International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 12|| December 2017 || PP. 31-36

Data security in Cloud Computing

Dr. Deepak Chahal[1],Dr.Latika Kharb[2] ,Tarun Punia[3]
[1,2]*Associate Professor (IT), Jagan Institute of Management Studies, New Delhi. India.*
[3]*Student Scholar(MCA), Department of IT, Jagan Institute of Management Studies, New Delhi. India.*
Corresponding Author: Dr. Deepak Chahal[1]

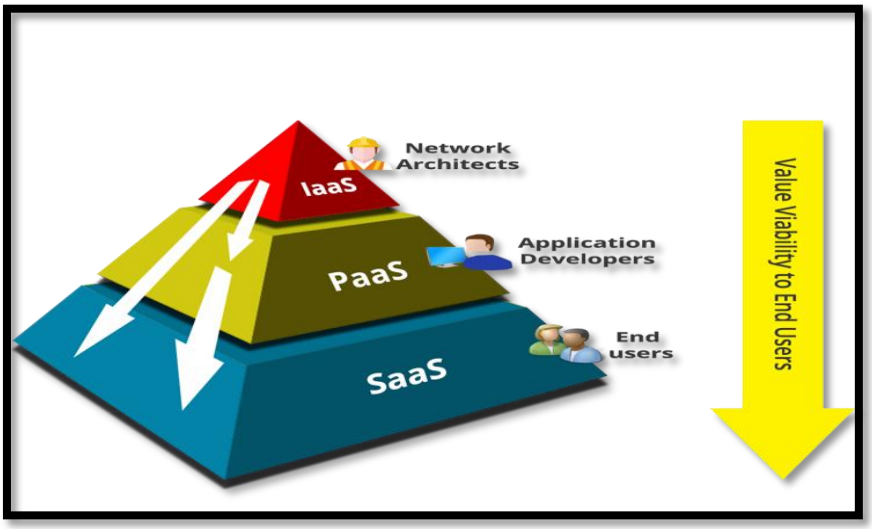
Abstract: *Data security means the protection of digital data from fortuitous or coincidental but unauthorized access such as data breach or cyber attacks. Data security has incessantly been a crucial matter in information technology. But in the world of cloud computing, it has become an extremely serious issue as data is located in different places/ location. Data security and data privacy are very interrelated and are the main concern in cloud technology for many users. Data security and privacy are the two main issues that an organization will need to address while considering a cloud computing solution. They are also relevant to both hardware and software components in cloud infrastructure such as servers/ storage as hardware requirements and a network and virtualization tool as a software requirement- in order to support the computing requirements of the cloud computing model. The aim of this study is to determine the various challenges for security in order to protect digital data in the cloud. And how can we maintain a balance between privacy and security in the digital age. In this paper, we have highlighted on security challenges in cloud based environment and its solutions.*

Keywords: *Data security, cloud computing, data privacy, data breach, data confidentiality, data availability, data integrity.*

Date of Submission: 14-12-2017 Date of acceptance: 28-12-2017

I. Introduction

In today's world organization around the globe are using cloud services. Cloud computing is the process of delivery of computing services. If you use an online service to send an e-mail, you are most probably using the cloud services. Let just take an example to understand this topic well. Imagine you start a company and you have a website for that company. The website is hosted on a server which you bought for your small company and your company is growing and growing and more people are visiting your site. Soon enough you start encountering issues with your website. Since the traffic on the site is very high and a lot of people are visiting it at the same time, the service slows down and the equipment cannot keep up which means that website slows down and because of that less and less people are visiting it. At this point you start losing you website's popularity. What do you do to resolve this issue? You probably need more servers to resolve this problem and set them up but it's very expensive, you have to pay for the installation and the servers and the IT support but you have no other choice.

