Internet of Things and Cloud Computing
2014; 2(2): 6-11
Published online August 20, 2014 (http://www.sciencepublishinggroup.com/j/iotcc)
doi: 10.11648/j.iotcc.20140202.11

Data security and privacy concerns in cloud computing

Masrat Yousuf Pandith

I.T Skills Department, King Saud University, Riyadh, Saudi Arabia

Email address:
masrat.pandit@gmail.com

To cite this article:
Masrat Yousuf Pandith. Data Security and Privacy Concerns in Cloud Computing. *Internet of Things and Cloud Computing.* Vol. 2, No. 2, 2014, pp. 6-11. doi: 10.11648/j.iotcc.20140202.11

Abstract: Cloud is a latest computing paradigm. Cloud computing means storing and accessing data and programs over the internet instead of computer's hard disk. Cloud storage makes it easy to access the software, resources and data anytime anywhere when connected to the internet. Now-a-days almost every organization is using cloud to store the data. There is a need to protect that data .Cloud data security goal aims at three main things: Availability, Confidentiality, and Integrity. Cryptography is used to achieve confidentiality. Three types of algorithms are used in Cryptography (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Hashing algorithms ensure integrity of data. Cloud provides three types of services to its users: SaaS – enables users to run applications online through cloud computing techniques PaaS – enables the users to build their own cloud applications using supplier-specific tools and languages through cloud computing techniques.IaaS – enables the users to run any application on supplier's cloud hardware. This paper discusses the types, service model, deployment methods, data security and privacy concerns in cloud.

Keywords: Cloud Computing, Cryptography, IaaS, PaaS , SaaS, Symmetric-Key, Asymmetric-Key, Hashing

1. Introduction

The Evolution of technology started with mainframe computers and Progressed to minicomputers, personal computers, and so forth and we are now living in cloud computing age. Rather than using local hard drives, servers or local applications cloud computing depends on sharing computing resources. In cloud computing, the word "cloud" is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing [Sreekanth Iyer IBM Cloud Computing Central] where different services are delivered to the cloud user :the services provided by the cloud supplier could be software, hardware or even a platform through the Internet.

Every organization is using the cloud services depending on their need. There is necessity to shield the cloud data against unauthorized access, modification or Denial of Service. A denial of service attack involves saturating the target with bogus requests to prevent it from responding to legitimate requests in a timely manner. An attacker typically uses multiple computers or a botnet to launch an assault. Even an unsuccessful distributed denial of service attack can quickly consume large amounts of resources to defend against and cause charges to soar. The dynamic provisioning of a cloud in some ways simplifies the work of an attacker to cause harm. While the resources of a cloud are significant, with enough attacking computers they can become saturated [Jen09]. For example, a denial of service attack against a code hosting site operating over an IaaS cloud resulted in more than 19 hours of downtime [Bro09,Met09][25].

The main goals of the data Security are: Availability, Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography is a vital part of preventing private data from unauthorized access. Even if someone is successful in intercepting your messages they still will not be able to understand the data if it is protected by cryptography. Cryptographic technique is not only used to protect data from alteration, but it has larger objectives which include:

i) Authentication: Proving One's identity, ii) Non-repudiation: Mechanism to prove that the sender has really sent the message, iii) confidentiality: Ensuring that no one can read the message except the intended receiver. iv) Integrity: The received message has not been altered in anyway.

Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

2. Cloud Deployments Models

There are four basic cloud deployment models, as outlined by NIST (Badger et al., 2011), based on who provides the cloud services. These four deployment models are:

2.1. Public cloud
2.2. Private cloud
2.3. Hybrid cloud
2.4. Community cloud

2.1. Public Cloud

Public cloud service is open to use for the general public .Service provider makes resources available to the users over the internet. Services provided by this type of cloud may be free or paid depending on the type of the service they deliver.

Cloud computing in a shared environment creates new opportunities for hackers seeking to discover vulnerabilities, which may ultimately allow them to deny service or gain unauthorized access [27]. Attackers could also rent space in the cloud and then use that space as a base of attack on neighbouring clients [28] .Other concerns are location of the data, data backups, restoration, and portability, How often are vulnerability scans initiated etc.

