A Study on Cloud Computing Applications and Security Challenges

Komal Sehwal[1],
[1]M.C.A. Student,
Master of Computer Application,
Ganga Institute of Technology and Management
Maharshi Dayan and University,
Rohtak, Haryana, India

Dhiraj Kumar[2]
[2]Assistant Professor,
Department of Computer Science & Engineering,
Ganga Institute of Technology and Management
Maharshi Dayan and University,
Rohtak, Haryana, India

Cloud computing is the delivery of computing services over the Internet with less cost and more reliability in getting services. With the increase in need of various technologies which satisfies customer's dynamic resource demands at one place and makes the job easier to work on all platforms for the user from any place with less cost makes the use of cloud important. Security is the main criteria when working on cloud, as the third party involvement will be there. Elaborating some security issues and the solutions to mitigate them.

Keywords: Cloud, Cloud computing, Server, Frontend, Backend, Middleware

I. INTRODUCTION

1 What is Cloud Computing?

Cloud is a computing model that refers to both the hardware and system software in the datacenters that provide those services, the applications derived as services over the Internet. It is treated as the high potential paradigm used for deployment of applications on Internet. This concept also explains the applications that are broaden to be accessible through the Internet. Cloud applications use effective servers and large data centers that host web applications and services.

1.1 Definition of Cloud Computing

Cloud Computing is rapidly being accepted as a universal access appliance on the Internet. A lot of attention has been given to its concept in deriving standard definitions. But here we consider the standard definition given by the National Institute of Standards and Technology (NIST):

"Cloud Computing is 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", [1].

2 What are Cloud Servers?

In some respects cloud servers work in the same way as physical servers but the functions differ. For opting cloud hosting, clients rather than renting or purchasing physical servers, theyare renting virtual server space. They are often paid for by the hour depending on the capacity required at any particular time.

Traditionally there are two main options for hosting: dedicated hosting and shared hosting. Dedicated hosting is a much more advanced form of hosting, whereby clients purchase a whole physical server which means that the entire server is dedicated to them with no other clients sharing it. In some instances the client may utilize multiple servers which are all dedicated to their use. Dedicated servers allow for full control over hosting .Shared hosting is the cheaper option whereby servers are shared between the hosting provider's clients. One client's website will be hosted on the same server with websites belonging to other clients that cause several disadvantages including the fact that the setup is inflexible and cannot cope with a large amount of traffic. The downside is that the required capacity needs to be predicted, with enough resource and processing power to cope with expected traffic levels. If it is underestimated then it can lead to a lack of necessary resource during busy periods, while overestimating makes us to pay for unnecessary capacity.

Clients get the best of both worldswith cloud hosting. Resource can be add or removed accordingly, making it more flexible and, therefore, more cost-effective. When there comes more demand on the servers, capacity can be automatically increased to match that demand without this needing to be paid for on a permanent basis. This is akin to a heating bill; you access what you need, when you need it, and then afterwards only pay for what you've used.

Unlike dedicated servers, cloud servers can be run on a hypervisor which is used to control the capacity of operating systems so it is allocated where needed. With cloud hosting there are multiple cloud servers which are available to each particular client. This allows computing resource to be dedicated to a particular client if and when it is necessary. Where there is a spike in traffic, additional capacity will be temporarily accessed by a website, for example, until it is no longer required. Cloud servers also offer more redundancy as if one server fails, others will take its place.

Below are the key benefits of cloud servers:

- Cost-effectiveness: whilst being available when needed, clients only pay for what they are using at a particular time
- Flexibility and scalability: extra resource can be accessed as and when required

- Reliability: if there are problems with some, the resource will be shifted so that clients are unaffected.
- Ease of set up: Cloud servers do not require much initial setup

