Cloud Implementation Issues and What to Compute on Cloud

Pardeep Sharma
Computer Science and Engineering
Yadwindra College of Engineering
Talwandi Sabo, India
shah4ash@yahoo.co.in

Sandeep K. sood
Department of Computer Science and Engineering
Guru Nanak Dev University, Regional Campus
Gurdaspur, India
san1198@gmail.com

Sumeet Kaur
Computer Science and Engineering
Yadwindra College of Engineering
Talwandi Sabo, India
purbasumeet@yahoo.co.in

***Abstract*— the development of worldwide networks, open systems and new technology trends a new type of computing where computational power is provided similar to utilities like water, gas or electricity. Cloud computing refers to the concept of grid computing, utility computing and virtualization. It elevates knowledge management to newer heights by providing huge data storage and computational power with feature of elasticity and scalability. It has a lot of advantages but still this field in its infancy as far as implementation and usage are concerned. The lack of security in cloud represents an obstacle for most enterprises for moving into the cloud. The purpose of this paper is to address the challenges and threats in deployment models and discuss obstacles in implementation of cloud computing. So researcher need to work at this high developing paradigm's highlighted areas.**

***Keywords*- Datacenters, Data Privacy, Hypervisor, Security, Utility Computing and Virtualization.**

I. INTRODUCTION

Cloud computing is next generation computing platform that provides dynamic resource pooling, virtualization and high availability. It enables the virtual organizations or enterprises to share geographically distributed resources as they pursue for common goals, assuming the absence of central location, omniscience and an existing trust relationship. The cloud offers several benefits like fast deployment, pay for use, lower costs, fewer maintenance issues, scalability, rapid provisioning, unlimited storage, ubiquitous network access, greater resiliency, instant software updates, low cost disaster recovery and data storage solutions, on demand security controls, real time detection of system tampering and rapid re-constitution of services[1-3]. Due to its benefits various enterprises across different sectors are eager to adopt cloud computing. But due to lack of security control on information they denied. This technique is driven from the mainframe systems. But because of some reasons it is difficult for enterprises to achieve this much high growth in past decades. Now these days, the tremendous growth of the web has given rise to the class of web scaling problems and challenges such as supporting thousands of concurrent e-commerce transactions or millions of search queries in a minute. It has become a large and growing market because of its value propositions of low costs, increased flexibility and shorter time to market. Security issues in cloud computing are hampering the interest of perspective organizations. There have been a lot of proven security attacks on different cloud computing providers such as Google (Gmail, App Engine), Amazon Web Services (Amazon S3) and Salesforce.com (Salesforce.com). Cloud computing has three delivery models by which different types of services are provided to end users. These service models are software as a service, platform as a service and infrastructure as a service. They need different security requirements at each level.

Software as a service (SAAS): It is a software deployment model in which applications are remotely hosted by service provider and made available to users on demand, over the internet. SAAS providers are responsible for implementing suitable security controls in their infrastructure, operating system and middleware as well as application software. Enterprises provide these service over the internet are Google docs, mobile me and Zoho [1]. Still most enterprises are uncomfortable with this model due to lack of visibility about the way their data is stored and secured. SAAS has challenges like maintaining multitenancy (in which cloud allow multiple users to use same hardware at the same time, without losing the trust and do not cumbersome the information among each other) and Virtualization (various programs may run on single machine and may be many machines run a single program). This feature has various lose ends like interception, modification of data at rest and in transit, privacy, impersonation, traffic flow analysis and session hacking. The security provided at this level by firewalls, intrusion detection, log inspection and integrity monitoring.

