RESEARCH ARTICLE OPEN ACCESS

The Risk and Challenges of Cloud Computing

Usman Namadi Inuwa
M.Sc. Computer Science Department of Computer Science Jodhpur National University, Jodhpur Rajasthan, India

Abstract
Cloud computing is a computing technology aiming to share storage, computation, and services transparently among a massive users. Current cloud computing systems pose serious limitation to protecting the confidentiality of user data. Since the data share and stored is presented in unencrypted forms to remote machines owned and operated by third party service providers despite it sensitivity (example contact address, mails), the risks of disclosing user confidential data by service providers may be quite high and the risk of attacking cloud storage by third party is also increasing. The purpose of this study is to review researches done on this technology, identify the security risk and explore some techniques for protecting users' data from attackers in the cloud.

***Index Terms*:** Cloud Computing, Review, Security challenges, Threats.

I. INTRODUCTION

Computers have become absolutely necessary part of our life today. We need computers everywhere, be it for work, research or in any field. The computing resources we are using increases as the use of computer in our daily activities increase tremendously. For companies like Google and Microsoft, managing the resources when they need it is not a problem. But when it comes to smaller enterprises, affordability becomes a huge factor[25]. With the huge infrastructure come problems like machines failure, hard drive crashes, software bugs, etc. This might be a big headache for such a community. Cloud Computing offers a solution to this situation.

Cloud computing helps in minimizing an organization's expenditure towards managing resources and also reduces the burden of maintaining software or hardware by its user. Cloud computing is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. Cloud Computing is a computing platform for sharing resources that include infrastructures, software, applications, and business processes. Cloud Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet.

We are in the era in which information protection is the goal of every organisation. The rapid growth o f cloud computing has brought many security challenges for users and providers. And the risk of attacking both personal and organisational data store in cloud storage by an attacker is high as such computer expert are using many techniques for protecting users' data from unautherized party. This paper explore some of the approach use in protecting the confidentiality of users' data from service providers, and ensures service providers cannot collect users' confidential data while the data is processed and stored in cloud computing systems.

To Understand the security issues of cloud computing which affect the confidentiality and vulunerability of this kind of system, this paper give a brief history of cloud computing and explore the deployment models and the service delivery models to identify the threat

1.2 BRIEF HISTORY AND DEFINITION

Cloud Computing (CC) is a new term given to a technological evolution of distributed computing and grid computing[10].

The idea of computing in a "cloud" traces back to the origins of utility computing, a concept that computer scientist John McCarthy publicly proposed in 1961[3].

The general public has been leveraging forms of Internet-based computer utilities since the mid 1990s through various incarnations of search engines (Yahoo!, Google), e-mail services (Hotmail, Gmail), open publishing platforms (MySpace, Facebook, YouTube), and other types of social media (Twitter, LinkedIn)[3]. Without the development of ARPANET (Advance Research Projects Agency Network) by J.C.R.Licklider in 1960's and many other researchers who dream of improving the interconnection of systems, CC would never have come into existence[10].

A Gartner report listing cloud computing at the top of its strategic technology areas further reaffirmed its prominence as an industry trend by announcing its formal definition as[3]:

"...a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies."

Forrester Research provided its own definition of cloud computing as[3]:

"...a standardized IT capability (services, software, or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way."

The definition that received industry-wide acceptance was composed by the National Institute of Standards and Technology (NIST)[3]. NIST published its original definition back in 2009, followed by a revised version after further review and industry input that was published in September of 2011[10]:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[26].

This cloud model is composed of five essential characteristics, three service models, and four deployment models[3].

1.3 BENEFIT OF CLOUD COMPUTING

Before, people use to run applications or programs from software downloaded on a physical computer or server in their building. Cloud computing simplify this, cloud computing which is based on Internet allows people to access the same kind of application through the Internet[1].

But, why so many organization are moving to cloud? The reason may be the following:-

(1) Flexibility: The aim of every business organisation is to have more customers and today's business are all online as customer increase in accessing organisation application, the amount of data that an application handles is increasing day by day and so is the CPU power that can harness. Organisation needs more bandwidth a cloud-based service can instantly meet the demand because of the vast capacity of the service's of remote servers.

