ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

EFFECTIVE REVIEW ON SECURITY AND INTEGRITY IN CLOUD INFRASTRUCTURE

Ashna Sharma

M.Tech. Research Scholar

Department of Computer Science and Engineering

Haryana Engineering College

Haryana, India

Bandana Sharma

Assistant Professor

Department of Computer Science and Engineering

Haryana Engineering College

Haryana, India

ABSTRACT

Cloud Computing is one of the major domains that is being used in number of applications and facing lots of security and integrity issues. Cloud computing is a model for enabling convenient,

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is the collective term for a group of IT technologies which in collaboration are changing the landscape of how IT services are provided, accessed and paid for. Some of the supporting technologies have already been available for quite some time, but it is the combination of several technologies which enables a whole new way of using IT. Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services. In this paper, different dimensions of security and integrity are underlined related to cloud infrastructure.

Keywords – Cloud Computing, Cloud Security, Integrity in Cloud Platform

INTRODUCTION

Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. The market research and analysis firm IDC suggests that the market for Cloud Computing services was $16billion in 2008 and will rise to $42billion/year by 2012. It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications. According to a Gartner press release from June 2008, Cloud Computing will be “no less influential than e-business”.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

Cloud computing evokes different perceptions in different people. To some, it refers to accessing software and storing data in the "cloud" representation of the internet or a network and using associated services. To others, it is seen as nothing new, but just a modernization of time-sharing model that was widely employed in 1960s before the advent of relatively lower-cost computing platforms. This development eventually evolved to the client/server model and to the personal computer, which placed large accounts of computing power at people's desktops and spelled the demise of time-sharing systems .

There is a lot of discussion of what cloud computing exactly is.

The NIST definition of cloud computing is :

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing is the collective term for a group of IT technologies which in collaboration are changing the landscape of how IT services are provided, accessed and paid for. Some of the supporting technologies have already been available for quite some time, but it is the combination of several technologies which enables a whole new way of using IT .

Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services .

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

The cloud is a metaphor for the Internet and is an abstraction for the complex infrastructure it conceals. There are some important points in the definition to be discussed regarding Cloud Computing. Cloud Computing differs from traditional computing paradigms as it is scalable, can be encapsulated as an abstract entity which provides different level of services to the clients, driven by economies of scale and the services are dynamically configurable .

To explain the definition in short, "convenient on-demand network access", together with "minimal management effort or service provider interaction," stands for easy and fast network access to resources that are ready to use. With a "shared pool of resources," the available computing resources of a cloud provider are combined as one big collection, to serve all users. The "rapid provisioning and releasing" of computing resources is used to quickly match available resources, with the need for those resources. This rapid provisioning prevents a lack of computing power when the need increases, while rapid release of assigned resources prevents that resources are idle while they may be required elsewhere .

There are many definitions of Cloud computing, a recent study noted more than 22 different definitions of cloud computing where variety of technologies in the Cloud makes the over-all picture confusing.

Table 1 - Description of Cloud by Assorted Practitioners

Author/Reference	**Year**	**Definition/Excerpt**
M. Klems	2008	*you can scale your infrastructure on demand within minutes or even seconds, instead of days or weeks, thereby avoiding under-utilization (idle servers) and over-utilization (blue screen) of in-house resources...*
P. Gaw	2008	*using the internet to allow people to access technology-enabled services. Those services must be 'massively scalable...*

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

R. Buyya	2008	*A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers*
R. Cohen	2008	*Cloud computing is one of those catch all buzz words that tries to encompass a variety of aspects ranging from deployment, load balancing, provisioning, business model and architecture (like Web2.0). It's the next logical step in software (software 10.0). For me the simplest explanation for Cloud Computing is describing it as, "internet centric software...*
J. Kaplan	2008	*a broad array of web-based services aimed at allowing users to obtain a wide range of functional capabilities on a 'pay-as-you-go' basis that previously required tremendous hard-ware/software investments and professional skills to acquire. Cloud computing is the realization of the earlier ideals of utility computing without the technical complexities or complicated deployment worries...*
D. Gourlay	2008	*...the next hype-term...building off of the software models that virtualization enabled*
D. Edwards	2008	*...what is possible when you leverage web-scale infrastructure (application and physical) in an on-demand way...*
B. de Haff	2008	*...There really are only three types of services that are Cloud based: SaaS, PaaS, and Cloud Computing Platforms.*