Infrastructure as a service (IAAS): It changes the way enterprises deploy their applications. It provides control over the operating system, data storage system and computational

resources. It offers an opportunity to the consumer to rent or lease the processing, storage, networks and power resources. Where the enterprises are able to deploy and run arbitrary software or control the underlying cloud infrastructure. IAAS is established on service delivery model that provisions a predefined and standardized infrastructure and specifically optimized for the customer's applications. An IAAS provider handles the transition and hosting of selected applications on their infrastructure. Customers maintain ownership and management of their applications while off-loading hosting operations and infrastructure management to the IAAS providers. The security threat is the reliability of data that is stored with in provider hardware. Attacks may be eliminated by using firewalls and load balancers etc. Customers even do not know the servers or datacenters location. So these are the challenges at this level to work for researchers.

Platform as a service (PAAS): It enables developers to build their applications on top of platform by using programming languages and tools supported by cloud providers. But the security provision below the application level like as host and network intrusion detection and prevention are still in the scope of the researchers. Providers assure that data is not shared between different applications. The consumer has control only over the deployed applications and on possibly application hosting environment configurations. It aims to support the complete life cycle of building, delivering web based applications and services that entirely available from the Internet. PAAS model aims a new modern era of mass innovation [1-3]. The challenges in this level are maintaining data security, network security, cloud management control, virtual cloud protection and communication security. Enterprises provide these applications are Microsoft azure, Google app engine.

This paper is organized as follows. In Section II, we introduce the security challenges and possible attacks on security of cloud. In Section III, we describe the implementation issues in cloud and how to overcome these obstacles. In Section IV, we propose our method how we can determine whether shifting to cloud is beneficial for enterprises or not. In Section V, we propose future research directions and Section VI concludes the paper.

II. SECURITY CHALLENGES

Securing an open information system simply means to identify unique threats and challenges. These are needed to be addressed by implementing the ear mark countermeasures. Due to the effective architectural design of cloud computing, it imposes many benefits like centralization of security, distribution of data, data segmentation and high availability. Due to these benefits many risks are also encountered. Numbers of security challenges in cloud are introduced as shown in table1. The security parameters in cloud are confidentiality, integrity, availability, non-repudiation and authentication.

Table1. Security Parameters

Goals	Description
Confidentiality	Ensures that information is not disclosed to any Unauthorized person.
Integrity	Ensures that information held in a system is a proper representation of the information intended, means information is not modified by any unauthorized person.
Availability	Ensures that information processing resources are not made unavailable by malicious action.
Non-repudiation	Ensuring that agreements made electronically can be proven to have been made.
Authentication	Receiver need to sure the sender identity and identify whether not any imposter send the message

A. *Confidentiality*

It means that the only authorized user or systems have ability to access the protected data. The message is transmitted over the network is private and secure between the sender and receiver. To others, the message should be garbage. The basic way to maintain confidentially is just to encrypt message at the sender side and decrypt the same message at the receiver side. So the meaningful information over network does not come into intruder hands. To achieve the confidentiality, symmetric and asymmetric keys are used. Both have own advantages and disadvantages [4]. The various feasible attacks on confidentiality are described ahead.

(1) Phishing cloud provider: The engineers and the phisher involved in developing the cloud have a new attack vectors. They created so many applications with their full control and remain some loop holes in the developed software. After implementing the software at cloud, they interfere with the user privacy. Salesforce showed phishing incident in past [3].
(2) VM-level attacks: Potential exposure in the virtual machine technology used by cloud providers is a potential problem in multitenant environment. These types of attacks are appeared in VMware and virtual servers [4].
(3) Multitenancy: It refers to the single instance of software running at the server side serves multiple instances at the client side. The clients may be organization or single users. To maintain the confidentiality the data of various clients stored on single server is not shared among them. So the privacy should not be leaked among different users [4, 5].

