Cloud Computing: The most important tectonic shift in IT

Abstract

Cloud computing has become the hotshot topic since Amazon's rollout of the first of its kind of cloud services in the year 2006. The enormous amounts of data that are being processed daily in various sectors, and there are signs that subscription to cloud services by the local companies will soon be on a skyrocket course, despite a slow start in previous years. This paper emphasizes on various issues and the zenith to which the cloud computing services would reach. It touches upon the history and introduction of cloud computing, it focusses on the services which cloud computing provides. This brief talk will outline some of the concerns pertaining to the further development of cloud computing into a sophisticated technology that meets its indigenous goals along with some countermeasures.

Introduction

Cloud computing follows its causes back to the 1960s when the PC business perceived the potential advantages of conveying figuring as an administration or a utility. Be that as it may, early processing came up short on the network and data transmission expected to execute figuring as a utility. It wasn't until the expansive accessibility of web transmission capacity in the late 1990s that registering as an administration wound up handy. In the late 1990s, Salesforce offered one of the main industrially fruitful usages of big business SaaS. This was pursued nearly by the entry of AWS in 2002, offering a scope of administrations, including capacity and calculation - and now grasping databases, machine learning, and different administrations. Today, Microsoft Azure, Google Cloud Platform and different suppliers have joined AWS in giving cloud-based administrations to people, independent ventures and worldwide endeavors.

The delivery of on-request computing resources everything from applications to data centers over the web on a compensation for-use premise. Cloud computing brags plenty appealing advantages for organizations and end clients. End clients can turn up process assets for a remaining task at hand on interest. This takes out the conventional requirement for IT admins to provision and manage resources. Organizations can scale up as processing needs increment and scale down again as requests decline. This wipes out the requirement for gigantic interests in the nearby framework, which might possibly stay active. Compute resources are estimated at a granular dimension, empowering clients to pay just for the resources and workloads they use.

Cloud computing can be divided into three broad service categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). IaaS providers supply a virtual server instance and storage, as well as APIs that enable users to migrate workloads to a VM. Users have an allocated storage capacity and can start, stop, access and configure the VM and storage as desired. IaaS providers offer small, medium, large, extra-large and memory- or compute-optimized instances, in addition to customized instances, for various workload needs. In the PaaS model, cloud providers host development tools on their infrastructures. Users access these tools over the internet using APIs, web portals or gateway software. PaaS is used for general software development, and many PaaS providers host the software after it's developed. Today's most common PaaS providers include Salesforce's Force.com, AWS Elastic Beanstalk, and Google App Engine. SaaS is a distribution model that delivers software applications over the internet; these applications are often called web services. Users can access SaaS applications and services from any location using a computer or mobile device that has internet access. One common example of a SaaS application is Microsoft Office 365 for productivity and email services.

Cloud computing Act

Sen. Amy Klobuchar has introduced a new bill, the "Cloud Computing Act of 2012" (S.3569), that purports to "improve the enforcement of criminal and civil law with respect to cloud computing." All I could think is that the Cloud Computing Act of 2012 is a group of proposed amendments to the Computer Fraud and Abuse Act that aim to “protect cloud-based businesses.”[1] Cloud Computing Act of 2012 amends the Computer Fraud and Abuse Act to provide that each instance of unauthorized access of a cloud computing account, access of such an account more than authorization, or an attempt or conspiracy to access such an account without or more than authorization in violation of such Act shall constitute a separate offense. It defines "cloud computing account" as information stored on a cloud computing service that requires a password or similar information to access and is attributable to an individual; and "cloud computing service" as a service that enables convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or interaction by the service provider.

But the two major things which the Cloud Computing Act of 2012 does are it establishes that each breach of a “cloud computing account” counts as a separate CFAA offense and it also sets the pecuniary penalty floor at $500 per violation. [1] In brief, the CFAA is a wide-ranging act, covering activities such as fake profiles, data scraping and former employees stealing sensitive information. It prohibits individuals from knowingly or intentionally accessing a computer without authorization or exceeding authorization provided. It is designed to punish hackers of computer systems and others who damage computer systems and misappropriate confidential and sensitive information about clients and customers without the requisite approval.

