Emerging Security challenges In Cloud Computing: “An Overview”

Akshat Sharma
akshatsharma0212@gmail.com

Abstract:

Cloud Computing is the on demand availability of computer system resources, especially data storage, computing power, collection of services with 24*7 availability with ‘all over functionality support’, flexibility, less cost, high redundancy, accuracy and efficiency. Cloud computing provide all the facilities and services through the medium of “Internet” and hence called as Online Service Provider (OSP). Cloud services are offered by different service providers and often they are referred to as “Cloud Vendors”. Cloud computing is mainly described in two categories one on which type of service it provides and other on the Deployment Model.On the type of service Cloud Computing comprises of :IAAS (Infrastructure As A Service), PAAS (Platform As A Service) And SAAS(Software As A Service).Based On Delivery Models Cloud Computing comprises of :Public Cloud, Private Cloud, Community Cloud And Hybrid Cloud.

Cloud Computing with all the commending features prove to be a, highly developing, growing and vastly spreading technology with all the advantages as per the “User”, but the major Set-Back or can rather say the only disadvantage of cloud computing is “SECURITY OF DATA”. Online Frauds and Crimes has led to a major Set-Back in development and spreading of Cloud Computing. This paper deals with “Emerging Security challenges In Cloud Computing”.

Keywords:

Cloud Computing, Delivery Models, Online Service Provider, Online Frauds and Crimes, Security of data, categories of Cloud Computing.

Introduction:

Cloud Computing is the use of various services, such as software development platforms, servers, storage software’s through a medium called Internet. Cloud Computing provides scalable services for the cloud users. Many cloud computing advancements are closely related to virtualization. Some consider Cloud Computing an overused buzzword that has been blown out of proportion by marketing departments at large software firms but it’s not the reality to be honest and also the technology has proved this wrong over a period of time. Cloud Computing was first introduced by John Mccarthy in the year 1960’s, In 1970’s timesharing was introduced by IBM, In 1980’s Arpanet came into existence, In 1990’s first cloud computing service namely software as a service came into existence, In 2000 Cloud Computing took off aflier and went on to hit the highest levels which continues till now and is finding a niche as per the current scenario. The major issue in Cloud Computing as per my knowledge and understanding is ‘security of data’. In the modern era most of the people or cent percent people are aware of backing up their data and making their data safe and secure so that nobody can access their useful and personal information. Mostly entrepreneurs face more difficult to trust such vendors as compared to common people because they always have a fear of stealing or selling of their useful and personal data as well as stealing of their innovative ideas. Exposure of critical data to third party was mainly a complaint of many people in the segment of security and risk associated with cloud computing.

Security in other terms also mean there is a risk of losing your data. Many complaints in the starting of cloud computing era were registered that cloud vendor is denying to give their data back. Irrespective of the situations still this type of complains are heard. Usually the cloud vendor creat the backup of the user's data so if by mistake data gets deleted due to any reason, they can still provide you your original data. But some cloud vendors charge extra to provide copy of your own data just because they already mentioned in their terms and conditions. Even sometimes after giving all the desired amount, still the user don't get their data back. This violates the security in cloud computing. Cloud computing also depends on the jurisdiction and forensics because it stores data in different countries across the globe. This is another security issue in cloud computing. You don't have "control of your own data". Data may be stored far away in data centers of the vendor. If any country changes its rules and regulations of their county then you may have to pay for your own data to get it back or you may lose your data permanently. These type of security problems face frequently been noticed in cloud computing.

Cloud computing in its many forms, has proven to be a powerful, effective set of technologies which can provide even the smallest enterprise with significant benefits.

However, cloud computing suffers its own challenges specially that are security related. These are some of the major security challenges faced by cloud computing:

Lack of Visibility and Control:

Relating to both public and hybrid cloud environments, the loss of overall service visibility and the associated lack of control can be a problem.

Whether you're dealing with public or hybrid cloud environments, a loss of visibility in the cloud can mean a loss of control over several aspects of IT management and data security. Where legacy style in-house infrastructure was entirely under the control of the company, cloud services delivered by third-party providers don't offer the same level of granularity with regards to administration and management.