B. *Integrity*

It means data received at the receiver side is exactly the same as the data sent by the sender. It is one of the crucial issues

that should be addressed by the cloud provider. It rises with the growth of web and internet. There are so many ways to preserve the integrity of cloud like by using the digital signature method (in which both the document and the electronic file which has signature is attached, if both are same means integrity is preserved otherwise not) and other method is message digest (in which message is passed through an algorithm called hash function. The hash function creates small piece of information, which is passed over network with document for checking the integrity. Hash based method takes less computational time and complexities). Now these days' message authentication codes are also used for maintaining integrity and authentication as well. The cloud obeys the property of ACID (atomicity, consistency, isolation and durability) for integrity [6]. The various feasible attacks on integrity are described ahead.

(1) Man in the middle attacks**:** These types of attacks are carried out when an attacker or malicious object lies between two users. Then there are possibilities that attacker can intercept and modify communication

(2) System misconfiguration: It analyzed that most of the time security vulnerability in the enterprises is the result of system misconfiguration. Misconfiguration means not updating system with latest released security fixes and not uses proper firewalls. Strong security always requires operational diligence which is driven by the requirements of policies, processes and a clear understanding of the underlying business risks that the organization takes when not clinging to the policies and processes [7].

(3) Worm and intrusion attack: Worms and intrusions attacks from inside or outside the cloud also affect the integrity at higher extent. Whenever network security is compromised, due to worm attacks or an intrusion, the integrity of enterprise's data is affected. Many e-mail viruses modify or remove files from users' disk drives. Successful attacks against Web sites deface their content and root kits that modify system executable which completely cover an intruder's tracks. These business assets are too valuable to be left open to compromise, at this position data Integrity Solutions come into play [8, 9].

C. Availability

It includes system abilities to carry on operations and services even when some authorities misconduct. It refers to software, data and hardware being available to the authorized user upon demand. It is one of the most critical issues for the information security requirement in cloud computing. It is a decision parameter for choosing among the public, private and hybrid cloud. It simply means how long the service will be provided to the user. This issue is simply resolved in service level agreements (SLA). SLA simply highlights the dread of availability in cloud computing services and resources between the cloud providers and users. Incidents of cloud outage in well established companies are shown in table2. The various feasible attacks on availability are described ahead.

(1) Uptime: As in traditional security concerns, enterprises ensures that their services availability and their server uptime is better than user's own datacenter. But in practice it is shown that the third party cloud would not scale well enough to handle the applications at peak load. We analyze that no utility company is going to run its billing for more than 1 billion consumers in the cloud.

(2) Single point of failure: The major threat to availability in cloud is single point failure or attack. In this the server has whole processing load of several clients. If server downs, all the clients get down because the clients do not run their own software. The attack on server in this case is like as denial of services [10].

(3) Assurance of computational integrity: Whether the enterprises assured that the cloud provider give results to user are valid. This feature raises the question of faithfulness of cloud providers.

Table2. Attacks on Availability

Companies	**Reasons**	**Duration (hrs.)**	**Date**
Amazon S3	Overloading of authentication server	2	15/02/08
Amazon S3	Single bit error lead to gossip protocol blow up	6	20/07/08
Goggle app engine	Programming error	5	17/6/08
Gmail	Due to breakdown in contacts system	1.5	11/08/08
flexi Scale	Due to peak workload	18	31/10/08

D. Non-repudiation

This involve the issue like when sender send a private message to receiver, due to some reasons it denies that message is not sent by him. It creates a problem for receiver to prove the original sender. The simple solution to this problem is provided by use of trusted third party, it may be any government organization [11]. The various feasible attacks on non-repudiation are described ahead.

(1) Denial of services attack: In this attacker attempts to make the computational resources unavailable to its intended user. Past data showed that every cloud provider enterprise comes into its attack. These types of attacks are generally found in computer network system and these days extended to CPU resource management.

(2) ICMP flood: These type of attacks are possible due to the misconfiguration of network devices. In this, packets sent to all addresses by imposters for the complete control of network after attaining the control, network works as smurf amplifier for intruders [12].