However, as per Eric Goldman, who is a law professor at Santa Clara University School of Law and Director of the law school's High-Tech Law Institute the Cloud Computing Act of 2012 could cause many more

problems than it would provide protection. He feels that It's flashy for legislators to tell their constituents that they are fighting hard to protect emerging technologies like "cloud computing." But legislators rarely understand cutting-edge technologies, and usually, rapidly evolving technologies are poor candidates for legislative intervention. He also made a point that this bill increases the CFAA's complexity with minimal or zero commensurate benefits. [2] He feels that if Sen. Klobuchar or anyone else really wants to fix the CFAA, a good start would be to reduce the law's length, organize it better, and reduce its implications for users' ordinary Internet activity. Also, critics strongly argue that the bill is not much different from the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) that triggered an internet blackout protest in January 2012. The only difference is that the Cloud Computing Act hasn't garnered the same level of media attention.

Also, the bill might be used to restrict freedom on the internet, given how the definitions can apply to most interactive websites. Critics argue that there is a chance that the bill will be abused, and even seemingly minor offenses could be charged as federal crimes.

The Boom factors of cloud technologies

Cloud providers are competitive, and they constantly expand their services to differentiate themselves. This has led public IaaS providers to offer far more than common compute and storage instances. For example, serverless, or event-driven computing is a cloud service that executes specific functions, such as image processing and database updates. Traditional cloud deployments require users to establish a compute instance and load code into that instance. Then, the user decides how long to run -- and pay for -- that instance.

Google and Microsoft have also played a pivotal role in the emergence of the cloud computing market by offering cloud-based services somewhat like Amazon's. Since its foundation as a search engine company,

Google has always delivered services to customers over the “cloud” - the Internet - and was also the first to publicize the Internet-based, on-demand shared service model as “cloud computing”. In 2008, Google officially became a major player in the cloud computing market by launching the Google App Engine, a platform for users to develop and run Web applications on Google’s infrastructure. Microsoft, with its long history of selling desktop software to businesses, also transitioned into a leader in cloud computing. In 2010, Microsoft launched the commercial version of Azure, which, like Google, provided development and hosting environments on Microsoft’s data centers.

With serverless computing, developers simply create code, and the cloud provider loads and executes that code in response to real-world events, so users don't have to worry about the server or instance aspect of the cloud deployment. Users only pay for the number of transactions that the function executes. AWS Lambda, Google Cloud Functions, and Azure Functions are examples of serverless computing services.

Public cloud computing also lends itself well to big data processing, which demands enormous computer resources for relatively short durations. Cloud providers have responded with big data services, including Google Big Query for large-scale data warehousing and Microsoft Azure Data Lake Analytics for processing huge data sets. Another crop of emerging cloud technologies and services relates to artificial intelligence (AI) and machine learning. These technologies build machine understanding, enable systems to mimic human understanding and respond to changes in data to benefit the business. Amazon Machine Learning, Amazon Lex, Amazon Polly, Google Cloud Machine Learning Engine and Google Cloud Speech API are examples of these services.

It is worth noting that several niche players, especially like Salesforce.com, also pioneered cloud computing market by providing “software as a service” over the Internet since the early 2000s. The second major category of vendors in the cloud computing market includes the traditional IT service firms, such as

IBM and HP. These firms specialized in providing customized IT and business outsourcing services to a limited number of clients, especially large enterprises, rather than mass market. Although their business models were significantly different from those of Amazon, Google, and Microsoft, these incumbent IT firms actively expanded in the cloud computing market by initially focusing on the "private" cloud segment. Private clouds are custom-built and operated by vendors for their clients, with the objective of capitalizing on the clients' existing IT infrastructure while improving its efficiency and effectiveness. The client firms also have the option to transition to "hybrid" cloud, that is, a mix of private and public clouds, and eventually fully utilize public clouds. Recently, IBM launched its next-generation Smart Cloud, which targeted large enterprises while HP has been promoting its "HP Hybrid Delivery" solution since 2011.

Issues concerning cloud computing

Cloud computing services have become ubiquitous these days. It is so prevalent that any interaction with the internet generates a web footprint that is saved somewhere in the cloud. The access to that kind of sensitive and personal information must be controlled otherwise it could lead to data abuses resulting in some criminal activity. This access control of data is usually done by the cloud service providers and they are bringing upon themselves a big risk. With the increase in the use of cloud computing services such as Gmail, Facebook, LinkedIn, etc. privacy concerns of cloud computing services have become pressing issues of utmost importance. The cloud service provider must take up the responsibility for privacy while giving access to a plethora of data to users. There is an immense risk of data leaks either accidentally or deliberately.