When it comes to visualizing potential security vulnerabilities, this lack of visibility can lead to a business failing to identify potential risks. In some sectors, such as media cloud adoption is very less around 20% to 25% in the current scenario.

Vendor Lock-In:

For companies that come to rely heavily on public and hybrid cloud platforms, there is a danger that they become forced to continue with a specific third-party vendor simply to retain operational capacity. If critical business applications are locked into a single vendor, it can be very difficult to make tactical decisions such as moving to a new vendor. In effect, the vendor is being provided with the leverage it needs to force the customer into an unfavorable contract.

Logicworks recently performed a survey that found showed that some 78% of IT decision makers blame the fear of vendor lock-in as a primary reason for their organization failing to gain maximum value from cloud computing.

Compliance Complexity:

In sectors such as healthcare and finance, where legislative requirements with regard to storage of private data are heavy, achieving full compliance whilst using public or private cloud offerings can be more complex.

Many enterprises attempt to gain compliance by using a cloud vendor that is deemed fully compliant. Indeed, data shows that around 50% of firms in USA rely on nothing more than a statement of compliance from their cloud vendor as confirmation that all legislative requirements have been met.

But what happens when at a later stage, it is found that the vendor is not actually fully compliant? The client company could find itself facing non-compliance, with very little control over how the problem can be resolved.

A Lack of Transparency:

When a business buys in third-party cloud services as either a public or hybrid cloud offering, it is likely they will not be provided with a full service description, detailing exactly how the platform works, and the security processes the vendor operates.

This lack of service transparency makes it hard for customers to intelligently evaluate whether their data is being stored and processed securely at all times. Surveys have shown that around 70-75% IT managers are only marginally confident that company data is being stored securely by their cloud vendor.

Shared Technology Vulnerabilities:

Using public or hybrid cloud offerings can expose a business to security vulnerabilities caused by other users of the same cloud infrastructure.

The onus is upon the cloud vendor to see that this does not happen, yet no vendor is perfect. It is always possible that a security vulnerability caused by another user in the same cloud will affect every user.

Insufficient Due Diligence:

For companies that lack the internal resources to fully evaluate the implications of cloud adoption, then the risk of deploying a platform that is ineffective and even insecure is real.

Responsibility for specific issues of data security needs to be fully defined before any deployment. Failing to do so could lead to a situation where there is no clearly defined way to deal with potential risks and solve current security vulnerabilities.

Insecure Interfaces and APIs

Cloud vendors provide their customers with a range of Application Programming Interfaces (APIs), which the customer uses to manage the cloud service.

Unfortunately, not every API is entirely secure. They may have been deemed to be initially, and then at a later stage be found to be insecure in some way. This problem is compounded when the client company has built its own application layer on top of these APIs. The security vulnerability will then exist in the customer’s own application. This could be an internal application, or even a public facing application potentially exposing private data.

Conclusion:

As we are heading towards the society where automated information resources are majorly used, cloud computing can find niche and edge in becoming the widest used and implemented technology with very high rise in the upcoming era. With some improvements in the above discussed fields as per the security is concerned cloud computing will move further and achieve all the peaks and pricks.

References:

[1] Liang Hu, Feng Wang, Jin Zhou and Kuo Zhao "A Survey from the Perspective of Evolutionary Process in the Internet of Things", International Journal of Distributed Sensor Networks, Article ID 462752, 2015

[2] The block diagram of WQP : https://link.springer.com/article/10.1186/s40713-017-0005-y

[3] ThingSpeak-Understanding your Things-The open IoT Platform with MATLAB analytics, MathWorks.

[4] User Manual Arm7-LPC2148 Development kitPantech Solutions.

[5] ESP8266 serial Wi-Fi wireless Transceiver Module for IoT, ESPRUINO-Wireless.

[6] irjet.net/archives/V5/i10/IRJET-V5I10219.pdf