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

B. Kepes	2008	*...Put simply Cloud Computing is the infrastructural paradigm shift that enables the ascension of SaaS. ... It is a broad array of web-based services aimed at allowing users to obtain a wide range of functional capabilities on a pay-as-you-go basis that previously required tremendous hardware/software investments and professional skills to acquire*
K. Sheynkman	2008	*Clouds focused on making the hardware layer consumable as on-demand compute and storage capacity. This is an important first step, but for companies to harness the power of the Cloud, complete application infrastructure needs to be easily configured, deployed, dynamically-scaled and managed in these virtualized hardware environments*
K. Hartig	2008	*..really is accessing resources and services needed to perform functions with dynamically changing needs...is a virtualization of resources that maintains and manages itself.*
P. McFedries	2008	*Cloud Computing, in which not just our data but even our software resides within the Cloud, and we access everything not only through our PCs but also Cloud-friendly devices, such as smart phones, PDAs... This is utility computing powered by massive utility data centers.*
Luis M. Vaquero	2009	*. . . a large pool of easily usable and accessible virtualized resources (such as hard- ware, development platforms and/or services).....This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs.*

These definitions are based on five attributes that can be used to describe a cloud-based system.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

Multitenancy (shared resources): Unlike previous computing models, which assumed dedicated resources (i.e., computing facilities dedicated to a single user or owner), cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level .

Scalability: cloud computing have property to scale to tens of thousands of system with bandwidth and storage also .

Elasticity: It is the property of increasing and decreasing the resources according to the users' need, as well as release the resources when they are no longer needed .

Pay as you go: One of the advantage of cloud computing is to pay according to the need or consumption like for one hour, two hour or cost per gigabyte and so on which has large impact on cost or economics. So cloud computing model provides a cheaper way for business to acquire and use the IT – capabilities .

Self provisioning of resources: Users self- provision resources like additional system and network resources.

Though each cloud computing platform has its own strength, one thing should be noticed is that no matter what kind of platform there is lots unsoloved issues. For example, continuously high availability, dealt mechanisms of cluster failure in cloud environment, consistency guaranty, synchronization in different clusters in cloud platform, interoperation and standarization, the security of cloud platform and data in transmission and so on are all among the issue to be better solved .

- **Control**

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

Some IT departments are concerned because cloud computing providers have a full control of the platforms. Cloud computing providers typically do not design platforms for specific companies and their business practices .

- **Performance**

The major issue in performance can be for some intensive transaction-oriented and other data-intensive applications, in which cloud computing may lack adequate performance. Also, users who are at a long distance from cloud providers may experience high latency and delays .

- **Bandwidth Costs**

With cloud computing, companies can save money on hardware and software; however they could incur higher network bandwidth charges. Bandwidth cost may be low for smaller Internet-based applications, which are not data intensive, but could significantly grow for data-intensive applications .

- **Political Issues Due to Global Boundaries**

In the cloud computing world, there is variability in terms of where the physical data resides, where processing takes place, and from where the data is accessed. Given this variability, different privacy rules and regulations may apply. Because of these varying rules and regulations, by definition politics becomes an element in the adoption of cloud computing, which is effectively multijurisdictional .

- **Reliability**

Cloud computing still does not always offer round-the-clock reliability. There were cases where cloud computing services suffered few-hours outages . In the future, we can expect more cloud computing providers, richer services, established standards, and best practices.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

- **Security**

Because cloud computing represents a new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved. That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing. The subsequent chapters present a detailed examination of those concerns to determine whether they are grounded .

- **Privacy**

The ability of cloud computing to adequately address privacy regulations has been called into question. Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear (i.e., not yet established) whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model .

- **Connectivity and Open Access**

The full potential of cloud computing depends on the availability of high-speed access to all.
Such connectivity, rather like electricity availability, globally opens the possibility for industry and a new range of consumer products. Connectivity and open access to computing power and information availability through the cloud promotes another era of industrialization and the need for more sophisticated consumer products .

- **Interoperability**

The interoperability and portability of information between private clouds and public clouds are critical enablers for broad adoption of cloud computing by the enterprise. Many companies have made considerable progress toward standardizing their processes, data, and systems through

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

implementation of ERPs. This process has been enabled by scalable infrastructures to create single instances, or highly integrated connections between instances, to manage the consistency of master and transaction data and produce reliable consolidated information. Even with these improved platforms, the speed at which businesses change may still outpace the ability of IT organizations to respond to these changes. SaaS applications delivered through the cloud provide a low-capital, fast-deployment option. Depending on the application, it is critical to integrate with traditional applications that may be resident in a separate cloud or on traditional technology. The standard for interoperability is either an enabler or a barrier to interoperability, and permits maintenance of the integrity and consistency of a company's information and processes .