2.2. Private Cloud

Private cloud is owned by a single company comprising multiple consumers and it may exist on or off premises. Private Cloud Computing is comprised of networking, server hardware (which usually provides server virtualization), storage and management tools. This is most often managed internally but also can be hosted externally by a Managed Service Provider (MSP), which is then known as a Virtual Private Cloud [1].

Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud[28].Having a private cloud infrastructure takes away concerns about lack of transparency on the service provider side [30].

The cloud environments break down departmental silos and offer increased accessibility, especially to non-employees outside of the organization if given access to the on-demand computer resources. Not properly locking data down becomes an issue leading to unwanted breaches. Protecting data from leaks becomes critical in a cloud environment [30].

2.3. Hybrid Cloud

It seems that cloud deployment is either public or private. The major benefit of using private cloud is flexibility and security on the other hand public cloud offers scalability and accessibility. Both of them have unique benefits but they also have tradeoff. Hybrid Cloud merges the advantages of public and private cloud. A hybrid cloud is a combination of a private cloud combined with the use of public cloud services where one or several touch points exist between the environments. The goal is to combine services and data from a variety of cloud models to create a unified, automated, and well-managed computing environment [By Judith Hurwitz, Marcia Kaufman, Fern Halper, and Dan Kirsch from Hybrid Cloud For Dummies].

2.4. Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises [2].

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or: Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

Fig 1. *Table - Cloud Computing Deployment Models [3].*

[1]Management Includes: Governance, operations, security, compliance, etc.. [3].
[2] Infrastructure implies physical infrastructure such as facilities, compute, and network & storage equipment[3].
[3]Infrastructure Location is both physical and relative to an organization's management umbrella & speaks to ownership versus control[3].
[4]Trusted consumers of service are those who are considered part of an organization's legal/contractual/policy umbrella including employees, contractors & business partners. Untrusted consumers are those that may be authorized to consume some/all services but not legal extensions of the organization.[3]

3. Service Models

As per National Institute for Standards and Technology (NIST) there are three basic types of cloud service Models. These models are:

(i) Software as a service (SaaS)
(ii)Platform as a service (PaaS)
(iii) Infrastructure as a service (IaaS)

3.1. Software as a Service (SaaS)

Application are accessed over the internet example Google, zoho provide word processor, spreadsheet and presentation web apps. Saas application can be free or paid via subscription. These apps are accessible from any computer connected to internet either through thin client interfaces like web browsers or program interfaces.

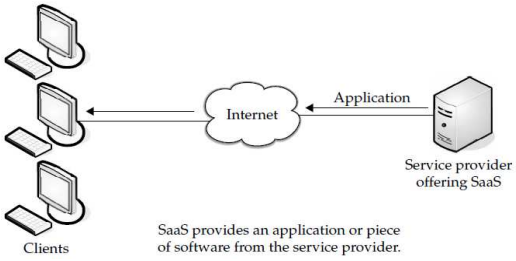

Fig 2. *Software as a Service (SaaS) [4]*

3.1.1. Security issues in SaaS

The SaaS model offers the customers with significant benefits, such as improved operational efficiency and reduced costs. SaaS is rapidly emerging as the dominant delivery model for meeting the needs of enterprise IT services. However, most enterprises are still uncomfortable with the SaaS model due to lack of visibility about the way their data is stored and secured. According to the Forrester study, ''The State of Enterprise Software: 2009,'' security concerns are the most commonly cited reason why enterprises are not interested in SaaS. Consequently, addressing enterprise security concerns has emerged as the biggest challenge for the adoption of SaaS applications in the cloud (Heidi Lo et al., 2009).However, to overcome the customer concerns about application and data security, vendors must address these issues head-on.There is a strong apprehension about insider breaches, along with vulnerabilities in the applications and systems' availability that could lead to loss of sensitive data and money. Such challenges can dissuade enterprises from adopting SaaS applications within the cloud [31]

3.2. Platform as a Service (PaaS)

It Provides tools and environment to the users for creating cloud applications. For example Google have a product called App Engine which allows anyone to build and run applications on Google's infrastructure. App Engine applications are easy to build, easy to maintain, and easy to scale as your traffic and data storage needs change. With App Engine, there are no servers for you to maintain. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