II. LITERATURE REVIEW

In [10] authors describe Cloud computing has surpassing shifted so far in terms of utilizing the current technologies. The trend of having cloud services as part of an organization seems to be gaining more importance. For the reduction of capital expenditures, organizations need to consider utilizing cloud services as an essential part of their foundations. Nevertheless, various challenges are prohibiting the attainment of vast deployment and acceptance levels and the main drawback of the existing cloud service implementations is their inability to provide an accredited high security level. In [11] they first discussed security issues for cloud which include storage security, data security, network security, middleware security and application security. Main goal is to manage data and securely store that is not controlled by the owner of the data. In particular, they are taking a bottom up approach to security in which they are working on small problems in the cloud that will solve the larger problem of cloud security. We discussed how secure co-processors may be used to enhance security. They implemented the Hadoop finally. Many new technologies emerging at a rapid rate, each with technological advancements and potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. In [12] authors study different architectures which are based on the services they provide. Data is stored on to centralized location called data centers having a large size of data storage. Data as well as processing is somewhere on servers. So, the clients have to trust the provider on the availability as well as data security. Before moving data into the public cloud, issues of compatibility and security standards must be addressed. A trusted monitor installed at the cloud server that can auditor monitor the operations of the cloud server. In minimizing potential security trust issues as well as adhering to governance issues facing Cloud computing, a prerequisite control measure is to ensure that a concrete Cloud computing Service Level. In [13] authors main focus on a new technology which is expected to significantly reduce the cost of existing technologies. For information security, there are both favorable factors and negative factors brought by cloud computing. The final effect depends on whether we can develop its strengths and avoid its disadvantages. Only in this way, the cloud can become improving productivity efficiency, a real cost savings and secure platform. Most serious of all these issues is security of information whether it is at rest or in transit. There are numerous security issues pertinent to cloud infrastructure of which most critical ones are discussed in this paper. Next cloud computing security considerations are discussed which must be included in every cloud for the data in it to be secure. Next secure cloud architecture is proposed to secure the data from external attacks.

III. ARCHITECTURE

When talking about a cloud computing system [5], it's helpful to divide it into two sections: the front end and the back end. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client, sees. The back end is the "cloud" section of the system.

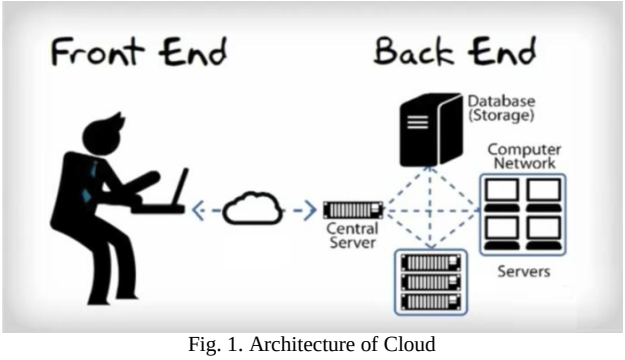

Fig. 1. Architecture of Cloud

The front end includes the client's computer (or computer network) and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients.

On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services. In theory, a cloud computing system could include practically any computer program you can imagine, from data processing to video games. Usually, each application will have its own dedicated server.

A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware. Middleware allows networked computers to communicate with each other. Most of the time, servers don't run at full capacity. That means there's unused processing power going to waste. It's possible to fool a physical server into thinking it's actually multiple servers, each running with its own independent operating system. The technique is called server virtualization. By maximizing the output of individual servers, server virtualization reduces the need for more physical machines.

If a cloud computing company has a lot of clients, there's likely to be a high demand for a lot of storage space. Some companies require hundreds of digital storage devices. Cloud computing systems need at least twice the number of storage devices it requires to keep all its clients' information stored. That's because these devices, like all computers, occasionally break down. A cloud computing system must make a copy of all its clients' information and store it on other devices. The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable. Making copies of data as a backup is called redundancy.

IV. ADVANTAGES OF CLOUD

Advantages of Cloud:

1. Flexibility

Cloud-based services are ideal for businesses with growing or fluctuating bandwidth demands. If your needs increase it's easy to scale up your cloud capacity, drawing on the service's remote servers. Likewise, if you need to scale down again, the flexibility is baked into the service.

3. Automatic software updates

The beauty of cloud computing is that the servers are off-premise, out of your hair and out of sight. Suppliers take care of them for you and roll out regular software updates – including security updates – so you don't have to worry about wasting your precious time in maintaining the system yourself.