CLOUD SECURITY AND PRIVACY ISSUES

Security and privacy are indeed interrelated because the security is provided without having privacy but the privacy is not maintained without security.

Today various small and medium size companies moved towards cloud environment because now they are capable to compete with the larger infrastructure companies by simply gaining fast access to best business application and drastically boost their infrastructure resources at negligible cost. While the cloud offers these advantages there are various issues and risks that reduce the growth of cloud computing.

During *communication process* consumers are front end and cloud service providers are back end. For resource pooling various steps are included:

- User authentication and login process: In this web browser collects all necessary information about consumer using various security technologies/protocols like SSL/SSH/TLS.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

- Web browser provides all information to policy manager which authenticate the consumer using public key infrastructure, certification authority and others.
- After that consumer request to browser for required services using Simple Object Access Protocol [XML or REST format + transfer protocols].
- Now web browser delegates the QOS requirements to policy manager, which evaluate the requirements according to service level agreement (SLA). For SLA policy manager also use cloud broker and resources engine.
- For resource discovery cloud broker collects the information about other cloud and their services and resource engine delegates the service requirement to VM schedulers which collaborates the required service from various VM / chunks provider.

DEPENDENCY AMONG CLOUD LAYERS

The application layer and core layer depends upon VMs layer and physical machine layer which further depend upon virtual network layer and physical network layer so damage at any layer also have great impact on other layers.

COMPLEXITY OF SECURITY ASPECTS

When we think about security of organization's core IT infrastructure there is need to provide security at network level, host level, application level and when we talk about data security two aspects are included 'data transmission security and data storage security'.

CLOUD SECURITY ISSUES

In cloud computing the Security issues deals with all the challenges associated with securing an organization's core IT infrastructure at the network, host, and application levels as well as the vulnerabilities and attacks related to the data security including: Data-in-transit, Data-at-rest, Processing of data including multitenancy, Data lineage, Data provenance . To cover all these

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

security issues possible within the cloud, and in-depth, would be herculean task. Existing efforts look to provide a taxonomy over the issues seen. The Cloud Security Alliance is a non-profit organisation that seeks to promote the best practises for providing security assurance within the cloud computing landscape. In Hubbard, Sutton et al. the Cloud Security Alliance identify seven threats to cloud computing that can be interpreted as a classification of security issues found within the cloud. They are:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service and Traffic Hijacking
- Unknown Risk Profile

In traditional on premises deployment model the data of enterprise must resides within its boundary and follow their own access control and security policies. Whereas in cloud computing data reside at distributed data centres of cloud with the lack of control and without the knowledge of how their data resides. Due to the nature of cloud system there are many questions that arise as to weather a cloud is secure enough or not from various threats and vulnerabilities that are:

NETWORK LEVEL ATTACKS

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

During resource pooling process all data or services flow over the network needs to be secured from following attacks to prevent the leakage of sensitive information or other vulnerabilities :

- **Denial of service/distributed denial of service attack**

  This attack can overwhelm target's resources so that authorised user is abstained from getting the normal services of cloud. DDOS is also based on DOS attack which can be distributed for more significant effects. This attack is a cause of failure of availability.

- **Eavesdropping**

  Eavesdropping is an interception of network traffic to gain unauthorized access. It can results in failure of confidentiality .

- **Man in the Middle attack**

  It is also a category of eavesdropping. The attack set up the connection with both victims that makes conversation and making them believe that they talk directly but infect the conversation between them is controlled by attack.

- **Replay attack**

  The attacker intercepts and save the old messages and then send them later as one of participants to gain access to unauthorized resources.

- **Back Door**

  The attacker gain access to network through bypassing the control mechanisms using "back door" such as modem and asynchronous external connections .

- **Impersonation**

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

It is vulnerability in which malicious node modify the data flow route and lure the node to wrong positions.

- **Sybil attack**

In *Sybil attack* a malicious user pretends to be distinct users after acquiring multiple identities and tries to create relationship with honest user if malicious user is successful to compromise one of the honest user then attack gain unauthorized privileges that helps in attacking process.

- **Byzantine failure**

It is a malicious activity which compromised a server or a set of server to degrade the performance of cloud.

