to some laws may be necessary in order to solve the remaining issues.
- Users should pay attention to the terms and conditions forced by the CSP therefore vigilance from the user's part is extremely important.

The Cloud Security Alliance (CSA) is another entity focusing all its efforts into the proper governance of the cloud and trying to facilitate its usage and adoption worldwide. In their revised guide published in 2009, CSA discussed a security guidance framework for critical areas in the cloud, their approach introduced domains of focus which are defined first, followed by important challenges that are facing these domains and finally given recommendations and solutions that can mitigate the challenges effects or eliminate their negative dominance.

What differentiates this guide from the latter document is that it is well organized, more comprehensive, introducing more domains of interest, presenting different challenges and finally providing more accurate and applicable solutions for outstanding issues.

One of the important concepts discussed in the guide, is introducing Identity as a service (Idaas) [5] which is defined as transferring the mission of complying with authorization and identity management requirements to the cloud. This transference of authority to third parties is critical to some organizations as there is a lack of staff in some small to medium sized organizations for performing these activities, in this case the distribution of the human capital can be enhanced yielding more focus on the core business of the organization therefore maximizing benefits.

The NIST (National Institute of Standards and Technology) has one of the most impressive guideline on this matter; they issued a document in 2011 focused mainly on the security and privacy of the cloud. The document is very detailed and comprehensive, as it tackles every issue known on the subject up to date, delivering advantages and drawbacks of the cloud.

The uniqueness in this document is characterized by its presentation of the upside for security and privacy gained from utilizing the cloud scheme.

Upsides are mainly the following [6]:

- Platform homogeneity which provides strength and compatibility.
- Staff specialization as the responsibility of providing security, backup and recovery and maintenance is shifted into the cloud.
- Limited resources organizations can flourish and reduce capital expenditure.
- Users need not be fully equipped with a cut edge technology machines, nonetheless they only need a web browser to perform all their desired activities which is referred to as mobile endpoints.
- The handling of data is better since distributed chunks of data on mobile devices (laptops, smart phones) are difficult to manage.

Although, there are many upsides to the cloud as per the authors of the NIST document, new challenges are presented in this context such as: the huge attack surface hence CSP operations environment is very capable but dispersed.

Another issue is the protection of ancillary data; which is data about cloud service provider's clients. This data should be confidential protecting customers' identities and privacy. Data Sanitization and availability are highlighted in the document as challenges that should be handled the CSPs in order to make their services appeal to potential and existing customers.

A summary of important recommendations addressing each aspect is provided in the last section of the NIST guideline.

To summon up what we illustrated above, we provide this table to compare between the different initiatives addressing cloud's issues therefore marketing its adoption.

Table 1: A Comparison between different cloud computing governance initiatives

Comparison criteria	Framework		
	WPF	CSA	NIST
Clearness	Yes	Yes	Yes
Completeness	Varies	Yes	Yes
Details	Simple	Yes	Very
Recommendations	Yes	Yes	Yes
Providing benefits	No	No	Yes
Recent	2009	2009	2011

5. Transitioning into the Cloud Risk Assessment

In order to outweigh between the risks and benefits associated with the adoption of cloud computing, an enterprise should consider performing a comprehensive risk assessment.

The methodology to be used can vary, for example; let us suppose that a small to medium sized organization specialized in software development is considering moving its core business to the cloud. Using the threat modeling approach, the company should follow these steps:

- Identify critical assets
- Decompose the system
- Identify possible points of attack
- Identify threats
- Categorize and prioritize the threats
- Mitigate risks
- Continually update the threat model

In our example, the company should first identify its assets; these include software development tools, middleware applications, testing scenarios, source code management tools (release management, software maintenance tracking tools) and finally data.

Assuming the company has an Oracle development suite for software coding, migrations tools for Oracle source code to work with web based technologies like ASP.Net or Java, various businesses oriented testing scenarios' and a source code reservation system to manage multiple program modifications by different development teams thus governing the process of making a new release.

The second step is to group related components and assets into clusters that are connected together in a work flow diagram.

Points of attack are usually entry points to the system and are considered as trust boundaries which can be exploited to the attacker's advantage since they deal with different zones of trust; internal trusted zone and an unknown external zone which can be trusted or not. Other points of attack are integration points between different components and assets. The integration point between the software development kit and the migration tools is considered a trust boundary which can cause vulnerability.

In our example, all assets mentioned before will be stored in the cloud and accessed by developers, quality assurance employees and documentation team simultaneously through web browsers.

Even though the functional diagram of the organization and its work flow may be clear but the residual uncertainty of the cloud is something that has to be taken into consideration. The identification of the threats that may exploit design or implementation vulnerabilities contains also known threats to the cloud architecture.