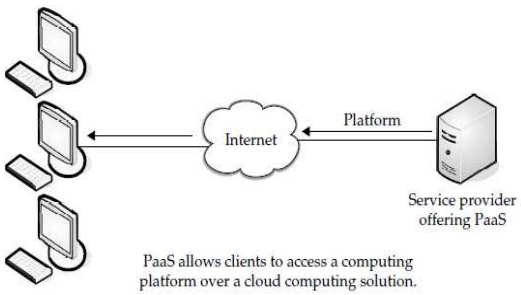

Fig 3. *Platform as a Service (PaaS) [4]*

3.2.1. Security issues in PaaS

It offers developers a service that provides a complete software development lifecycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the ''view'' of the developers. The dark side of PaaS is that, these advantages itself can be helpful for a hacker to leverage the PaaS cloud infrastructure for malware command and control and go behind IaaS applications [31].

3.3. Infrastructure as a Service (IaaS)

It Allows users to run any existing application on cloud supplier's hardware. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) [2].

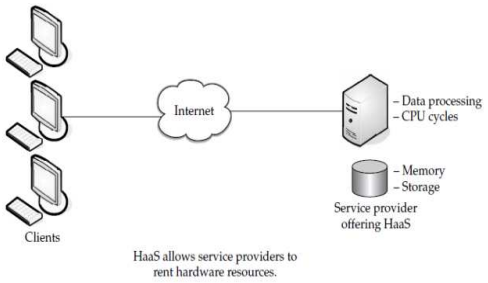

Fig 4. *Infrastructure as a Service (IaaS) [4]*

3.3.1. Security issues in IaaS

IaaS completely changes the way developers deploy their applications. Instead of spending big with their own data centers or managed hosting companies or colocation services and then hiring operations staff to get it going, they can just go to Amazon Web Services or one of the other IaaS providers, get a virtual server running in minutes and pay only for the resources they use.

With cloud brokers like Rightscale, enStratus, etc., they could easily grow big without worrying about things like scaling and additional security. In short, IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but ''out of the box'' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host[31].

4. Data Security Concerns

Cloud computing is being adapted in many sectors. "Everyone wants to use the cloud due to cost savings and

new agile business models. But when it comes to cloud security, it's important to understand the different threat landscape that comes into play" [Data Security in the Cloud Derek Tumulak, Vormetric] .Virtualizing and pooling IT resources in the cloud enables organizations to realize significant cost savings and accelerates deployment of new applications. However, those valuable business benefits cannot be unlocked without addressing new data security challenges posed by cloud computing [A Trend Micro White Paper July 2010].No doubt Cloud computing provides business benefits, but there are some concerns as well when moving data to cloud. Data security and data residency are the key concerns.

Encrypting data and using a non-secured protocol (e.g., "vanilla" or "straight" FTP or HTTP) can provide confidentiality, but does not ensure the integrity of the data (e.g., with the use of symmetric streaming ciphers). We know how to effectively encrypt data-in-transit, and how to effectively encrypt data-at-rest. Although using encryption to protect data-at-rest might seem obvious, the reality is not that simple. If you are using an IaaS cloud service (public or private) for simple storage (e.g. Amazon's Simple Storage Service or S3), encrypting data-at-rest is possible—and is strongly suggested. However, encrypting data-at-rest that a PaaS or SaaS cloud-based application is using (e.g., Google Apps, Salesforce.com) as a compensating control is not always feasible.

Data-at-rest used by a cloud-based application is generally not encrypted, because encryption would prevent indexing or searching of that data. Data, when processed by a cloud-based application or stored for use by a cloud-based application, is commingled with other users' data (i.e., it is typically stored in a massive data store, such as Google's BigTable). Although applications are often designed with features such as data tagging to prevent unauthorized access to commingled data, unauthorized access is still possible through some exploit of an application vulnerability (e.g., Google's unauthorized data sharing between users of Documents and Spreadsheets in March 2009). Although some cloud providers have their applications reviewed by third parties or verified with third-party application security tools, data is not on a platform dedicated solely to one organization [O'Reilly Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and privacy].

An organization's data-in-transit might be encrypted during transfer to and from a cloud provider, and its data-at-rest might be encrypted if using simple storage (i.e., if it is not associated with a specification application).An organization's data is definitely not encrypted if it is processed in the cloud (public or private). For any application to process data, that data must be unencrypted. Until June 2009, there was no known method for fully processing encrypted data. Therefore, unless the data is in the cloud for only simple storage, the data will be unencrypted during at least part of its life cycle in the cloud—processing at a minimum[O'Reilly Tim Mather ,Subra Kumaraswamy ,Shahed Latif Cloud Security and privacy].