ATTACKS AND VULNERABILITIES BASED ON SECURITY TECHNIQUES

If any security technique has weakness in implementation it can cause various vulnerabilities:

- Inside channel attack gain the information from physical implementation of cryptosystem to break the security. The information is like technical knowledge on which encryption implement, time information, power consumption and others.
- SSL/SSH/TLS use the cryptography techniques to secure the data but any crucial flow in implementation of cryptography algorithm can make stronger cryptography technique to weak technique which is a main target of hackers .

LANGUAGE AND MALICIOUS PROGRAM INJECTION BASED ATTACK

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

One of the most frequently discovered vulnerabilities in cloud are a direct result of language and programmes that are as follow .

- **Buffer overflow**

  It is a favourite exploit for hacker which takes the advantage of programme that is waiting for user's input. But in place of user the hacker would enter the input which results to move the control to attack code.

- **Trojan horses/Malware**

  They are the unauthorized program that are contained or injected by malicious user within legitimate program to perform unknown and unwanted function.

- **XML Signature wrapping Attack**

  It is well known attack on protocols like SOAP that use XML format to transfer the request for services. In this, attack moves the original body of SOAP message to newly inserted wrapping element writing within SOAP header and create a new body which contains the operation that an attack wants to perform.

WEB APPLICATION ATTACKS

Web browser is one of the way of providing the web application virtually to users but at the same time they also creates vulnerabilities that has detrimental impact on customers as well as on cloud system .

- **Weak authentication or weak username- password**

  It is one of the main target of malicious users to gain unauthorized access to the services.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

- **SQL injection flaws**

In which malicious SQL code is erroneously executed in database backend.

- **Cross-site-scripting (XSS)**

In which the malicious java script code is executed erroneously by browser.

VIRTUAL MACHINE BASED VULNERABILITIES

Following are the various VM based vulnerabilities create challenges and issues for service providers.

- Any malicious programme in VM also transferred between other VMs using shared clipboard technology which is an issue for security.
- Many VMs co-exist on same server share CPU, memory, I/O have virtual boundaries. So securing the virtual boundaries is also a challenge for service provider.

Hypervisor is main controller that maps the physical resources to virtual resources. So if any hypervisor is compromised, it is possible to trace the VMs operations unencrypted .

PRIVACY/JURISPRUDENCE ORIENTED ISSUES

The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions. It is shaped by public expectations and legal interpretations; as such, a concise definition is elusive if not impossible. Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data (or personally identifiable

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 3 Issue 2 March 2015
International Manuscript ID : 23482001V3I2032015-07
(Approved and Registered with Govt. of India)

information—PII). At the end of the day, privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization's practice around personal information .

Another definition gaining popularity is the one provided by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in the Generally Accepted Privacy Principles (GAPP) standard: "The rights and obligations of individuals and organizations" with respect to the collection, use, retention, and disclosure of personal information . Jaeger, Lin and Grimes discusses the widening gap between technology and local, national and international legislation. Technological innovation occurs at a much more rapid pace than the pace at which legislation can change. This rapid pace has left a cloud of ambiguity concerning how users' data can be treated legally within the cloud. Given the nature for `ever changing' service level agreements, the terms and conditions that one originally agreed to may not be the current versions. Furthermore, the laws and regulations themselves may not be suitable, are open for interpretation and also bounded by jurisdiction. These issues are discussed below.

SERVICE LEVEL AGREEMENTS

Users implicitly trust the service provider not to violate terms and conditions, and be in a position to securely store their information. The terms and conditions set by the service provider may not actual conform with the established policies set by the consumers organisation. Non-compliance with such policies could lead to a loss of reputation and credibility.

Service providers will also adapt their terms and conditions over time and often not inform users of these changes in an explicit manner. This presents the user with a dilemma: Either they accept terms that are not absolute or a privacy policy that they disagree with, or they do not use the

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

service. Users may be unaware that the terms and conditions have changed and will use a service governed by policies and agreements which were not the ones originally agreed upon. Even more so, the user may be subject to peer pressure in which the service is also used by the users' peer group and used actively for collaboration. Leaving the service may have an adverse affect upon the users interaction with their peers. Further problems arise when the users themselves fail to adhere to the conditions set out in the agreement e.g. failure to pay or the uploading of inappropriate material. What happens to the users data when this occurs? Will the data be retained and can it be extracted from the service provider? Furthermore a CSP will also change, over time, the terms and conditions attached to the service to further the CSPs own business interests. Users are not in full control over the security of their data and that the protection offered by the service provider is not absolute.