(2) Disaster Recovery: When an organisation start relying on cloud-based services, they no longer need complex disaster recovery plans. Cloud computing providers take care of most issues, and they do it faster. Aberdeen Group found that businesses which used cloud were able to resolve issues in an average of 2.1 hours nearly four times faster than those not on cloud[1].

(3) Automatic Software Update: In 2010, Uk companies spent 18 working days per month managing on-site security alone[1]. But today with cloud computing the providers do the server maintenance including security update within a short time, freeing up their customers' time and resources for other task.

(4) Work From Anywhere: As long as there is internet access customers' and organisation employee can access there information anywhere. In addition, since document are stored dirctly onto the cloud, anyone with authorized access can access the documents and work on the same project at the same time. Avoiding time lost and documents with several untrackable versions.

(5) Better for the Environment: Many small to corporate size companies require the use of mor servers to get jobs don because server utiliation rates are about 5-10%, whereas cloud utilization raates are int the 70% range, this is because cloud computing eliminates in-house servers, there is no need for the constant climate control involved in maintaing servers and elimanate carbon footprints.

(6) Security: Large number of laptops with vital 0information are report yearly stolen or loss. This can have some serious monetary implications, but when everything is stored in the cloud, data can still be accessed no matter what happens to a machine.

II. SECURITY ISSUES IN CLOUD COMPUTING

Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption [6]. Because Cloud Computing represents a relatively 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 and how applications security is moved to Cloud Computing [7]. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing [8].

2.1 SERVICE DELIVERY MODELS

2.1.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor’s dedicated resources are only shared with contracted clients at a pay-per-use fee. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications[4].

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.

2.1.2. Platform as a Service (PaaS)

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and offers an integrated set of developer environment that a developer can tap to build applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to maintenance [1].

2.1.3 Software as a Service (SaaS)

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

The architecture of SaaS-based applications is specifically designed to support many concurrent users (multitenancy) at once. The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure[4].

2.1.4 Anything as a Service (XaaS)

Anything as a Service (XaaS): This is more general form of representing deployment of a service. These services could be of any type and ‘X’ in XaaS can be substituted by software, hardware, infrastructure, data, business, IT, Security, monitoring, etc. These days new service models are being developed. Examples are: IT as a service, Cloud as a Service (CaaS), Management as a Service (MaaS), Storage as a Service, Hardware as a Service (HaaS), Identity as a Service, Privacy and Anonymization as a Service etc., are some other services that are identified in literature[10].

2.2 CLOUD DEPLOYMENTS MODELS

The Cloud Computing model has four main deployment models which are:

I. **Public cloud**: describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

II. **Community cloud:** is similar to a public cloud except that its access is limited to a specific community of cloud consumers. The community cloud may be jointly owned by the community members or by a third-party cloud provider that provisions a public cloud with limited access[1]. Membership does not necessarily guarantee access to or control of all the cloud's IT resources.

III. **Private cloud:**It is set up within an organization’s internal enterprise data center. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. 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.[12]

IV. **Hybrid cloud:** is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [14]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems.

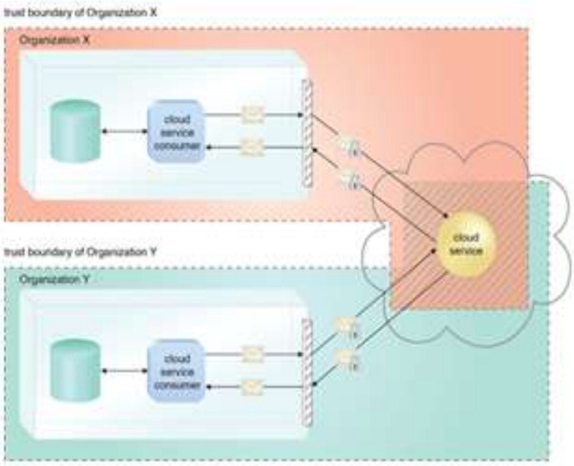
2.3 RISK AND CHALLENGES

Several of the most critical cloud computing challenges and the security risk pertaining mostly to cloud consumers that use one of the services described above located in clouds are examine