Even efforts to effectively manage data that is encrypted are extremely complex and troublesome due to the current inadequate capabilities of key management products. Key management in an intra-organizational context is difficult enough; trying to do effective key management in the cloud is beyond current capabilities and will require significant advances in both encryption and key management capabilities to be viable.

These concerns with data security do not negate the capabilities or advantages of utilizing storage-as-a-service in the cloud—for non-sensitive, non-regulated data. If customers do want to (simply) store organizational data in the cloud, they must take explicit actions, or at least verify that the provider will and can adequately provide such services, to protect their data stored in the cloud [15].

5. Privacy concerns

People of all ages care about privacy like: Who manages and access to data? Where is data stored? Do you know when data is breached?

Some of the privacy concerns are:

1. Who manages and have access to the data. Will data remain on the cloud even after termination of the service?

2. Legal and regulatory issues are extremely important in cloud computing that have security implications. To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider's policies and practices to ensure their adequacy. The issues to be considered in this regard include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion, trusted storage and trusted platform module access techniques can play a key role in limiting access to sensitive and critical data [16].

3. Where is the data in the cloud stored? What is the location of the data center?

Privacy laws in various countries place limitations on the ability of organizations to

transfer some types of personal information to other countries. When the data is stored in the cloud, such a transfer may occur without the knowledge of the organization, resulting in a potential violation of the local law.

4. Will you know when data is breached? How do you ensure that the Cloud service provider notifies you when a breach occurs, and who is responsible for managing the breach notification process (and costs associated with the process)? If contracts include liability for breaches resulting from negligence of the Cloud service provider, how is the contract enforced and how is it determined who is at fault?

5. Will data remain in the cloud even after deleting it as Cloud storage providers usually replicate the data across

multiple systems and sites—increased availability is one of the benefits they provide? This benefit turns into a challenge when the organization tries to destroy the data—can you truly destroy information once it is in the cloud? [15]

6. Security Enhancements for Cloud Computing

To improve the Security of cloud computing the following practices can be followed :

1. Security practices should be implemented at organizational level and make sure security policy of the service providers are in alignment with the business.

2. Security infrastructure should be maintained and employed in client side .The default passwords should be changed. Host side firewalls and antivirus programs should be installed . Antivirus updates must be done with out fail.

3. At both sides appropriates user permissions and restrictions should be allotted.

4. Encryption /decryption keys should be kept secured.

5. Providers should verify the authenticity of their clients.

6. Frequent data backup policy should be in place

7. System logs must be maintained with the following details users accessed the data, when, how much time was spend, and modifications made [27].

7. Conclusion

Cloud computing is in high demand. As the organization grows it has more resources, applications, services and data. Organizations are moving their data to cloud. Cloud characteristics bring in a set of Concerns and some sort of controls are required to reduce those concerns. Cryptography addresses the problem of security concern but encrypted data cannot be processed, indexed, or sorted, to do any of these important activities requires that the data be unencrypted—hence, a security concern, Especially if that data is in the cloud and is beyond the data owner's direct control.

Cloud computing has a lot of benefits but it has privacy and security concerns too like: Who manages and access to data? Where is data stored? Do you know when data is breached?

References

[1] Private Cloud Computing Essentials- 2 X Software white papers available at: http://www.2x.com/docs/en/whitepapers/pdf/Private_Cloud_Computing_Essentials.pdf

[2] NIST Definition of Cloud Computing. Peter Mell Timothy Grance NIST Special Publication 800-145 computer security .Computer Security Division Information Technology Laboratory .National Institute of Standards and Technology Gaithersburg, MD 20899-8930 September 2011 U.S. Department of Commerce Rebecca M. Blank.

[3] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1Prepared by the Cloud Security Alliance December 2009

[4] Cloud Computing basics available at: http://south.cattelecom.com/rtso/Technologies/CloudComputing/0071626948_chap01.pdf

[5] A survey of cryptographic algorithms for cloud computing Rashmi Nigori, Manoj Jhuria, Dr. Shailendra Singh. International Journal of Emerging Technologies in computational and Applied Sciences (IJETCAS). ISSn (print): 2279-0047, ISSN (online) : 2279-0055.