he Fourth Amendment of the United States Constitution states:

> "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . .* "

Similarly, Article 8 of the European Convention of Human Rights states:

> "*Everyone has the right to respect for his private and family life, his home and his correspondence*"

This has resulted in a `reasonable expectation of privacy' existing, and being guaranteed, over ones home and its contents. Couillard discusses this problem under the auspices of United States Common Law. In the United States the contents of ones briefcase and also school satchel is governed under this expectation of privacy. With Cloud Computing society has naturally extended this reasonable expectation of privacy to cloud services that offer similar functionality e.g. Dropbox. Such services are often described using the terminology Virtual Containers. This raises the legal problem of can data stored in the cloud afford the same level of protection as data

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 3 Issue 2 March 2015
International Manuscript ID : 23482001V3I2032015-07
(Approved and Registered with Govt. of India)

stored within ones home. The Katz Test, used to determine ones reasonable expectation of privacy requires that: a) there was a subjective expectation of privacy over the object; and b) the expectation was reasonable. Implying that there is some form of concealment i.e. opacity, to the object in question. Within the Cloud this would imply that simple password protection or data encryption would be sufficient. Couillard comments that these measures have only been upheld within case law and not in written law. Furthermore, under US Law this expectation of privacy is diminished if the data is handed over to a third-party. The third-party doctrine is that transactional data, data that contains information regarding the transaction itself, can no longer be afforded the same expectation of privacy as the contents of the transaction. The third-party needs transactional data to operate. Couillard contends that a URL can be seen as transactional data and that unlisted links i.e. dynamic ones, do not fall under the fourth amendment. This implies that the contents of a URL that may include authentication tokens and other identifying information will also not be protected by the fourth amendment .

Though there is some debate concerning expectations of privacy, existing legislation exists that CSPs should comply with. Such legislation governs the country that the CSP is operating within. Failure to comply with local legislation, or if the information of service users were to be lost, stolen or exposed then such acts could lead have potential legal ramifications for the service provider. This in turn could result in loss of credibility, loss of reputation and possible reduction in user base .

Service provision is not in principle bound at a national level. Users from one country commonly access services located in another. This presents service providers and consumers with problems of under whose laws must the service abide by, and to what degree. Are the consumers allowed

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

to export their data to a foreign country? And what provisions are there for the safety of the data? Amazon.com, for example, offer their Simple Storage Service from US (Northern California), European (Ireland) and Asian (Singapore) based data centers to be able to offer services within the different regulatory frameworks of those regions. Furthermore the European Commission's Directive on Data Protection prohibits the transfer of personal data to non-EU nations .

The Safe Harbour Framework is a supra-national framework for US based companies to comply with the data protection laws of Switzerland and the European Union. Thus providing a `safe harbour' for Swiss and EU citizens data residing within the United States. For a US company to comply it must adhere to seven principles, derived from the Directive on Data Protection, of: Notice, Choice, Onward Transfer, Access, Security, Data Integrity and Enforcement. However, there has been significant criticism of this framework concerning the compliance and its enforcement. It was noted in an external study that false claims were made by US companies concerning membership and certification.

CONCLUSION

One of the primary goals of information security is to protect the fundamental data that powers our systems and applications. As we transition to Cloud Computing, our traditional methods of securing data are challenged by cloud-based architectures. Elasticity, multi-tenancy, new physical and logical architectures, and abstracted controls require new data security strategies.

REFERENCES

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 3 Issue 2 March 2015

International Manuscript ID : 23482001V3I2032015-07

(Approved and Registered with Govt. of India)

[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[3] Ostermann, S., Iosup, A., Yigitbasi, N., Prodan, R., Fahringer, T., & Epema, D. (2010). A performance analysis of EC2 cloud computing services for scientific computing. In *Cloud computing* (pp. 115-131). Springer Berlin Heidelberg.

[4] Mell, P., & Grance, T. (2009). The NIST definition of cloud computing. *National Institute of Standards and Technology*, *53*(6), 50.

[5] Buyya, R., Yeo, C. S., & Venugopal, S. (2008, September). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on* (pp. 5-13). Ieee.

[6] Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on* (pp. 109-116). IEEE.

[7] Sabahi, F. (2011, May). Cloud computing security threats and responses. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on* (pp. 245-249). IEEE.