3. Disaster recovery

Businesses of all sizes should be investing in robust disaster recovery, but for smaller businesses that lack the required cash and expertise; this is often more an ideal than the reality. Cloud is now helping more organizations buck that trend. According to Aberdeen Group, small businesses are twice as compare to larger companies that have implemented cloud-based backup and recovery solutions that avoid large up-front investment, save time and roll up third-party expertise as part of the deal.

4. Capital-expenditure Free

Cloud computing cuts out the high cost of hardware. You simply pay as you go and enjoy a subscription-based model that's kind to your cash flow. Add to that the ease of setup and management and suddenly your scary, hairy IT project looks a lot friendlier.

5. Work from anywhere

If you've got an internet connection you can be at work with cloud computing. And with most serious cloud services offering mobile apps, you're not restricted by which device you've got to hand.

6. Increased collaboration

When your teams can access, edit and share documents anytime, from anywhere, they're able to do more together, and do it better. Cloud-based workflow and file sharing apps help them to make updates in real time and gives them full visibility of their collaborations.

7. Document control

The more employees and partners collaborate on documents, the greater the need for watertight document control. Before the cloud, workers had to send files back and forth as email attachments to be worked on by one user at a time. Sooner or later – usually sooner – you end up with a mess of conflicting file content, formats and titles.

When you make the move to cloud computing, all files are stored centrally and everyone sees one version of the truth.8. Competitiveness

Moving to the cloud gives everyone access to enterprise-class technology. It also allows smaller businesses to act faster than big, established competitors. Pay-as-you-go service and cloud business applications mean small outfits can run with the big boys, and disrupt the market, while remaining lean and nimble.

9. Security

Lost laptops are a billion dollar business problem. And potentially greater than the loss of an expensive piece of kit is the loss of the sensitive data inside it. Cloud computing gives you greater security when this happens. Because your data is stored in the cloud, you can access it no matter what happens to your machine.

10. Environmentally friendly

When your cloud needs fluctuate, your server capacity scales up and down to fit. So you only use the energy you need and you don't leave oversized carbon footprints. This is something close to our hearts at Sales force, where we try our best to create sustainable solutions with minimal environmental impact.

V. APPLICATION OF CLOUD

The applications [2, 3] of cloud computing are practically limitless. With the right middleware, a cloud computing system could execute all the programs that a normal computer could run. Potentially, everything from generic word processing software to customized computer programs designed for a specific company could work on a cloud computing system. Why would anyone want to rely on another computer system to run programs and store data?

Here are just a few reasons:

Clients would be able to access their applications and data from anywhere at any time using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network.

It could bring hardware costs down. Cloud computing systems would reduce the need for advanced hardware on the client side. You wouldn't need to buy the fastest computer with the most memory, because the cloud system would take care of those needs for you. Instead, you could buy an inexpensive computer terminal which include a monitor, input devices like a keyboard and mouse just enough processing power to run the middleware necessary to connect to the cloud system. You wouldn't need a large hard drive because you'd store all your information on a remote computer.

Corporations might save money on IT support. Streamlined hardware would, in theory, have fewer problems than a network of heterogeneous machines and operating systems.

Corporations that rely on computers have to make sure they have the right software in place to achieve goals. Cloud computing systems give these organizations company-wide access to computer applications. The companies don't have to buy a set of software or software licenses for every employee. Instead, the company could pay a metered fee to a cloud computing company.

Servers and digital storage devices take up space. Some companies rent physical space to store servers and databases because they don't have it available on site. Cloud computing gives these companies the option of storing data on someone else's hardware, removing the need for physical space on the front end.

VI. SECURITY CHALLENGES IN THE CLOUD

There are various security threads that stops customer from taking the benefits of the cloud. Following are few threats present in the cloud and their mitigation [7].

A. VM Attacks

Cloud computing is based on VM technology. For implementation of cloud, hypervisor such as VMware, Sphere etc are used.

Developers need to take care of attacks. When coding and also by using IDS and IPS we can solve these and use the suitable firewall.

B. Data Loss or Leakage

It is a negative impact on business. By encrypting and protecting the integrity of data in transit. Analysis of data protection at both design and runtime should be done initial phases.

C. Loss of Governance

SLA may not have commitment on part of cloud provider or cloud provider. But there is no proper SLA i.e. standard SLA‘s are not present.