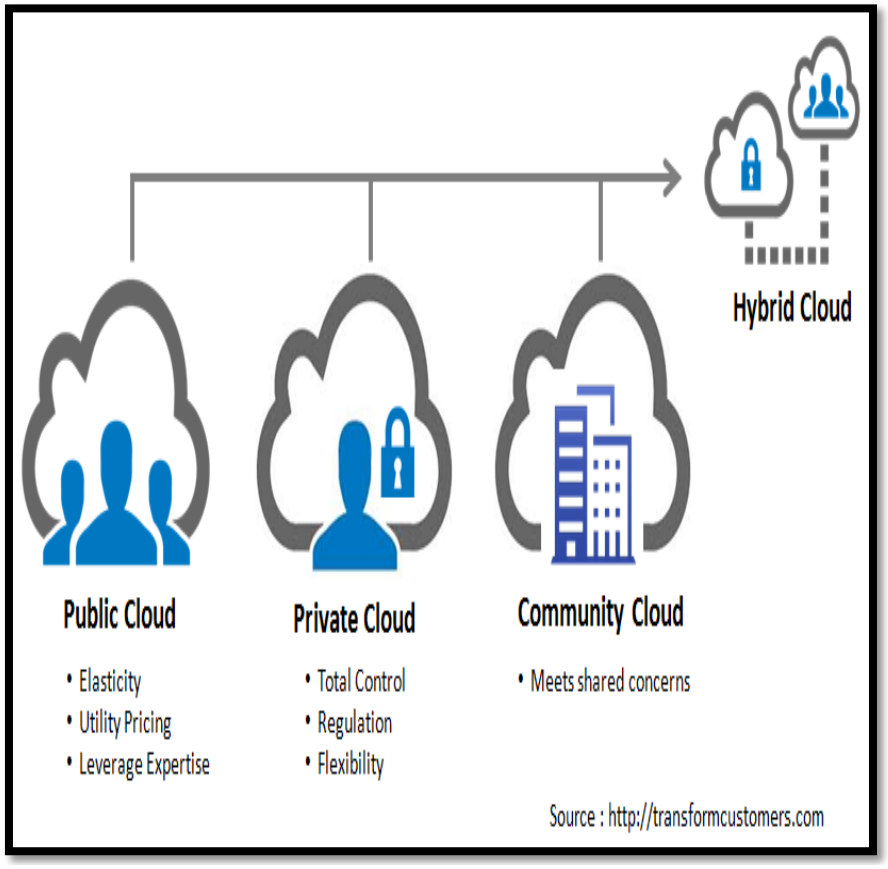


Now with cloud computing you don't have to buy any physical equipment, it is all online and it is always available. You only pay for the power when you need the power, you can turn it off and on almost instantly and scale and up and down instantly to fit what you need when you need it. It is a lot cheaper and more effective. You don't have to focus on hardware, you can now focus on growing your company and you are saving time and money. With the help of cloud computing you can create new apps and services, deliver software on demand, host websites and blogs, store, back up and recover data, stream audio and video, analyze data for patterns and make prediction.

There are so many reasons that organizations are turning to cloud services these days- first it is a cost effective method in which you can eliminate capital expenses of buying hardware and software, datacenters set-up and run. It maximizes speed giving businesses a lot of flexibility, cloud computing helps organization to work more elastically on a global scale giving the right amount of IT resources. It also helps in achieving more productivity, on-site datacenter requires a lot of "racking and stacking" – from hardware setup to software patching, the racks of servers, around the clock electricity for power and cooling, and the IT experts for managing the infrastructure, all these can add up in cloud computing and the It team can spend their time on more important business goals.