Data Security and Privacy in Cloud Computing

The following is a meaningful way to define Privacy found in the journal page: Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively. Privacy has the following elements.

I. When: a subject may be more concerned about the current or future information being revealed that information from the past.

II. How: a user may be comfortable in his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.

III. Extent: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

Usually in data centers, where data is stored in-house and is managed by a dedicated IT department. But the cloud is an off-premise system in which users outsource their data needs to a third-party provider. The third-party provider does everything from performing all updates and maintenance to managing security. However, the more important thing here is that users are trusting their data for someone else to look after, said Steve Santorelli, a former Scotland Yard detective, now manager of outreach at the Internet security research group Team Cymru. "The downside is that you are abrogating responsibility for your data. Someone else has access to it and someone else is responsible for keeping it safe," Santorelli said. Although cloud providers may ensure your data is safe, some are not always looking after your best interests. They are in the business of making money from the clients/users, after all.

Some Privacy Issues:

- Attackers can abuse the cloud service and acquire extra data or destroy the interests of other users. This may lead to the cost increase of cloud service.
- Cloud systems should be capable of averting Denial of Service (DoS) attacks.

- Use a trusted third party independent approach for Identity Management to use identity data on untrusted hosts.

Countermeasures:

I feel that clients can make use of cryptographic procedures, to mitigate and safeguard the confidentiality and integrity of their outsourced data. Also, when the fact is about availability, when it comes to availability, the use of multiple data centers, ideally in different regions, is the only efficient solution, if the cloud provider will not face a global outage. Stringent separation of duties for the provider employees and especially system administrators is one of the most effective mechanisms for limiting the potential damage of those attacks.

Cyber attacks on cloud

There is a risk of cyberattack, every time you store data on the Internet. This is particularly problematic on the cloud, where huge volumes of data are stored by a variety of users on the same cloud system.

One major concern is the vulnerability to Distributed Denial of Service(DDoS) attacks and the concentration of so much data. Cloud is the single point of failure and If something goes bad it impacts a very wide group of people and It is easier to steal and disrupt in bulk. Although most cloud providers have stringent security measures, as technology becomes more sophisticated, so do cyber attacks. When cloud companies get the security right — and many do a reasonable job — then it makes it impossible for miscreants to get their hands-on data.

For example, a Cyber Attack launched by some state-sponsored hackers on a Portland-based Cloud Computing Company named Cedexis resulted in a bunch of news websites going dark. And as per Bloomberg, the knocked off news sites were most popular in France and had a very good reader base and

bounce rate. The hack took place at 7 am Pacific Time on the Cedexis Infrastructure being hosted in a US Data Center in the form of a DDoS attack. Distributed Denial of Service (DDoS) attack is a form of cyber-attack where servers hosting critical data and applications are bombarded with fake traffic. Cedexis confirmed that the attack caused a partial but widespread outage affecting its premium customers from France and the service provider is still busy in restoring and mitigating the risks. And as per sources of Cybersecurity Insiders, more than 13 websites related to manufacturing companies of France were also down due to the attack.

Countermeasures:

I strongly feel that organizations can avoid or reduce and mitigate the impact of an attack on their company if they use the correct cloud strategy when controlling their security. Having worked in a software company, I do understand the criticality of web servers. Encapsulating the browser into a VM and operate on a separate hardened guest operating system. Apart from this, even web filters can be used which will block infected websites and analyses loaded data and checks for any malicious codes in the system.

Insider threats on the cloud

Security breaches from inside are on the rise just as cyber attacks. For Example, Vodafone's breach of 2 million customer records and the Edward Snowden breach at the NSA are wake-up calls that the most serious breaches are due to insider threats and privileged user access. Everything from customer data to confidential information and intellectual property is up for grabs once the company misplaces access control to the cloud in the wrong hands.

This is also more difficult for companies to avoid as the cloud makes this problem 10 times worse since administrative access to the cloud management platform, either by an employee or an attacker posing as

an employee, enables access to copy and steal any virtual machine, undetected, as well as potentially destroy the entire cloud environment in a very less time.