D. Use of Cloud Computing

This is used mainly due to weak registration system

- By credit card fraud monitoring.
- By implementing stricter registration process

E. Lock-IN

Customer cannot move from one service provider to another. So to overcome this API‘s should be used which should be standardized. So anybody can use them on cloud.

VII. SECURITY CHALLANGES AND ITS POSSIBLE SOLUTIONS

The cloud is the delivery of on-demand computing resources—everything from applications to data centres—over the Internet on a pay-for-use basis. Advantages of cloud include Reduced capital costs, Improve accessibility, improve flexibility. Despite of its merits the most serious of all is being that is the security of information. There are many security implications of which the serious issues are concentrated in this paper which investigates the possibility of the data/information being secure in the cloud computing environment. The cloud security issues are summarized as follows [4][5][6]:

A. Multi tenancy

Implies sharing of database, computational resources, services, storage, physical and logical access with other tenants residing on same physical or logical platform at provider‘s premises. This sharing of resources violates the confidentiality of tenants IT assets which leads to the need of secure multi tenancy and to deliver these there should be a level of isolation among tenant data as well as location transparency where tenants may not have knowledge of where their data is located or their process resident. To have secure multi tenancy platform, location transparency and isolation among tenants data where tenants have no knowledge or control over specific location of resources to avoid planned attacks. Always keep data at multiple locations so that even if at one place attack occurs back up is in other place.

- Isolation on PAAS should be done on running services and API.
- Isolation on SAAS isolate among transaction carried out on same instance by different tenants.
- Isolation on IAAS is on VM storage, memory network and cache memory.

B. Availability of information

Implies that when an organization ports its process, services and applications to cloud they take a calculated risk in terms of non-availability of critical data or information or processes when needed the most. The way to mitigate the unavailability of resources is to have backup plan to cover an outage event also for local resources for crucial information. The provider should provision a monitoring and notification system that enable the consumers know of the possible down time.

C. Elasticity

Implies that consumers are able to scale up or down resources assigned to resources based on current demand. The solution for this can is that data location should be within the tenant‘s country boundaries. In addition, the placement engines include mitigation strategy where services are migrated from logical or physical host to another or from one cloud provider to another in order to meet demands and efficient utilization of the resources.

D. Information integrity and privacy

Means exposing resources over the internet to valid users and malicious attackers. Tenants resources can be accessed through remote connections web browsers, etc. Some of major information security privacy and authentication issues are absence of authorization and authentication, accounting controls and no management of encryption and decryption keys. To overcome this problem there should be proper authentication and authorization should be implemented so that any attempt to access the information goes through multilevel check to ensure only authorized tenants have access to the information.

E. Secure information management

Cloud management layer is the microkernel that can be extended to incorporate and coordinate components such as service monitoring, billing, services registry and security management of the cloud. This layer is very critical since any breach of this layer will result in a malicious user ending up in having control alike an administrator, over the whole cloud platform. Solution for this is to include security policies and requirements specifications derived from tenant organizations which are reviewed and applied in tenant‘s specific physical and logical environment, security configurations and feedback from environment to security management and cloud consumer base.

F. Multiple Stake holders

Different stake holders in cloud computing are

1. Service provider is the one who uses cloud infrastructure to deliver applications to end users.
2. Cloud provider, is the one who delivers infrastructure to cloud customers.
3. Customer is the one who uses the service hosted on cloud environment.

Each of the above has their own security issues. Each customer will have different trust relation with

providers, sometimes user himself can be attacker. Provider and customer need to agree on conditions, however so standard conditions are present.

G. Cloud secure federation

Is an issue when cloud consumer leverages applications and information that depend on services from different clouds, it needs to maintain its security requirements enforced on both clouds and in between. This problem can be overcome by identity federation, leveraging density attributes federation, single sign on, authentication and authorization can help resolve federation security issues.

H. Third Party Control

Owner has no control on their data processing as this is a third party issue. Cloud providers are not aware of architecture of Cloud so effective security is not provided. Sometimes user can be locked with one vendor. This happens because of agreement or difficult in migrating data to new vendor.