Cloud computing consists of three service models:

- IAAS: In infrastructure as a service you can find scalable it solutions resources are available when you need it. A physical hardware is set up and maintained by the cloud service provider which save your time and cost, you can easily accessed the service demanded and have to pay for the resources that you actually use. Services can be accessed from anywhere using the internet within the cloud security protocol. It provides basic computing resources as a service compute, storage, networking etc. it typically offers some virtual machine that has some operating system running on it, installed on it, so that you are able to remotely connect to that machine.
- PAAS: In Platform as a service, there is a provision of the hardware and software to create environments porting application design development and delivery thus reducing the capital investment of quite start up a new business.
- SAAS : Software as a service is a pretty simple thing its one of those things that most people are already used to most people are already using. When users borrow any online software instead of purchasing it: for e.g. people are using Gmail or yahoo mail services.



There are three types of cloud namely: public cloud, private cloud, and hybrid cloud. Public cloud is cost effective method which are owned and managed by the cloud service provider, they provide computing resources and all the hardware, software and IT infrastructure is owned and managed by cloud provider. The data used in public cloud resides in a multi-tenant environment so there are risks of data security and also because services are running on the public cloud or in the multi-tenant environment which means the server's is implemented and shared across multiple users that are using the services connecting to the public cloud where is just minimal control or customization that the user has been easy oh she's using the service on the public hawk. Private cloud where the services and infrastructure are maintained on a private network, this is basically used when there are security concerns and availability requirements and this offers the greatest level of security and control when compared the other two types.

A hybrid cloud is the combination of private cloud incorporated with the use of public cloud services. The actual goal is to combine these services and data from a variety of cloud models to create a unified and automated computing environment. It allows organization for public cloud platform providers. Without offloading the entirety of their data to a third party data center so this provides a great deal of flexibility in the computing tasks while keeping the most vital components within the company firewall. Community cloud is the multitenant cloud service model that is shared among various organization and that is governed managed and secured commonly by the entire participating organization or a third party managed service provider.

The Security Issues Of Cloud Storage

Privacy has been associated with physical access. The danger of cloud storage so this is about storing your personal information online effectively a backup or even maybe a primary copy of your hard drive online. Social media is largely responsible for that. When the internet was first commercialized in the early 90s we were all told be very careful online, do not share any personal information, don't include your real name if you are on a chat, don't put up your photographs, don't give your birth dates, don't do all these things and social media has made us more social, they kind of softened us up and primed us for where we are now which is where we just freely giving away our information to market ears to companies to businesses so we are putting up this information about what we did this weekend where we work our interest our friends our family everything so the next logical step is cloud storage.

There are number of areas of concern it begins a cloud backup and then it eventually becomes like chrome book type technology but in future there are tablets and smart phones and laptops won't have their inbuilt storage they'll be in or they may be hybridized to a certain degree reliant on the cloud to get most of their data to retrieve most of your information we already have this with your gmail account and I think youtube is a sort of cloud as it stores videos then we have facebook and twitter, Pinterest and all these other social media forms are all forms of cloud as well because there are some degree of storage but in the strictest sense cloud-based backup for many people can become cloud-based primary storage as well so wifi becomes more prevalent everywhere and we're constantly connected all the time and they're you know to get harder and harder to find a place where you're not we don't have a signal, it just becomes more of like opportunity for cloud-based storage to become a big deal and in that respect it means that these devices will become nothing more than dumb terminals reliant on the internet.

So I think social media has played into that, it's basically made us much more trusting overly so of these organization who may not necessarily have our best interests at heart. If you have a gmail account you know the occasion to get these little ads or you know things that you have bought on amazon for example you may get alerted to things so you like this or maybe you like this they target based on the content of your email or based on the content if you got as I say an amazon or ebay account based on things that you purchase so what's to say that they don't conduct some sort of analysis on the data that's on your hard drive which means that they scan some files and it's crazy to think that they were able to perform that analysis.