Insider attacks can be executed by malicious employees at the provider's or user's location. This threat can break the trust of Cloud users on the provider. A malicious insider can very easily obtain passwords, cryptographic keys, and files. These attacks may include many types of fraud, damage or theft of information and misuse of IT resources. The threat of malicious attacks has enhanced due to the lack of transparency in Cloud provider's processes and procedures. It means that a provider may not reveal how employees are granted access and how this access is monitored or how reports, as well as policy, are analyzed. Additionally, users have little visibility about the hiring practices of the provider that could open the door for an adversary, hackers or other Cloud intruders to steal confidential information or to take control over the Cloud. The level of access granted could enable attackers to collect confidential data or to gain complete control over the Cloud services with little or no risk of detection.

Malicious insider attacks can damage the financial value as well as the brand reputation of an organization. Moving critical applications and sensitive data to a public and shared Cloud environment is a major concern for the organization. That is because the organization has lost control of the data and totally depends on Cloud provider data security and defense. To alleviate these concerns, a Cloud solution provider must guarantee that customers can remain to experience the same security and privacy controls over their applications and services by providing evidence to these customers that their organization and customers are secure.

Countermeasures:

It's the responsibility of the organization to have a complete understanding of the users (i.e., employees and stakeholders) behavior in the cloud, including detailed and granularity about the devices, services, activities, and locations, to make well-informed policy choices. Granular visibility will help the company

target careless or malicious insider behavior without getting in the way of the legitimate use of your cloud services. This can be accomplished using various tools available in the industry today.

Government intrusion on cloud computing services

After the recent NSA leaks and the consequences on government surveillance programs, competitors aren't the only ones who may want to get access to the sensitive data. [14]

It is also possible that government entities and technology companies in the U.S. and elsewhere may be inspecting your data as it is transmitted or where it resides on the Internet, including within clouds. Although it is a well-known fact, that privacy has always been a concern with the cloud, businesses now must worry about government intrusion as well. This doesn't change the threat of Loss of confidentiality to data. It is just that the sources of threat sources might not have been same companies that were previously worried about.

Countermeasures:

I think a cloud service provider should be selected based on to what extent they can fight the government to protect user data. Unless a warrant is produced, the data should not be handed over to the government. There should be transparency between the provider and the user if the access to personal data is given to the government. Since protecting user data is the main objective for the providers, they should be willing to even fight for user privacy rights in the courts or with Congress.

Legal liabilities concerning cloud computing services

As with several other changes in the landscape of cloud computing, certain legal issues arise with cloud computing, including trademark infringement, security concerns and sharing of proprietary data resources. [6]

One of the major problems with cloud computing, often not mentioned, is the problem of who is in "possession" of the data. If a cloud company is the possessor of the data, the possessor is entitled to certain legal rights. If the cloud company is the "custodian" of the data, then a different set of rights may apply. The second major problem in the legalities of cloud computing is the problem of legal ownership of the data. Many Terms of Service agreements are silent on the question of ownership and they do not explicitly mention this [8].

These legal issues are not limited to the time in which the cloud-based application is actively being used. There must be a consideration for what happens when the provider-customer relationship ends. [8] In most of these cases, this event will be addressed before an application is deployed to the cloud. However, in the case of provider insolvencies or bankruptcy, the state of the data may become blurred along with the ownership of it.

Countermeasures:

I think it is important to have clear Terms of Service Agreement where both parties involved lay out clear guidelines or principles on who possesses the data and who holds the legal ownership of it even before a business engagement.

Lack of standardization of cloud computing

What makes cloud computing safe? A provider may have the latest security features, but there are no clear standards established for general safety measures. This general lack of standardization, no clear-cut guidelines makes it difficult to unify cloud providers. Further, given the plethora of cloud services in different sectors, this is especially problematic for users when determining or assessing exactly how "safe" their cloud really is.

The extent of cloud safety has many facets, and the answer depends on the cloud services provider, the type of industry a company is in, and the accompanying regulations concerning the data it is considering storing in the cloud. Since not all cloud providers are built the same, their respective definitions of safety are not the same as others.

Countermeasures:

It is difficult to bring all the cloud providers under one umbrella since they cater to a variety of applications, but a generic framework on a higher level that can address the different types of cloud applications. It is not impossible, but we have a lot of ground to cover.

Cloud service's lack of support

Imagine being unable to access your cloud before a big meeting or, worse, being in the middle of a cyber attack that has taken down your entire bread and butter —your website. Now imagine trying to contact your provider, only to find that their customer service is nonexistent. While some cloud providers have excellent customer support, others could leave you in the cold [5].