E. Authorization and Authentication

Authorization is simply like as privileged user access. Depending upon the type of cloud and delivery models, permissions and priorities are granted on role basis to users. Methods used for authorization are passwords, biometric sensors etc. which bound the specified user in to their own limit or simply user can access only those privileges or rights which are granted to him. Authentication shows the originator of message. This feature is used to check that not any imposter communicate with the sender and receiver. For this, we use message authentication codes (MAC) and hashed message authentication codes (HMAC) [13]. The various feasible attacks on authorization and authentication are described ahead.

(1) Write to file system: As a user has permissions to write file in the cloud, this user may use this function illegally or in malicious manner. The user may create or upload virus or Trojan programs to the cloud server which may cause a serious security problem.
(2) Ping request: This feature gives the control of sockets to host that would able to simply ping the user to see their connection records. The security significance of this are various types of attacks like smurf attack, denial of services attack and ping of death attacks that can be launched through sockets.
(3) System call: In this, if the user has access to command prompt console this means user has full control over the target system. Therefore in cloud these types of permissions should not be given to anyone. This is simple ways to give chance to a person to destroy target systems [14].

III. IMPLEMENTATION ISSUES IN CLOUD

Major obstacles in the implementation of cloud computing are discussed. Data lock-in is a provision that a consumer of cloud can be easily shift from one cloud to another for the fulfillment of their requirement. Some provider companies bound a person in their cloud by applying certain terms and conditions [15]. Conditions are not shown to user at entry level. Data auditability means to check that any intruder or imposter harm the data or not. It simply record the changes made on data whether it is static or transit. Data bottlenecks relate with the bandwidth problems. It rises in peak load time or in congestion period when more users communicate at limited bandwidth. Performance unpredictability relates to the feature of elasticity and scalability of cloud [16]. It means if a user consume single server power for some time but certainly he need 20 times more resources then how they will be provided. Scalable storage means cloud should provide elasticity in storage system as well. Fate sharing means bad behavior of single user can affect the reputation

Table 3. Issue in cloud computing and solutions shows how to overcome them.

	Obstacles	Solutions
1	Data lock-in	Use standardized application program interfaces.
2	Data auditability	Deploy encryption, firewalls and intrusion detection
3	Data transfer bottlenecks	Data backups, higher BW switches
4	Performance unpredictability	Improved virtual machine support; flash memory.
5	Scalable storage	Invent scalable store
6	Reputation fate sharing	Offer reputation guarding services like those for email sharing
7	Software licensing	Pay for use licenses
8	Data location	Location finding algorithms
9	Data segregation	Trusted testing department
10	Cloud lose you lose	Jurisdictions and service level agreements
11	Metering and billing	Mechanism by hash based techniques

of cloud. Software licensing method should be clear and in simple format that the user can easily grasp the matter written in the licensing document. Data location represents the geographically distribution of data. Whether the data stored at single place or distributed at different location to increase the reliability [17-18].Data segregation simply means the software runs in the cloud should be properly tested and developed by recognized and authenticated organizations. Cloud lose you lose means simply a cloud company lose everything then how it will return your important data. The last and most important obstacle is how the enterprises show the procedure of billing of resources used by the user. This obstacle create fear in the user mind regarding the billing charges , so many doubts for user like the provider charges fairly and using proper metering methods raises [19].

IV. PROPOSED WORK

User always thinks about the benefits to shift to cloud, to show the benefits of using the cloud over the datacenter, a method is proposed. The algorithm given below calculates and compares the net revenue by using the cloud and datacenters. Left hand side of step 3 multiplies the net revenue (revenue earned per user hour minus price of paying cloud computing per user hour) shows the profit by using cloud computing. We assume that customer's net revenue is directly proportional to total number of hour user spend whether on cloud or datacenter.