- **Increased Security Vulnerabilities**

The moving of private and organizational data to the cloud guarantee access to share the data with the cloud provider. The remote usage of the services requires an expansion of trust boundaries by the cloud consumer to include the external cloud. It can be difficult to establish a security architecture that spans such a trust boundary without introducing vulnerabilities, unless cloud consumers and cloud providers happen to support the same or compatible security frameworks which is unlikely with public clouds[3].There can be overlapping trust boundaries from different consumers who share the same cloud services and resources.

The overlapping of trust boundaries and the increased exposure of data can provide malicious cloud consumers (human and automated) with greater opportunities to attack IT resources and steal or damage business data[3].



Figur*es- 1 The shaded area with diagonal lines indicates the overlap of two organizations' trust boundaries.*

- **Reduced Operational Governance Control**

Cloud consumers are usually allotted a level of governance control that is lower than that over on premise IT resources. This reduced level of governance control can introduce risks associated with how the cloud provider operates its cloud, as well as the external connections that are required for communicate between the cloud and the cloud consumer.

- **Limited Portability Between Cloud Providers**

Due to a lack of established industry standards within the cloud computing industry, public clouds are commonly proprietary to various extents. For cloud consumers that have custom-built solutions with dependencies on these proprietary environments, it can be challenging to move from one cloud provider to another[3].

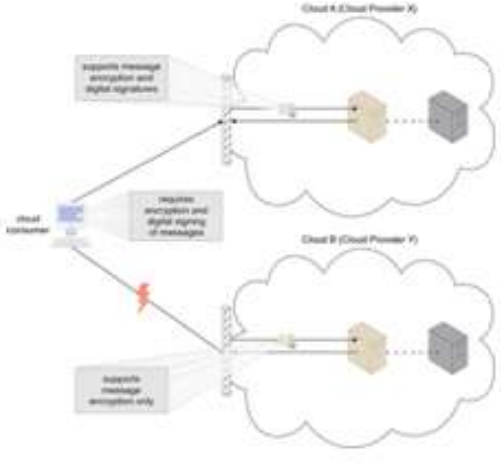

Cloud A (Cloud Provider X)
supports message encryption and digital signatures
cloud consumer
requires encryption and digital signing of messages
Cloud B (Cloud Provider Y)
supports message encryption only

Figure 2 - A cloud consumer's application has a decreased level of portability when assessing a potential migration from Cloud A to Cloud B, because the cloud provider of Cloud B does not support the same security technologies as Cloud A.

- **Multi-Regional Regulatory and Legal Issues**

Cloud providers establish there data centers in affordable or convenient geographical locations. There is transparancy of the physical location of their resources and the data hosted in the clouds. For some organizations, this can pose serious legal concerns pertaining to industry or government regulations that specify data privacy and storage policies. For example, some UK laws require personal data belonging to UK citizens to be kept within the United Kingdom.

Some countries have laws that require some types of data to be disclosed to certain government agencies or to the subject of the data. For example, a European cloud consumer's data that is located in the U.S. can be more easily accessed by government agencies (due to the U.S. Patriot Act) when compared to data located in many European Union countries[3].

2.4 THREATS IN CLOUD

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [12].

The threats to information assets residing in the cloud can vary according to the cloud delivery models used by cloud user organizations[17].

Cloud computing alliance did research in 2013 on cloud computing security threats and identified these threats[14].

υ Traffic Hijacking
υ Insecure Interface and APIs.
υ Denial of Service.
υ Malicious Insiders.
υ Abuse of Cloud Services.
υ Insufficient Due Diligence.
υ Shared Technology Vulnerabilities
υ Data Breaches
υ Unknown Risk Profile
υ Perimeter Security Model Broken

2.5 PROPOSED SOLUTION

Cloud providers should address information security and privacy risks associated with deploying information into any cloud computing environment. Below are some proposed solution to the issues discuss

ν Cloud providers should ensure that data in the cloud environment is tamper proof, protected through encryption at the kernel level. Communication between the customer and the provider's server is secure, thus avoiding the risk of any man-in-the-middle attacks to gain access to the encryption keys.