The most frustrating thing when something goes wrong is not being able to speak directly with an engineer. "If your systems are not mission-critical, you don't need to worry so much about security and availability," Sage said. "However, if you support mission-critical systems, or your online presence is critical for your business to operate smoothly, you have to be prepared to invest in a cloud and cloud provider that is capable of providing a level of protection commensurate with your needs."

Although that in earlier days of cloud computing, poor customer service was a constant complaint from users, fortunately, now most vendors have made great steps in improving technical support over the past few years, but that support comes for a price. Google's basic "Silver" support package for their cloud

platform currently costs $100/month, which has four-hour response time (during business hours only) and does not include phone support. Other cloud vendors have similar support options [5].

Countermeasures:

This is a difficult task to avoid. However, some measures can be taken from organization's end on this. The first and foremost step to take in is to thoroughly read the terms and conditions of the cloud contract before signing up. Those often specify restrictions on the access method, duration availability and associated cost for extracting data from a cloud application or repository. For example, AWS Redshift is a stealth approach to lock-in.

There's always a risk

The biggest risk when it comes to cloud computing is that you never know what is up ahead. Hackers have been around from the start and they are not going anywhere any time soon. And as technology advances, so do the risks that come with adopting them.

Cloud services gather data from thousands of small businesses. The small businesses believe that by pushing their data on cloud maintained by a larger firm their data is safe and secure. However, each business that uses a cloud service increases the value of that service as a potential target. This concentrates risk on a single point of failure. A disaster at a cloud provider can affect every one of its customers. If a company outsources the processing or storage of data that it is required to protect, then it is relying on a cloud service provider to maintain their compliance. If the company does not have adequate legal protections, then it may be liable when there is a data breach at the cloud service that exposes the company's data [4].

Countermeasures:

I feel that for business using or planning to migrate to the cloud, all one can do is prepare for it. The key here is getting to know providers as much as one can, both as a company and from an end-user perspective. Also, It is impossible to shield the cloud from all types of risks, but efforts can be put in place to make sure that all the previously mentioned risks are thoroughly checked at regular intervals.

Conclusion:

To conclude, Cloud computing is, of course, the latest technology that promises immense benefits. There is a lot of research which is still required in this area. Many of the concerns related to security and privacy issues are not been answered by the experts as yet and it remains open. However, there is a lot of research and investment as well in the same by technology giants like Microsoft, Google, Cisco, IBM and I feel that the day is not far when the cloud will be widely adopted meeting all the security, legal and privacy issues.

References:

[1] Cloud Computing, https://www.ugc.edu.hk/doc/eng/rgc/theme/hall/abs2.pdf

[2] The Proposed "Cloud Computing Act of 2012," and How Internet Regulation Can Go Awry https://www.forbes.com/sites/ericgoldman/2012/10/02/the-proposed-cloud-computing-act-of-2012-and-how-internet-regulation-can-go-awry/

[3] INTRODUCING THE CLOUD COMPUTING ACT OF 2012, http://www.aaronkellylaw.com/introducing-the-cloud-computing-act-of-2012/

[4] Top 5 Risks of Cloud Computing, https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/

[5] The Cons of Cloud Computing for Business, https://www.thebalancesmb.com/disadvantages-of-cloud-computing-4067218

[6] THE LIABILITY ISSUES of CLOUD COMPUTING SERVICE PROVIDERS, Jan 2012, https://www.advisenltd.com/wp-content/uploads/liability-issues-of-cloud-computing-service-providers-2012-02-12.pdf

[7] Top Five Legal Issues For The Cloud, https://www.forbes.com/2010/04/12/cloud-computing-enterprise-technology-cio-network-legal.html#1427f1402ebe

[8] Cloud Computing Legal issues, https://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf

[9] Lack of Standards in the Cloud, https://telecomreseller.com/2011/06/22/lack-of-standards-in-the-cloud/

[10] The Problem with Cloud-Computing Standardization, https://www.infoq.com/articles/problem-with-cloud-computing-standardization

[11] https://www.businessnewsdaily.com/5215-dangers-cloud-computing.html

[12] https://cloudacademy.com/blog/disadvantages-of-cloud-computing/

[13] https://journals.sagepub.com/doi/full/10.1155/2014/190903

[14] Is your cloud data safe from government searches? https://iapp.org/news/a/is-your-cloud-data-safe-from-government-searches/

[15] The Insider Threat in Cloud Computing, https://pdfs.semanticscholar.org/b510/fc913adc1bc248329bd26f0e7656adfb0e7c.pdf