IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-17, May 2019 E-ISSN: 2347-2693

Cloud Computing: Study of Security Problems and Analysis Challenges

M. Angelin Rosy[1*], V. Shanthakumar[2], M. Felix Xavier Muthu[3]

[1,2,]Department of MCA, Er.Perumal Manimekalai College of Engineering, Anna University, Hosur, India
[3]Dept. of Mechanical Engineering, St.Xavier's Catholic College of Engineering, Anna University, Nagercoil, India

Corresponding Author: angel_rosym@yahoo.co.in, Tel- 9944579754

Available online at: www.ijcseonline.org

Abstract - Cloud computing is that the apply of employing a network of remote servers hosted on web to store, manage and method information on demand and pay as per use.
It provides access to a pool of shared resources rather than native servers or personal computers. As it doesn't acquire the items physically, it saves managing value and time for organizations. Cloud computing could be a utterly web dependent technology wherever consumer knowledge is hold on and maintain within the knowledge center of a cloud supplier like Google, Amazon, Microsoft etc .Cloud computing is an rising domain and is acclaimed throughout the globe. There are some security problems locomotion in whereas mistreatment services over the cloud. This analysis paper presents a review on the cloud computing ideas moreover as security problems inherent inside the context of cloud computing and cloud infrastructure. This paper additionally analyzes the key analysis and challenges that presents in cloud computing and offers best practices to service suppliers moreover as enterprises hoping to leverage cloud service to enhance their bottom line during this severe economic climate and intensify its usage. The main stress of our study supported existing literature and to know the idea of multi-tenancy security issue.

Keywords–Cloud computing, Multitenancy, Data, management.

I. INTRODUCTION

Cloud Computing could be a distributed design that centralizes server resources on a ascendable platform therefore on offer on demand computing resources and services.

Cloud Service suppliers (CSP's) provide cloud platforms for his or her customers to use and build their net services, very like web Service suppliers (ISP's) provide costumers high speed broadband to access the internet. CSPs and ISPs both offer services. [1]

Cloud computing might be a model that allows convenient, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications which will be quickly

Figure1

Provisioned and discharged with token management effort or service provider's interaction. [6]

Clouds are a unit the new trend within the evolution of the distributed systems. Earlier to Cloud we used Grid.
In Cloud Computing, the user doesn't need information or experience to regulate the infrastructure of clouds; it provides solely abstraction. [2]
It may be utilized as a service of the net with high measurability, higher outturn, quality of service and high computing power.

Cloud computing suppliers deliver common on-line business applications that square measure accessed from servers through application. [4]

Recent developments within the field of Cloud computing have vastly modified the method of computing likewise because the thought of computing resources.

In a cloud based mostly computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users. [3]

In some cases, it would be needed or a minimum of attainable for someone to store information on remote cloud servers.

This offers the subsequent 3 sensitive states or situations that are a unit of specific concern among the operational context of cloud computing:

• The transmission of private sensitive knowledge to the cloud server.

• The transmission of knowledge from the cloud server to clients' computers.

• The storage of shoppers' personal knowledge in cloud servers that are unit remote servers not closely-held by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one. [2]
The aspects presented in this paper are organized with a view to discuss and indentify the approach to cloud computing as well as the security issues and concerns that must be taken under consideration within the preparation towards a cloud based mostly computing infrastructure.

Discussion on the technological ideas and approaches to cloud computing together with the bailiwick illustration has been taken into thought among the context of dialogue during this paper.
Security problems inherent in cloud computing approach are mentioned afterward.
The exploration within the technological and security issues of cloud computing has LED to the terminal realization on the general aspects of cloud computing.

II. CLOUD COMPUTING DESIGN

2.1 SERVICE MODELS [1]

Loosely cloud suppliers supply 3 kinds of services:

- Software as a Service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Software as a Service (SaaS):
It's additionally known as a delivery model wherever the package and therefore the knowledge that is related to is hosted over the cloud setting by third

Party called cloud service provider, just like your Gmail account, you use that application on someone else's system. [1]

Platform as a Service (PaaS):
During this service, you'll be able to use Web-based tools to develop applications in order that they run on program that is provided by another company, like Google App Engine. [1]

Infrastructure as a Service (IaaS):
It provides services to the business with computing resources including servers, networking, storage, and datacenter space on a pay-per-use basis. [1]

