Security Issues and Challenges in Cloud Computing

Palvinder Singh
M-Tech (CSE) Student
Geeta Institute of Management & Technology,
Kanipla, Kurukshetra, India

Er. Anurag Jain
Assistant Prof.
Dept. of Computer Science & Engg.
Geeta Institute of Management & Technology,
Kanipla, Kurukshetra, India

***Abstract*— Cloud computing is an emerging computing paradigm that gives the concept of time shared remote services with attractive technological and financial advantages. The infrastructure uses new technology and services that haven't been absolutely evaluated with relevancy security. In this paper, first of all we glance into the impacts of the distinctive characteristics of cloud computing such as multi-tenancy, elasticity and third party management, upon the protection necessities. Then, we tend to analyze the cloud security necessities in terms of the elemental security problems, i.e., confidentiality, integrity, convenience, trust, and audit and compliance.**

***Keywords*— Cloud security; Data Availability; Integrity; Authentication; Side channel attack**

I. INTRODUCTION

All around digital computer science history, numerous endeavors are created to separate shoppers from machine fittings wants, from time-imparting utilities notional within the Sixties, system machines of the Nineteen Nineties, to the business network frameworks of later years. This deliberation is unrelentingly turning into associate existence as numerous scholastic and business pioneers during this field of science are spiral towards distributed computing. Distributed computing is an ingenious data system (IS) construction modeling, pictured as what is also what is to come back for calculation, a main impetus requesting from its gathering of individuals to canvass their understanding of operating frameworks, client–server architectures, and programs. Distributed computing has leveraged shoppers from instrumentality stipulations, whereas decreasing general client aspect requirements and many-sided quality. As distributed computing is attaining enlarged infamy, issues are perpetually voiced concerning the protection problems conferred through the choice of this new model. The adequacy and effectiveness of universal security systems are endlessly rethought, because the attributes of this inventive organization model, vary typically from them of accepted architectures. During this paper we have a tendency to endeavor to clear up the novel security tests conferred during a cloud setting and clear up problems from a security viewpoint.

The thought of trust and security is researched and explicit security stipulations are recorded. This paper proposes a security result that powers customers from the protection load, by basic cognitive process a 3rd Party. The Third Party is tasked with guaranteeing explicit security aspects within a circulated knowledge framework, whereas understanding a trust work between enclosed components, structuring leagues of mists. The examination approach embraced towards accomplishing this objective relies upon programming building and knowledge frameworks define approaches. The elemental steps for designing the framework building style incorporate the gathering of requirements and therefore the dissection of theoretical utilitarian determinations [1].

The new thought of Cloud Computing offers dynamically ascendable resources provisioned as a service over the net and thus guarantees lots of economic edges to be distributed among its adopters. Betting on the kind of resources provided by the Cloud, distinct layers may be outlined (see Figure 1). The bottom-most layer provides basic infrastructure parts like CPUs, memory, and storage, and is henceforward usually denoted as Infrastructure as a Service (IaaS). Amazon's Elastic figure Cloud (EC2) may be a distinguished example for associate IaaS supply.

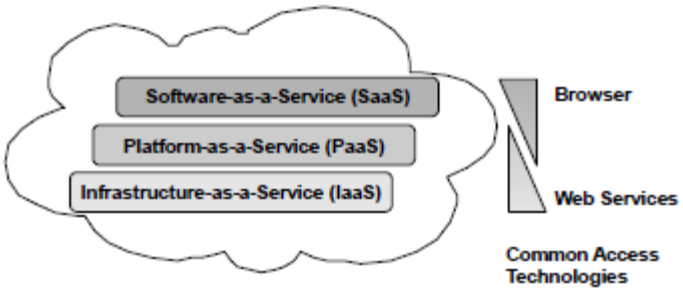

Figure 1. Cloud Layers and Access Technologies [2].