1. Calculate actual average utilization of server per hour in cloud.
2. Calculate peak provisioning usage of server per hour in datacenter.
3. Factorize the results of step 1 and step 2 by using the method described below

$$UH_C * (\text{Gross income} - \text{Cloud}_{cost}) \geq UH_D * (\text{Gross income} - \text{Datacenter}_{cost} / \mu)$$

4. Evaluate the results and choose the better option for your enterprises.

UH_C = Utilization of server per hour in cloud.
UH_D = Utilization of server per hour in datacenter.
μ = Utilization factor.

The right hand side calculates the same for a fixed capacity datacenters as like of our home computer systems by factoring in the average utilization. This always works on average work load. These two equations are same except the utilization factor on the right hand side. In practice the utilization of resources in datacenters is always lies in 0.6 to 0.8. If utilization is 1 means all the resources in datacenter are utilized 100%, then two equation results the same. Greater value of cloud side represents the opportunity of higher profit in cloud. But in practice if we lease 100 Mb/s internet links we utilize only 60Mb/s to 80 Mb/s. Similar in all resources it is difficult to achieve the 100% of utilization. So in maximum cases cloud side gives you more profit.

Case1. Suppose the enterprise has predictable demand of 700 servers in the peak work load at noon but at midnight the demand of server required is decreased to 100. Then the average utilization of server over the whole day is 400 servers. The utilization of server per hour over whole day is 400*24 = 9600 server per hour. So we pay for 9600 server-hour in cloud. But in datacenter we require 700 servers in peak. Server-hour usage is 700*24 = 16800 server-hours. In datacenter we pay for 16800 server-hours. Therefore in utility computing, cost per server-hour over 3.5 years is less than 1.8 times the cost of buying the server. So shifting to cloud is right option.

Case2. Suppose the lab in enterprise create 600GB of data for experiment. In lab, computer has speed of 2GB/hour. The lab has 20 equivalent instances for creating data. So the time required to create the data is (2*600)/20 = 60 hours in case of datacenters. Similar work is done on cloud by using 1000 instance at the same time in single hour. The cost of single instances is $0.1 in all cloud provider enterprises, so the total cost is 1000*$0.1 + 600*$0.1(network transfer fees) = $160. The data transfer rate is 20Mb/s. The total transfer time required is = (600GB * 1000MB/GB * 8bits/bytes) / 20Mb/s = 66.6 hours. Therefore these results shows cloud is not beneficial for user.

V. FUTURE DIRECTIONS

Although the cloud has more advantages than its shortcomings, but still the thrust and major area of research in the field of security in cloud is to find technical solutions for the interoperability among the cloud. We discussed various attacks and threats in different deployment and development models. These all are highlighted areas as per as the implementation of the cloud is concerned. All Cloud enterprises should assure an exit or a migration policy across multiple clouds thereby avoiding the obstacle of data lock-in. Second is enabler ecosystem. At infrastructure level various complex domains attacks happened. So researchers need to work on these attacks. These domains are computing, network, storage, security, software applications and service management. Within those domains, there are several areas of complexity including integration, interoperability, operation, scalability, and compliance. Still the dominating part of cloud is security at each level of deployment model. Different solutions to security have been suggested. These solutions include cloud trust models, reconfigurable computing and cryptography and identity access management. Still, efficient solutions are required for different domains of clouds.

VI. CONCLUSION

Inevitably cloud computing is a new and promising paradigm that support information system as their benefits, which outnumber its shortcomings. It delivers its services as utility computing. Cloud computing's growth is in its awful phase due to its value propositions of low costs, improved performance, unlimited storage capacity and increased computational power. Enterprises across all sectors are eager to adopt cloud computing but the security is required for both to accelerate cloud adoption on large scale and to respond regulatory drivers. Currently cloud computing security issues have lot of loose ends which create uncertainties in the mind of potential user. Until a proper security module is not placed, the enterprises or single users are unable to leverage the advantages of this growing technology. By enhancing security and privacy policies more enterprises are attracted towards the world of cloud computing. In this paper deployment models, threats in security parameters, key security issues and challenges at each layer of cloud are highlighted. This paper describes the requirement of security at different service models and focus to under developed areas. By following this paper, the anxiety of cloud can be easily expelled, saving enterprises time and investment. This service can be easily integrated by different organizations such as banking, search engines and enterprise applications.