[6] Efficiency of Modern Encyrption Algorithm in cloud computing.Omer k jasmine, Safia Abbas, El-Sayed M.Horbaty and Abdel-Badeeh M. Salem International Journal of Emerging Trends of Technology in computer science (IJETICS) ISSN 2278-6856.

[7] Analyzing Data Security for cloud computing using cryptographic Algorithms. Gurpreet Kaur, Manish Mahajan Gurpreet kaur et al.int Journal of Engineering Research and Applications. ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.782-786

[8] Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing Manpreet Kaur, Rajbir Singh. International Journal of Computer Applications (0975 – 8887) Volume 70– No.18, May 2013

[9] Cloud Computing A collection of working papers Thomas B Winans John Seely Brown

[10] Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., et al. (2009). Above the clouds: A berkeley view of cloud computing. EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28.

[11] Boniface, M., Nasser, B., Papay, J., Phillips, S., Servin, A., Yang, X., et al. (2009). Platform-as-a-Service Architecture for Real-time Quality of Service Management in Clouds.

[12] Murphy, M., Abraham, L., Fenn, M., & Goasguen, S. (2009). Autonomic Clouds on the Grid. Journal of Grid Computing, 1-18

[13] Cryptography and Cloud Security Challenges Nitin Singh Chauhan and Ashutosh Saxena.CSI Communications

[14] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing Wiley Publishing, Inc. Indianapolis, Indiana 2010.

[15] Cloud Security and privacy An Enterprise perspective on risks and compliance.O'Reilly Tim Mather, Subra Kumaraswamy, Shahed Latif

[16] Security and Privacy Issues in Cloud Computing Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.

[17] Introduction to Cloud Computing.office of the privacy commissioner of Canada.Fact Sheet available at: http://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf .

[18] US-CERT united states computer Emergency Readiness Team The Basics of Cloud Computing Alexa Huth and James Cebula Available at: http://www.uscert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf.

[19] Cloud Computing Security Issues and Challenges Kuyoro S. O., Ibikunle F. & Awodele O. International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[20] Privacy, Security and Trust in Cloud Computing Siani Pearson HP Laboratories HPL-2012-80R1

[21] Bisong and S M Rahman, "An overview of the security concerns in enterprise cloud computing," CoRR, vol. abs/1101.5613, 2011.

[22] Cloud Computing Security and Privacy Issues: The Council of European Professional Informatics Societies LSI SIN (10)02 Source: Marko Hölbl Version: V17/15.032011Available at: http://www.cepis.org/media/CEPIS_Cloud_Computing_Security_v17.11.pdf

[23] Data Security In The Cloud Protecting Business-Critical Information In Public, Private and Hybrid Cloud Environments available at: http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud.pdf

[24] Addressing Data Security Challenges In he Cloud The Need for Cloud Computing Security A Trend Micro White Paper | July 2010. available at: http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_addressing-security-challenges-in-the-cloud.pdf

[25] NIST National Institute of Standards and Technology U.S department of commerce. Guidelines on Security and Privacy in Public Cloud Computing .Draft Special Publication 800-144.Wayne Jansen Timothy Grance.available at: https://cloudsecurityalliance.org/wp-content/uploads/2011/07/NIST-Draft-SP-800-144_cloud-computing.pdf

[26] zenith international journal of multidisciplinary research vol.2 issue 4, april 2012, issn 2231 5780.Security and privacy issues of cloud computing; solutions and secure framework prof: asha mathew assistant professor (research), welingkar institute of management development and research banglore.

[27] Securing the Cloud: Addressing Cloud Computing Security Concerns with Private Cloud .Available at: http://www.rackspace.com/knowledge_center/article/securing-the-cloud-addressing-cloud-computing-security-concerns-with-private-cloud

[28] Public Cloud Security Concerns Remain after Recent Study Available at: http://www.jurinnov.com/cloud-security/

[29] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." KM World, pp14-22.Available at: www.kmworld.com [Aug. 19, 2009].

[30] Private clouds Krishnan Subramanian Analyst & Researcher Krishworld.com.A whitepaper sponsored by Trend Micro Inc.

[31] Review A survey on security issues in service delivery models of cloud computing. S. Subashini n, V. Kavitha. Journal of Network and Computer Applications.