On prime of IaaS, a lot of platform-oriented services permit the usage of hosting environments tailored to a selected would like. Google App Engine is associate example for an internet platform as a service (PaaS) that permits to deploy and dynamically scale Python and Java primarily based net applications. Finally, the highest layer provides it users

with able to use applications additionally called code as-a-Service (SaaS). To access these Cloud services, two main technologies may be presently known. Net Services are normally wont to give access to IaaS services and net browsers are wont to access SaaS applications. In PaaS environments each approach may be found.

All of those layers associate with the promise to scale back 1st of all capital expenditures (CapEx). This includes reduced hardware prices within the IaaS layer and reduced license prices altogether layers. particularly within the IaaS layer it's not needed any longer to engineer the own knowledge center for peak performance cases, that occur generally terribly rarely and that typically lead to a poor utilization of the obtainable resources. In addition, reductions of the operational expenditures (OpEx) in terms of reduced hardware, license and patch management are securing still [2].

II. SECURITY CHARACTERISTICS OF CLOUD

Cloud has following security characteristics:

A. Multi-Tenancy-

Multi-tenancy, because the term implies, refers to having over one tenants of the cloud living and sharing different tenants the provider's infrastructures, together with process resources, storage, services, and applications. By multi abidance, clouds offer synchronic, secure hosting of services for varied customers utilizing identical cloud infrastructure resources. Multi-tenancy may be a feature distinctive to resource sharing in clouds, particularly publicly clouds. Primarily, it permits cloud suppliers to manage resource utilization a lot of expeditiously by partitioning a virtualized, shared infrastructure among varied customers. High degrees of multi-tenancy over giant numbers of platforms square measure required for cloud computing to attain the visualized flexibility of on-demand provisioning of reliable services and therefore the price advantages and efficiencies because of economies of scale. To succeed in the high scales of consumption desired, service suppliers got to guarantee dynamic versatile delivery of service and isolation of user resources. Multi abidance in cloud computing is completed generally by multiplexing the execution of VMs for doubtless totally different users on identical physical server. Virtualization and multi-tenancy square measure the large problems on victimization cloud computing. because the cloud may be a shared resources setting, organization need to confirm that every one tenant domains square measure properly isolated from one another that no risk exists for information or transactions to leak from one tenant domain into ensuing. Shoppers want the flexibility to tack trustworthy virtual domains or policy-based security zones. From a customer's perspective, the notion of employing a shared infrastructure might be an enormous concern. This undoubtedly raises a hair attributable to inadequate segregation among cloud customers. What happens once a security vulnerability causes one client to look at (and within the worst case to change) another client's data? The opposite customer won't have evil intents however you ne'er grasp. However, the amount of resource sharing and accessible protection mechanisms will create a giant distinction.

Cloud computing is predicated on a business model within which resources square measure shared (i.e., multiple users use identical resource) at different level (network level, host level, and application level). In multi abidance, many aspects of the data system square measure shared together with, memory, programs, networks and information. Though user's square measure isolated at a virtual level, hardware isn't separated. With a multi-tenant design, a package application is meant to nearly partition its information and configuration in order that every client organization works with a custom virtual application instance.
Providers should account for problems like access policies, application preparation, and information access and protection to produce a secure, multi-tenant setting.

B. Elasticity-

In cloud computing, customers ought to use resources as way required whereas having the ability to extend or decrease resources consumption supported actual demands. To fulfill such desires, cloud services got to be ascendible, i.e., the desired resources of storage and computing power may be magnified or belittled supported customers' desires.

Elasticity implies having the ability to proportion or down resources allotted to services supported this demand. Scaling up and down of a tenant's resources offers the chance to different tenants to use the tenant's antecedently allotted resources. This might cause confidentiality problems. As an example, once Tenant A scaled down therefore it releases resources, these resources square measure currently allotted to Tenant B United Nations agency successively uses it to deduce the previous contents of Tenant A. Moreover, physical property contains a service placement engine that maintains a listing of the accessible resources from the provider's offered resources pool. This list is employed to assign resources to services. Such placement engines ought to incorporate cloud customers' security and legal needs like competitors services ought to be avoided being placed on identical server; information location ought to be among the tenants' country boundaries. Placement engines might embrace a migration strategy wherever services square measure migrated from one physical host to a different or from cloud to a different so as to fulfill demands and economical utilization of the resources. This migration strategy ought to take into consideration identical security constraints. Moreover, security needs outlined by customers ought to be migrated with the service and initiate a method to enforce security needs on the new setting, as outlined by cloud customers, and updates this cloud security model.