A few years ago cloud-based storage is really taken off because of ubiquity of wifi and the fact that the internet connections are so much faster than what they were before, upload speeds are so much higher (download speed) so it's easier to store a lot of information in the cloud prior to this the idea of putting your information is absolutely ridiculous no one would do it no one would take that risk the idea it's kind of like saying a few years ago here's my hard drive and give it to a company and they look after it for you, someone can go through your data and we already have this issue the NSA and the people's personal information they're the web activity and their behaviors online being monitored. We talked a lot about big data in social what about the big data of cloud storage that's going to be bigger than anything that they could ever hope to get out of you when it comes to your facebook account or you twitter or linkedin if you look at the potential all for data mining and big data analysis maybe they won't go into specifics about what you're having your hard drive but there are lots of analytics companies out there who are chomping at the bit to do something like this not produce annual reports for example and surveys saying that in India 86 percent of people have this on their hard drive and 73 percent are using it for games or storage of documents.

The point is that we are surrendering our privacy, it's not being taken from us but we are surrendering our right to have it we're acquiescing here which simply giving in we'll just e saying sure let the floodgates open where does it end so it they may not be able to do much with our data because they'll have their own legal terms and conditions and they'll be bound by law but there are obviously those concerns and there's a lot of organization out there who are there. I think cloud storage is gray area it's something that we're going to deal in the future.

II. Insider Threats And Data Breaches

With the introduction of cloud computing technology every business whether it's a small or big are very much reliant on digital data which results in data breach. In organization people saved sensitive business data on local machines, on third party severs it will become very easy for hackers to breach data. In 2014 an employee of this asian credit institution pulled of one of the largest cases of identity theft for over a year and a half, a hacker secretly copied personal data from over 20 million people which is nearly 40% of the country's entire population.Office of personal management the records of more than 22 million current and former federal employees were compromised during this 2015 breach which leading experts believe was carried out by hackers connected to the Chinese government undetected for nearly a year the hackers gained access to the federal network by using a contractor stolen credential escalating their privileges and then planting a malware backdoor.

Anthem the second largest health insurer in the united sates was hacked in February 2015 from a personal information from as many as 80 million customers were compromised, investigators believe hackers gained access to anthems network via a watering hole attack that obtained an administrators login credentials which went undetected for almost a yearOver 70 million credit and debit cards were stolen from this popular retailer after a high profile hack in December 2013 investigators believe that the data was obtained from illegal software installed on physical card readers at target storeHeartland payment system in 2009 this new jersey based payment processing company fell victim to the largest credit card scam in American history over a hundred and thirty million credit and debit card numbers were siphoned via plantin malware heartland eventually paid over a hundred million to credit card companies to settle related claims In early 2014 the personal information for over 145 million people or customers were compromised when hackers used login credentials from a small number of employees they accessed the database containing name addresses birthdays phone numbers and passwords

With a recent flurry of high profile data breaches that many big retailers hundreds of million of consumers had their credit and debit card compromised not to mention the other personal information the consequences of suffering data breaches caused major brand damage and range from consumer mistrust, a drop of traffic and a decrease in sales cyber criminals are getting increasingly sophisticated with no end in sight so much so that retailers retail standards organizations audit committees and retail organizational boards are testifying before congress and implementing strategies that will protect them from the next costly data breach so in 2014 data security and the enforcement of security controls has become priority number one so here are the 10 ways to protect your company from data breach while maintaining required PCI complianceMinimize the customer data you collect in store acquire and keep only data required for legitimate business purposes and only for as long as necessary to manage the costs and administrative burden of the PCI compliance validation process try segmenting your infrastructure among multiple teams to minimize the complexity associated with the applicable compliance metrics Maintain PCI compliance throughout the checkout process to guard data against all the possible points of compromise or develop a strategy to protect your infrastructure on multiple level this include closing every opportunity for cyber criminals to exploit their POS terminals kiosks workstations and serversMaintain real time inventory and actionable intelligence on all endpoints and servers and control the overall security of your infrastructure to maintain PCI compliance employ multiple layers of security technology to stymie sophisticated hackers.