I. Repudiation of information

The provider and the consumer find themselves in a deep-hole when it comes to prove the transaction they did was indeed them, or may decline that it was them. To prevent this issue at cloud level, cloud provider has to ensure that non-repudiation enabled protocol or handshake is deployed whereby, the engaging parties cannot dismiss their participation in argued transaction.

J. Integrity of information

Is achieved when there is a mutual trust between the provider and consumer and they complement each other and support the security such that whole system works seamlessly. To achieve this proper authentication, Authorization and accounting controls should be implemented by the cloud service provider and consumer. The credentials to access the information on cloud should be individual, secure (RSA tokens or one time password) and should not be shared among the entities of the consumer organization.

K. Service disruptions

It can land any business/organization into a difficult situation, the information required is not available when it is most desired and also unpleasant behavior can be caused by DOS, DDOS attack. This issue can be addressed by employing defence–in-depth technique in order to have security controls implemented at various layers throughout the cloud access path as well as within the consumer and provider network, sharing of account credentials between consumers should be strictly denied.

L. Loss of Control

Loss of controls can be a disaster for an organization. This is one of the CIO‘s major concerns before they take a decision to move their data/information to the cloud. To minimize this effect the organizations should understand cloud provider‘s security policies, storage policies and SLAs. This will enable in mutual understanding between the provider and consumer about the way the consumer‘s data will be handled in cloud.

M. Security Management

The successful security management in cloud depends on two parts: what security controls must the customer provide over and above the controls inherent in the cloud platform and how must an organization‘s security in the cloud. Both of these factors must be continually reevaluated based on the sensitivity of the data and the service-level changes over time.

VIII. CONCLUSION

Cloud computing is the development trend of IT industry as a new technology which is expected to significantly reduce the cost of existing technologies. For information security, there are both positive and negative factors brought by cloud computing. The final effect depends on whether we can develop its strengths and avoid its disadvantages. Only in this way, the cloud can become improving productivity efficiency, a real cost savings, and secure platform. The most serious of all these issues is security of information whether it is at rest or in transit. There are numerous security issues pertinent to cloud infrastructure of which most critical ones are discussed in this paper. Next secure cloud architecture is proposed to secure the data from external attacks. Next cloud computing security considerations are discussed which must be included in every cloud for the data in it to be secure.

REFERENCES

[1] Peter Mell, “The NIST Definition of Cloud”, Reports on Computer Systems Technology, sept., p. 7.,2011
[2] Ni Zhang Di Liu Yun-Yong Zhang, “Research on cloud computing security”, International Conference on Information Technology and Applications, IEEE, 2013
[3] Rabi Prasad Padhy , ManasRanjanPatra , Suresh Chandra Satapathy , “ Cloud Computing: Security Issues and Research Challenges”, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011
[4] AkhilBehl, KanikaBehl, “Security Paradigms for Cloud Computing”, Fourth International Conference on Computational Intelligence, Communication Systems and Networks, IEEE, 2012
[5] AkhilBehl, KanikaBehl, “An analysis of cloud computing security issues”, World Congress on Information and Communications Technologies IEEE,2012
[6] HuagloryTianfield, “Security Issues In Cloud Computing”, International Conference on Systems, Man, and Cybernetics, IEEE, OCT 14-17,2012
[7] MeikoJensen, JorgSehwenk et al., “Technical Security, Issues in cloud Computing”, IEEE International conference on cloud Computing, 2009
[8] 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.
[9] Shuai Z; Shufen Z; Xuebin C; Xiuzhen H; (2010), “Cloud Computing Research and Development Trend”, 2nd International conference on Future Networks, 2010. ICFN ' 10. pp 23, 22-24 Jan 2010.
[10] Osama Harfoushi, “Data Security issues and challenges in Cloud Computing: A Conceptual Analysis and Review”, *Communications and Network*, 2014, 6, 15-21
[11] P.Radha Krishna Reddy, “The Security Issues of Cloud Computing over Normal & IT Sector”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, p. 4, March 2012.
[12] Geethu Thomas, ” Cloud Computing Security using encryption technique”, https://arxiv.org/ftp/arxiv/papers/1310/1310.8392.pdf
[13] Manas M N, “Cloud Computing Security issues and Methods to Overcome”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 4,p. 3, April 2014.