C. Multiple Stakeholders-

In a cloud computing model there are totally different stakeholders involved: cloud supplier (an entity that

delivers infrastructures to the cloud customers), service supplier (an entity that uses the cloud infrastructure to deliver applications to finish users), and client (an entity that uses services hosted on the cloud infrastructure). Every neutral has their own security management systems and their own expectations (requirements) and capabilities (delivered) from different stakeholders. This ends up in the subsequent problems.

(i) Every neutral has their own security management processes accustomed outline their assets, expected risks and their impacts, and the way to mitigate such risks;

(ii) Suppliers and customers got to talk terms and agree upon the applied security properties. However, no normal security specification notations are accessible which will be utilized by the cloud stakeholders to represent and reason regarding their required security properties;

(iii) With respect to the multi-tenant atmosphere, the protection necessities for every tenant would possibly dissent, which may create a multi-tenant cloud one purpose of compromise. A group of security necessities outlined on a service by totally different tenants that will conflict with one another. thus security configurations of every service ought to be maintained and implemented on the service instances level and at runtime taking under consideration the chance of fixing necessities supported current customers' has to mitigate new risks;

(iv) Additionally, every tenant may have totally different trust relations with the provider and some tenants may truly be malicious attackers themselves— therefore generating advanced trust problems.

D. Third-Party Control-

The major security challenge is that the third-party issue, that is, the owner of the information has no management on their processing. the most important amendment for info Technology (IT) department of the organization victimization cloud computing are going to be reduced management as they're being tasked in-tuned raised responsibility for the confidentiality and compliance of computing practices within the organization. A connected concern is correct governance of cloud connected activity. Even as in ancient IT outsourcing, victimization cloud services needs the client to convey up management over his IT infrastructure. To create customers take this step easier, cloud suppliers ought to create the management and maintenance of cloud services additional clear and auditable by the purchasers. This could embrace recording logs and complete body sessions moving the part of the cloud infrastructure utilized by the client - and if requested by the client creating these accessible.

On the opposite facet, cloud suppliers aren't able to deliver economical and effective security controls as a result of they're not conscious of the hosted services' architectures. Moreover, cloud suppliers are two-faced with plenty of changes to security necessities whereas having a spread of security controls deployed that require to be updated. This any complicates the cloud providers' security administrators' tasks. A key issue for cloud computing is that aspects of ancient infrastructure security move on the far side associate degree organization's management and into the cloud. This may cause basic changes within the range and roles of security stakeholders as enterprises flip over management of security infrastructure and processes to outside contractors. Trust relationships between varied cloud stakeholders (users, companies, networks, service suppliers, etc.) want careful thought as public cloud computing evolves to manage sensitive enterprise information [3].

III. GENERAL REQUIREMENTS ON CLOUD SECURITY

Security is in general related to the important aspects of confidentiality, integrity, authentication, Trust and availability.

i. Cloud Availability

Availability is crucial since the core perform of cloud computing is to produce on-demand service of various levels. If an explicit service isn't any longer accessible or the standard of service cannot meet the Service Level Agreement (SLA), customers could lose religion within the cloud system. During this section, we've studied 2 sorts of threats that impair cloud handiness.

Threats to Cloud Availability:

a) Flooding Attack via information measure Starvation:

In a flooding attack, which might cause Deny of Service (DoS), a large quantity of nonsensical requests square measure sent to a specific service to hinder it from operating properly. In cloud computing, there square measure 2 basic forms of flooding attacks:
Direct DOS – the assaultive target is decided, and also the handiness of the targeting cloud service is totally lost.
Indirect DOS – which means is twofold:

1) All services hosted within the same physical machine with the target victim are affected;

2) The attack is initiated while not a particular target.

b) Fraudulent Resource Consumption (FRC) attack:

A representative Economic Denial of property (EDoS) attack is FRC that could be a delicate attack which will be dispensed over a protracted amount (usually lasts for weeks) so as to require result. In cloud computing, the goal of a FRC attack is to deprive the victim (i.e., regular cloud customers) of their semi permanent economic handiness of hosting net contents that square measure in public accessible. In different words, attackers, UN agency act as legal cloud service purchasers, endlessly send requests to web site hosting in cloud servers to consume information measure that bills to the cloud client owning site; appears

to the web server, those traffic doesn't reach the amount of service denial, and it's tough to differentiate FRC traffic from different legitimate traffic. A FRC attack succeeds once it causes money burden on the victim [4].

ii. Privacy and Integrity of Cloud Data

Resource exposure over the web by the Cloud computing is employed for the valid users and malicious attackers. Net browsers and remote connections, SOAP, REST, Virtual Private Network, Extensible Markup Language and Remote Procedure Connection Protocols, APIs area unit accustomed access the resources of the tenants. Organizations or Business should have trust with the cloud supplier once it ports its info within the cloud. Poor cloud infrastructure results in the planning or security design flaws in a very shell and area unit varied problems that comes with the integrity and confidentiality of the resident info within the environments of cloud supplier. A number of the authentication and privacy problems area unit Absence of authentication, accounting protocols and authorization.

- Key for coding and decoding isn't managed.

Specific problems like mutual trust between the patron and supplier of the cloud isn't convenient. Authentication ought to be done properly, providing Cloud Services by the supplier to the patron with accounting details, specified any try of knowledge access is finished by structure checking and ensures solely the tenants UN agency area unit approved will have the rights for accessing the data. The data access ought to be individual by the credentials, access secured mechanism that ranges from RSA certificate to secure shell (SSH) tunnel based mostly. A key management augments have secure access to the information, and is aware of regarding the key accessibility either with the shopper or supplier for the aim of coding and decoding sympathy between the cloud supplier and organization is finished for porting the information [5].

iii. Data Security

The sensitive knowledge of an enterprise exist among the enterprise state boundary, however within the SaaS model the enterprise knowledge is hold on at the SaaS service supplier finish. That the further security checks should be enforced by the SaaS service supplier to make sure the information security. This might embrace the strong encoding and authorization systems to manage the unauthorized access to the information. Some assessments to manifest the safety of the enterprise knowledge at the SaaS service supplier finish are:

- Cross-site Scripting (XSS)
- Access management weaknesses
- OS and SQL injection flaws
- Cookies manipulation
- Hidden filed manipulation

If any weakness is perceived in these take a look at results in access of sensitive knowledge by an unauthorized person [6].

iv. Trust

Under the cloud computing paradigm, a corporation relinquishes direct management over several aspects of security and, in doing therefore, confers an unprecedented level of trust onto the service supplier.

a. Business Executive Access-

Knowledge processed or holds on outside the scope of a corporation, its firewall, and alternative security controls bring with it an inherent level of risk. The business executive security threat could be a well-known issue for many organizations and, despite the name, applies also to outsourced cloud services. Business executive threats transcend those expose by current or former staff to incorporate structure affiliates, contractors, and alternative parties that have received access to an organization's networks, systems, and knowledge to hold out or facilitate operations. Incidents might involve numerous kinds of fraud, sabotage of data resources, and felony of data. Incidents can also be caused accidentally. Moving knowledge and applications to an external cloud computing atmosphere expands the business executive security risk not solely to the service provider's employees, however additionally doubtless among alternative customers victimization the service. for instance, an inside denial of service attack against the Amazon Elastic calculate Cloud (EC2) was incontestable that concerned a service user making AN initial twenty accounts and launching virtual machine instances for every, then victimization those accounts to form an extra twenty accounts and machine instances in an unvaried fashion to grow and consume resources exponentially.