REFERENCES

[1] G. Cheng, H. Jin, D. Zou and X. Zhang, "Building Dynamic and Transparent Integrity Measurement and Protection for Virtualized Platform in Cloud Computing", Concurrency and Computation: Practice and Experience, vol. 22, pp. 1893–1910, 2010.

[2] M. Armbrust, A. Fox, R. Griffith, A. D Joseph, R. Katz, L. Konwinski and G. Lee, "Above the clouds: A Berkeley View of Cloud Computing", University of California, Berkeley, Tech. Rep. USB-EECS-2009, vol.28, pp. 23-29, 2009.

[3] Y. Shen, K. Li and L. T. Yang, "Advanced Topics in Cloud Computing", Journal of Network and Computer Applications, vol. 12, pp. 301- 310, 2010.

[4] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing", Journal of Network and Computer Applications, vol. 34, no. 1, pp.1-11, 2010.

[5] R. Chow, P. Golle, M. Jakobsson, E. Shi and Jessica Staddon, "Controlling Data in the Cloud Outsourcing Computation without Outsourcing Control", CCSW', Chicago, Illinois, USA, 2009.

[6] F.Lombardi and R. D. Pietro, "Secure Virtualization for Cloud Computing", Journal of Network and Computer, vol. 12, pp. 407- 412, 2010.

[7] K. Julisch and M. Hall, "Security and Control in Cloud", Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 299-309, 2010.

[8] R.Farrell," Securing the Cloud-Governance, Risk and Compliance Issues Reign Supreme", Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 310-319, 2010.

[9] B.T.Ward and J.C.Sipior, "The Internet Jurisdiction Risk of Cloud Computing", Information Security Systems Management, vol.27, no. 4, pp. 334-339,2010.

[10] E.Orakwue, "Private Cloud: Secure managed services", Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 295-298, 2010.

[11] A.Parakh and S.Kak, "Online Data Storage Using Implicit Security", Information Sciences, vol.179, no. 6, pp. 3323-3331, 2009.

[12] A.Butt, S.Adabala, N.Kapadia and A.B.Fortes, "Grid-Computing Portal and Security Issues", Journal of Parallel and Distributed Computing, vol. 63, no.10, pp. 1006-1014, 2003.

[13] R.Buyya, S.Yeo, S.Venugopal, J.Broberg and I.Brandic, "Cloud Computing and Emerging IT Platform: Vision, Hype and Reality for Delivering Computing as the 5th Utility", Future Generation Computer System, vol. 25, no.7, pp. 599-616, 2008.

[14] H. Sato, A. kanai and S. Tanimoto, "A Cloud Trust Model in a Security Aware Cloud", IEEE International symposium on Applications and the Internet, pp. 121-124, 2010.

[15] L.M. Kaufman, "Data Security in the World of Cloud Computing", IEEE Security and Privacy, vol. 7, no. 4, 2009.

[16] Y. Shen, K. Li and L. T. Yang, "Advanced Topics in Cloud Computing", Journal of Network and Computer Applications, vol. 12, pp.301- 310, 2010.

[17] V. Casola, A. Mazzeo, N. Mazzocca, and V. Victoriana, "A Security Metric for Public key Infrastructures", Journal of Computer Security, vol. 15, no. 2, pp. 78-85, 2007.

[18] F.Lombardi and R. D. Pietro, "Secure Virtualization for Cloud Computing", Journal of Network and Computer, vol. 12, pp. 407- 412, 2010.

[19] S. A. Almulla and C. Y. Yeun "Cloud Computing Security Management" IEEE International Conference on Service Computing, pp. 121-126, 2010.