Some of the threats that may face such a transition are:

- Network threats: IP spoofing, DoS, MAC spoofing, Man in the middle attack and ARP poisoning.
- Integrity threats: incomplete transactions and falsification of data, change management issues.
- Availability threats: system crash, pharming, system halt and unexpected maintenance.
- Confidentiality threats: unauthorized disclosure of information whether internal (by CSP staff) or external (attackers or rogue organization employees).

- Software threats: Malwares, Trojans, RATS (Remote Access Tools), unpatched servers or software and out dated antivirus definitions.
- Access control threats: phishing and taking control of privileged users.

Classification and prioritization of threats is the next step. We will use the STRIDE scheme [7] to classify known threats according to the kinds of exploits that are used as this method would be useful in this context. Table 2 classifies the possible threats using the STRIDE scheme.

We will use DREAD which is a classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated threat [7]. Table 3 presents the risk quantification and prioritizing process.

Table 2: Possible threats classification using STRIDE scheme

Letter	Stands for	Associated Threat
S	Spoofing Identity	IP spoofing, MAC spoofing and ARP poisoning.
T	Tampering with data	Man in the middle attack, change management issues.
R	Repudiation	Incomplete transactions and falsification of data, change management issues.
I	Information Disclosure	Man in the middle attack, Malwares, Trojans, RATS, unpatched software and out dated antivirus definitions.
D	Denial of Service	System crash, pharming, system halt and unexpected maintenance.
E	Elevation of Privileges	Taking control of privileged users, phishing and unauthorized disclosure of information whether internal or external.

Table 3: Risk quantification and prioritization using DREAD scheme

Risk calculation (Risk = (Reprod. + Exploit.) x (Damage Pot. + Affected Users + Disc.))						
	Probability		Business Impact			
Description	Reproducibility (R)	Exploitability (E)	Damage Potential (D)	Affected Users (A)	Discoverability (D)	Risk
Network threats: IP spoofing, DoS, MAC spoofing, Man in the middle attack and ARP poisoning.	3	2	3	3	3	45 (High Risk)
Integrity threats: incomplete transactions and falsification of data, change management issues.	2	1	3	3	2	24 (Medium Risk)
Availability threats: system crash, pharming, system halt and unexpected maintenance.	2	2	3	3	3	32 (Medium Risk)
Confidentiality threats: unauthorized disclosure of information whether internal (by CSP staff) or external (attackers or rogue organization employees).	3	3	3	1	1	30 (Medium Risk)
Software threats: Malwares, Trojans, RATS (Remote Access Tools), unpatched servers or software and out dated antivirus definitions.	2	3	3	3	2	40 (High Risk)
Access control threats: phishing and taking control of privileged users.	3	3	3	2	1	36 (Medium Risk)

Risk mitigation is then performed according to the risk score of each threat using proper controls. However, some risks can be accepted by the management while others may be transferred (E.g. Insurance companies).

Risk assessment is a continuous process to keep up to date with the most recent threats and avoid the company great losses. This analysis can give decision makers a glimpse

of what they are going to face by transitioning into the cloud and make taking this strategic directive more clear and objective.

6. Future work

Addressing cloud's CIA concerns will have a positive impact on cloud's admissibility as a computing approach and harness its growth.

Proposing a novel security framework that governs the cloud computing society and facilitates the extraction of security information is of great importance. This framework along with its applications will be our next topic of research.

We will focus on the proper way to apply this framework on the existing cloud architecture, compare it with other frameworks found in the literature outweighing its strengths and weaknesses and finally presenting real time analysis results that will support our claims.

7. Conclusion

Cloud computing has many benefits compared to other computing streams. Its virtualization, customizability and reduced capital expenditure can enhance conducting businesses efficiently. Nevertheless, it is also faced with many implicit risks and concerns which have appeared due to its design, these risks mainly evolve around privacy and security concerns.

Finally, we conclude that in order for the cloud computing scheme to meet enterprises expectations and needs, service providers should fiercely try to address these risks and deem them negligible. Building trust in the cloud seems to be an impossible task but tackling this issue in the proper method will produce results in the near future.

Cloud computing is indeed a unique field, a fresh perspective and will ease the approach of making the world a small village equally accessible to all its inhabitants.

Resources:

Lori M. Kaufman, Data Security in the World of Cloud Computing, co published by the IEEE Computer and Reliability Societies, JULY/AUGUST 2009.

Kui Ren, Cong Wang, and Qian Wang, Security Challenges for the Public Cloud, Published by the IEEE Computer Society, JANUARY/FEBRUARY 2012.

Rajarshi Chakraborty, Srilakshmi Ramireddy, T.S. Raghu, H. Raghav Rao, The Information Assurance Practices of Cloud Computing Vendors, Published by the IEEE Computer Society, JULY/AUGUST 2010.

Robert Gellman for the World Privacy Forum, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, February 2009.

The Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, DECEMBER 2009.

Wayne Jansen, Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, DECEMBER 2011.

Threat Risk Modeling, The Open Web Application Security Project (OWASP), https://www.owasp.org/index.php/Threat_Risk_Modeling