b. Composite Services-

Cloud services themselves may be composed through nesting and layering with alternative cloud services. For example, a SaaS supplier may build its services upon those of a PaaS or IaaS cloud. Cloud service suppliers that subcontract some services to third-party service suppliers ought to raise issues, together with the scope of management over the third party, the responsibilities concerned, and therefore the remedies and recourse obtainable ought to issues occur. Trust is usually not transitive, requiring that third-party arrangements be disclosed beforehand of reaching AN agreement with the service supplier, which the terms of those arrangements square measure maintained throughout the agreement or till comfortable notification may be given of any anticipated changes. Liability and performance guarantees will become a significant issue with composite cloud services. The Linkup, an internet storage service that closed down when losing access to a big quantity of knowledge from its

20,000 customers, illustrates such a state of affairs. As a result of another company, Nirvanix, hosted the info for the fixing, and yet one more, Savvis, hosted its application and info, direct responsibility for the explanation for the failure was unclear.

c. Visibility-

Migration to cloud services relinquishes management to the service supplier for securing the systems on that the organization's knowledge and applications operate. To avoid making gaps in security, management, procedural, and technical controls should be applied commensurately with those used for internal structure systems. The task is formidable, since metrics for examination the protection of two laptop systems square measure AN in progress space of analysis.

Moreover, network and system level observance by the user is mostly outside the scope of most service arrangements, limiting visibility and therefore the means that to audit operations directly. To confirm that policy and procedures square measure being enforced throughout the system lifecycle, service arrangements ought to contain some means that for gaining visibility into the protection controls and processes utilized the service supplier, also as their performance over time [7].

v. Side Channel Attack

Infrastructure as a Service (IaaS) model in cloud computing provides infrastructures sort of a assortment of multiple computers, virtual machines(VMs) and different resources to its users to store their application, file, wind, documents so on. mistreatment the Amazon EC2 service as a case study, it's doable to map the interior cloud infrastructure and establish wherever a specific target VM is probably going to reside, and so instantiate new VMs till one is placed co-resident with the target VM. once the with success placement of instantiate VM to targeted VM then extract the wind from the targeted VM known as a Side channel attack.

Side channel attack needs two main steps: Placement and Extraction.

- Placement refers to the antagonist or assaulter composition to position their malicious VM on an equivalent physical machine.
- Extraction: once with success placement of the malicious VM to the targeted VM extract the wind, file and documents on the targeted VM [8].

vi. Audit and Compliance

For compliance and audit the access are going to be monitored and tracked to make sure that there'll be no security breaches within the system. It additionally can facilitate auditors to verify the fulfillment to completely different access management policies, periodic auditing and coverage. Auditing is that the method of reviewing and examining the authorization and authentication records so as to see whether or not compliances with predefined security standards and policies are assured. Also, it'll aid in police investigation any system breaches. For the cloud systems utilized by the client, the client ought to be able to authorize and probably monitor access to the system. Such observance might be as straightforward as following the logs on a web interface, or as subtle as looking at a period of time audit path of the administrator's actions on the system - be it on a particular virtual machine, or the hypervisor of the complete system. Reliable, secure and tamper-proof log assortment and log storage is additionally necessary. Looking on the sort of access to cloud system, solutions that may record the actions of the user's particularly privileged users like directors - are extraordinarily useful not just for knowledge abuse hindrance, however additionally for forensics and compliance reasons. Audit problem is additionally the result of the dearth of management within the cloud. Is there decent transparency within the operations of the cloud supplier for auditing purposes? Presently, this transparency is provided by documentation and manual audits.

A cloud supplier should have practices and powerful policies that address regulative and legal problems, and also the client has to examine cloud supplier policies and practices to make sure their adequacy. Cloud customers are ultimately answerable for the safety and integrity of their own knowledge even once it's command by a service supplier. The shoppers got to be able to prove compliance with security standards no matter the situation of their systems. It is necessary to make sure that cloud computing suppliers are duty-bound to endure external audits and security certifications within the same manner that ancient service suppliers do [9].

vii. Distributed Denial of Service Attack (DDoS)