- Extend the life of your system and keep them compliant
- Use real time sensors to test your security system regularly
- Build measurable business intelligence around your business assets
- Conducts regular audits of security measures especially connections commonly used as gateways for attacks.

III. Data Integrity

When we store data in cloud it could suffer from damage while transmitting to or from cloud based storage. Data integrity is process of keeping the data safe from any modification otherwise the data should be detected. With the help of data integrity we could recover lost data and notifying about any data manipulation.
But there are certain condition in which data integrity could be violated. We as a users have many files and we store these files on the internet for this we need storage as a service so that we can access them anytime anywhere, your data can be accessed or modified by an unauthorized users. However data integrity can be maintained by techniques such as HAIL system which uses POR mechanism to check the storage of data in

cloud, RAID- strategies and digital signature and trusted platform module remote checking to check the data integrity remotely.

Business always suffers from the challenges of data integrity and security while there is a clear operational and strategic value in accurate and dependable data for decision making the operational cost of achieving and maintaining data integrity can be a substantial barrier to success for many organization as IT and OT or operational technology systems involved legacy data is continuously migrated to new systems example include the off-the-shelf software and SAS solutions which come with their own technologies or data models which are merged with homegrown systems as the needs of the business change the maintenance of any level of data integrity can easily become cumbersome and costly executive constantly ask their IT leaders how they can improve the quality of data in order to improve the insights needed to guide their company effectively while it sounds reasonable it may well be the wrong question rather than focusing the quality of raw data a better approach is to focus on the quality of the insight available and the speed and the cost to obtain them by asking how can we better leverage the data we already have to cost effectively obtain the insights.

We need advances in machine learning data science and correaltion analysis during the past decade have enabled the broader range of capabilities to analyze data from disparate operational processes and information system this has been accomplished without developing some of the structured relationships and incurring data model integration costs normally associated with traditional data warehousing and reporting approaches keep in mind that modern analysis methods are most appropriately suited to gaining operational insights and do not presently replace the structured data required for financial reporting and regulatory compliance through assessment of the trends and relationships between different data elements modern data analysis systems are able to discover a variety of insight that may not have been available during the past.

IV. Data Confidentiality

Confidentiality ensures that only authorized people with sufficient privileges can view the information. The most powerful tool to achieve confidentiality is encryption. Whenever you transfer encrypted information your computer turns that data into a cipher text that can only be put back into a readable form by unlocking it with a key of some sort that tells the receiving computer how to decode the incoming message this basic concept has actually been used to send secret messages since long before the computer invention. Modern electronics often use a widespread encryption scheme called public key encryption. Once the data actually arrives at its destination there are number of other encryption methods use to make sure it can sit on the computer or server safely for example you probably have a password or credit card number stored with amazon for example how do they keep those things safe often web servers build hash your passwords meaning that they are converted into encrypted string of text through a process that is extremely difficult to reverse and can't be unlocked with a key. It is important to remember that no system of encryption is perfect and experts in the field are constantly searching for weaknesses in encryption algorithms and devising new ones to outsmart hackers.

Data Availability

Availability ensures network resources are readily accessible to authorized users although a secure computer must restrict access attempts by unauthorized users it still must allow immediate access to authorized users for instance a banking customer should be able to check their balance or withdraw their funds in a timely manner. Data unavailability attacks are basically attacks where a malicious miner creates or publishes a block that the block header is present but some or all of the block data is missing so you can think of this as being a block that has a transactions well the first transaction here it could be a valid transaction or it could be invalid transaction that gives me 50 million ether out of nowhere if you do not have the data you have no way of verifying which is which and technically in an informatics theoretic sense there is a node there is basically an infinite number of valid transactions that have the same hash so it really could be any of them and there's also an infinite number of invalid transactions that have the same hash.