- Cloud provider should use industry standard AES encryption to make data unreadable and unusable to those without the encryption key. Rendering the data useless greatly reduces the risks associated with data theft, exposure to unauthorized parties or data seizure through judicial subpoena.
- Providers should provide a unique policy-based approach to key management and data access which allows users to determine exactly which server gets access to secure data.

III. CONCLUSION

As Individuals, government and non-governmental organization, small and large scale enterprises make plans to deploy their data and other applications in private, community and public cloud environments, new security challenges need to be addressed. Optimal cloud security practices should include encryption of sensitive data used by cloud-based virtual machines; centralized key management that allows the user (and not the cloud provider) to control cloud data; and ensuring that cloud data is accessible according to established enterprise policies.

This paper discuss the benefit of using cloud computing, the risk and challenges of this new technology and the threat that are emerging which attack the confidentiality and vulnerability of the information in cloud. At the end proposed solution for safeguarding information in both private, public, community cloud services were cited.

REFERENCES

[1] Why Move to the cloud? http://www.salesforce.com/uk/socialsucess/cloud-computing/why-move-to-cloud-10-benefits-cloud-computing.jsp 24/10/2015 15:03

[2] Ken E. Stavinoha "What is cloud computing and why do we need it?" http://isacahouston.org/documents/WhatisCloudComputingandWhyDoWeNeedIt.pdf 27/10/2015 00:09

[3] http://whatiscloud.com/cloud_deployment_models/ 27/10/2015 2:01

[4] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013), An analysis of security issues for cloud computing, Journal of Internet Services and Application

[5] Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011

[6] KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey.. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/238429

[7] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487

[8] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA

[9] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy (2011) Cloud Computing: Security Issues and Research Challenges, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011

[10] Santosh Bulusu, Kalyan Sudia (2012), A Study on Cloud Computing Security Challenges, Masters Thesis: School of Computing Blekinge Institute of Technology SE-371 79 Karlskrona Sweden.

[11] Prince Jain (2012), Security Issues and their Solution in Cloud Computing, International Journal of Computing & Business Research - ISSN (Online): 2229-6166

[12] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), 39-51, University of Texas, USA, April-June 2010.

[13] Thomas Erl, Zaigham Mahmood, Ricardo Puttini "**Cloud Computing: Concepts, Technology & Architecture**

[14] Rajani Sharma, Rajender Kumar Trivedi (2014) "Literature review: Cloud Computing –Security Issues, Solution and Technologies" International Journal of Engineering Research Volu me No.3, Issue No.4, pp : 221-225

[15] Mohammad Sajid,Zahid Raza (2013), "Cloud Computing: Issues & Challenges", International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV

[16] Patrick Höner "Cloud Computing Security Requirements and Solutions: a Systematic Literature Review"

[17] Jaydip Sen, "Security and Privacy Issues in Cloud C loud Computing"

[18] Monjur Ahmed, Mohammad Ashraf Hossain "CLOUD COMPUTING AND S ECURITY ISSUES IN THE CLOUD" International Journal of Network Security & Its

Applications (IJNSA), Vol.6, No.1, January 2014

[19] Sharma, Rajeev, and Bright Keswani. "STUDY& ANALYSIS OF CLOUD BASED ERP SERVICES."

[20] A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[21] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[22] R. L Grossman, “The Case for Cloud Computing,” IT Professional, vol. 11(2), pp. 23-27, 2009, SSN: 1520-9202.

[23] B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[24] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, “On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[25] Maheswaran.M (2008) “CLOUD COMPUTING”, seminar report, school of engineering cochin university of science and technology, cochin – 682022

[26] Patricia Yancey Martin and Barry A. Turner. Grounded theory and organizational research. The Journal of Applied Behavioral Science, 22(2):141–157, April 1986.