There are 2 kinds of threats i.e. Extortionists-Using DDoS attack to exhaust server resources and Competitors-Using famous vulnerabilities to interrupt services. Once the flood of messages attacks all nodes by totally different nodes system at same time it's called Distributed Denial of Service (DDoS). complicated and easy kinds of DDoS attack tools we've got, Agobot, Mstream and Trinoo area unit in complicated classes and X-Dos (XML primarily based} Denial of service) yet as H-Dos (HTTP based Denial of service) area unit in easy classes. (Extensible Markup Language)-based Denial of Service (X-DoS) and (Hypertext Transfer Protocol) primarily based} Denial of Service (H-DoS) area unit employed by most assaulter as they inclined to use easier internet based attack tools owing to their easy implementation and in need of real defences against them. X-DoS with DX-DoS(distributed XML based mostly Denial of Service), it distributed version happens once message of XML varieties is shipped to an online server with or while not wicked content by victimization their all resources. Powerful Parsing attack is associate degree example of associate degree X-Dos attack during

this internet Service request is manipulated once content is parsed by SOAP (Simple Object Access Protocol) to remodel it into accessible type to the applying. An eternal series of open tags area unit use by powerful Parsing attack to create central processor usage exhausted on associate degree Axis2 internet server. Some 1500 threads area unit starts up by communications protocol Flooder to create communications protocol randomized requests to victim internet server to create communication channels exhaust within the H-Dos attack. That the purpose is created that there's no thanks to filter such traffic and to differentiate between communications protocol request that area unit legitimate and illegitimate [10].

IV. CONCLUSION

Every new technology has its execs and cons, similar is that the case with cloud computing. Though cloud computing provides straightforward knowledge storage and access. However there are many problems associated with storing and managing knowledge that's not controlled by owner of the information. This paper mentioned security problems for cloud. These problems embrace cloud integrity, cloud confidentiality, cloud handiness, cloud privacy. There are many threats to cloud confidentiality as well as cross-VM attack and malicious sysadmin. On the opposite hand integrity of cloud is compromised because of knowledge loss and dishonest computation in remote servers. DoS (Denial of Service attack is that the commonest attack that is additionally doable in cloud computing network. This attack tries to forestall the information offered to its supposed users. The last issue is cloud privacy and it's just like cloud confidentiality. If cloud confidentiality is in danger, cloud privacy also will be in danger.

REFERENCES

1. Dimitrios Zissis, Dimitrios Lekkas "Addressing cloud computing security issues" in Proceeding of Future Generation Computer Systems, pp. 583–592, 22 December 2010.
2. Meiko Jensen, J¨org Schwenk, Nils Gruschka, and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in Proceeding of 2009 IEEE International Conference on Cloud Computing, pp. 109-116, 21-25 Sept. 2009.
3. Huaglory Tianfield "Security Issues In Cloud Computing" in Proceeding of 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC'12), Seoul, Korea, pp. 1082-1089, 14-17 October 2012.
4. Abhishek Goel, Shikha Goel "Security Issues in Cloud Computing" in Proceeding of International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 1, Issue 4, December 2012.
5. Dr. A. Askarunisa; N.Ganesh; A.Athiraja; Venkatesh; "Security Issues in Cloud Computing" in Proceeding of International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 3 Issue 1 September 2013.
6. Prashant Kumar, Lokesh Kumar, Kapil Kumar, Sachin Kumar, Sohan Lal " Security Threats to Cloud Computing" in Proceeding of International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) Volume 2, No. 1, December 2013.
7. Wayne A. Jansen; "Cloud Hooks: Security and Privacy Issues in Cloud Computing", in Proceedings of the 44th Hawaii International Conference on System Sciences – 2011.
8. Bhrugu Sevak " Security against Side Channel Attack in Cloud Computing", in Proceeding of International Journal of Engineering and Advanced Technology (IJEAT) Volume-2, Issue-2, December 2012.
9. Huaglory Tianfield "Security Issues In Cloud Computing" in Proceeding of 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC'12), Seoul, Korea, pp. 1082-1089, 14-17 October 2012.
10. Aman Sagar, Bineet Kumar Joshiyand Nishant Mathurz "A Study of Distributed Denial of Service Attack in Cloud Computing (DDoS)" in Proceeding of HCTL Open Science and Technology Letters (HCTL Open STL), August 2013.