Data Privacy

Data privacy is legislation. It's the protection of that data from various levels. What data are you collecting on me what are you doing with that data , why are you using that data for. So data privacy incorporates not only the security aspects but it's the data that you're collecting and people do have an expectation of privacy. Everybody is moving to the cloud and they think about the security around the cloud, but they don't think about the privacy around the cloud. Data can be abused by other users. You have to make sure that privacy and data security are built into your system and processes from the ground up. There are things that are basically consider if you're a vendor in your contracts number one is to make sure that you impose the right kind of responsibilities on your customers. Number two make sure you tell your customer what you do and what you don't do not over promise, number three make sure that you include appropriate reasonable waivers

disclaimers and limitations on liability suppose on the other hand you are a recipient of cloud services in that case there are four major areas to consider in your contracts number one at the very basic level make sure your vendor commits to complying with all applicable privacy and data security laws number two make sure your vendor agrees to use adequate security measures technical administrative and physical number three if you're dealing with particularly sensitive and valuable information consider audit rights forth what we see increasingly among sophisticated companies where personal information is at court.

V. Limitations

Establishing trust in a piece of hardware, software or a network is somewhat similar to the process that an individual uses to trust a service organization. With the new technology with the computing cloud there always come a disadvantage we have controlled security, privacy, compatibility and down time these are the bridge of disadvantages of computing cloud now in terms of control you have to trust your provider because you will give them access to your information your data so if your company has more sensitive data and a lot of data you must have trust in your provider or your cloud provider and also it will limited your control so you will not have all the control like what you have in house so this is one big disadvantage of the cloud security and privacy .

Future Scope

Cloud computing emerges as the best technology in the future. It's a cost attractive method you don't have to build the whole infrastructure. Google, amazon and Microsoft are the leading examples of cloud services the future of cloud is the hybrid cloud in which the client can choose from the best of cloud modalities environmental solutions to build a hybrid hosting environment that exactly conforms to their needs the internet of things is growing rapid pace and for the most sophisticated IOT applications such as driverless delivery automated factories that demand real time feedback and make sense to push the processing of data and communications to the edge of the cloud known as edge computing the outward movement of cloud processing will enable a more reactive and collaborative data environment which will help fulfill the potential of internet of things serve. Despite of its drawback cloud computing becomes more and more popular and has a great potential in the future

VI. Conclusion

Cloud computing is our future it is the new emerging technology in the field of IT. There are many barriers and hurdles in the way of cloud computing which need an immediate attention as most of our data are stored in cloud. Abstract restriction on online privacy can have physical consequences in the offline world: what we do to protect and strengthen privacy and data protection, an easy first step is taking digital security measures yourself, this can be as simple as using encryption and anonymity tools, and encouraging your friends to do the same.

Refrences

[1]. Pearson S., Benameur A. Privacy, security and trust issues arising from cloud computing IEEE International Conference on Cloud Computing Technology and Science
[2]. H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, "Multi-tenancy in cloud computing," in Service Oriented System Engineering (SOSE),
[3]. F. Zhang and H. Chen, "Security-preserving live migration of virtual machines in the cloud," Journal of network and systems management, vol. 21, no. 4, pp. 562–587, 2013.
[4]. A. Corradi, M. Fanelli, and L. Foschini, "Vm consolidation: A real case based on openstack cloud," Future Generation Computer Systems, vol. 32, pp. 118–127, 2014.
[5]. S. Fiebig, M. Siebenhaar, C. Gottron, and R. Steinmetz, "Detecting vm live migration using a hybrid external approach."
[6]. Kharb L, CCTF: "Component Certification & Trust Framework", International Journal of Scientific Research in Computer Science and Engineering, Vol-1, Issue-6, 2013.
[7]. H. Wu, Y. Ding, C. Winer, and L. Yao, "Network security for virtual machine in cloud computing," in Computer Sciences and Convergence Information.

Rehana Ismail. "An Overview of International Financial Reporting Standards (IFRS)." International Journal of Engineering Science Invention, vol. 06, no. 12, 2017, pp. 31-36.