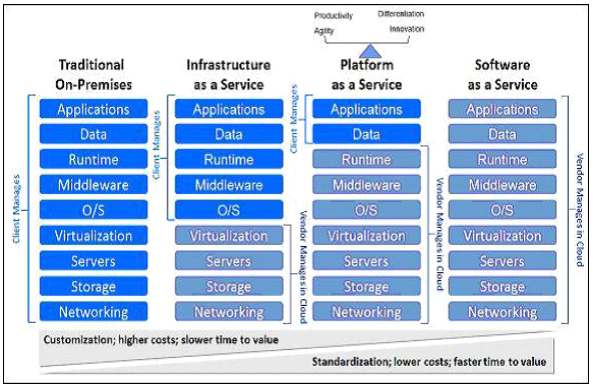

Figure 2

2.2 Deployment models[3]

There square measure 3 readying Models and square measure represented below:

* Public Model
* Private Model
* Hybrid Model

Public Model: This infrastructure is on the market to the overall public.
As the name suggests, public cloud is be a model with in which resources are a unit typically on the market to everyone and anyplace. [3]

Private Model: This model is developed for the non-public organizations like one house and a company and that they will use it for his or her own purpose.
This kind of a service is not accessed by everyone. [3]

Hybrid Model: Hybrid Clouds square measure combination of public and personal cloud in an exceedingly same network.
This will be done if non-public cloud want some necessary services from the general public cloud like non-public cloud will store some data on their non-public cloud and that we can use that information on public cloud. [3]

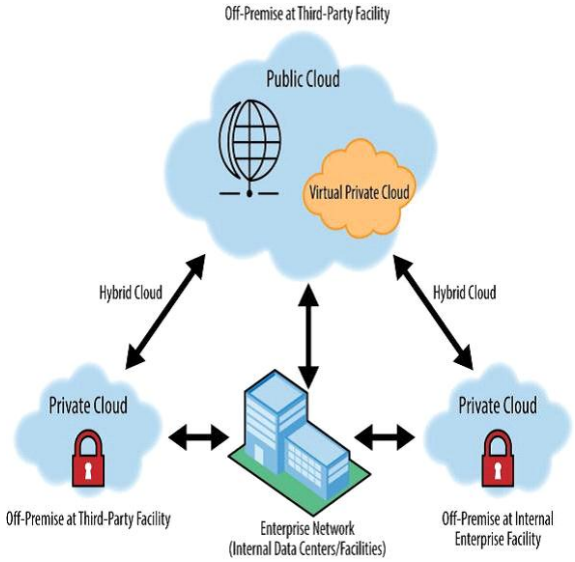

Figure 3

III. SECURITY ISSUES IN CLOUD COMPUTING[5]

Cloud computing contain applications, platforms and infrastructure segments.
Every phase performs totally {different | completely different} operations and offers different merchandise for businesses and people round the world.
There are a unit various security issues for cloud computing because it encompasses several technologies which incorporates networks, databases, operating systems, virtualization, resource scheduling, transaction management, concurrency control and memory management.
Therefore, security problems for several of those systems and technologies square measure applicable to cloud computing.

Data security involves encrypting information the info the information} additionally as guaranteeing that acceptable policies square measure implemented for data sharing.

The given below square measure the varied security considerations in an exceedingly cloud computing setting.

• **Access to Servers & Applications**[6]
• Data Transmission
• Virtual Machine Security
• Network Security• Data Security
• Data Privacy
• Data Integrity
• Data Location
• Data Availability
• Data Segregation
• Security Policy and Compliance

3.1 Data Transmission

It is the method of causation digital or analog knowledge over a communication medium to 1 or additional computing network.
In Cloud surroundings most of the information isn't encrypted within the time interval.
To method knowledge for any application that knowledge should be unencrypted.
In similarity secret writing that permits the information to be processed while not being decrypted.
The attack is administered once the attackers place themselves within the communications path between the users.

Here there's the chance that they will interrupt and alter communications.

3.2 Virtual Machine Security

The term Virtual Machine (VM) describes sharing the resources of 1 single physical pc into varied computers at intervals itself.
VM's offer legerity, flexibility and scalability to the cloud resources by allowing the vendors to copy, move and manipulate their VM's.

The cloud computing state of affairs isn't as clear because it claims to be.
The service user has no plan regarding however the information is processed and keep and can't directly management the flow of information storage and process.
Having VM's would indirectly permits associate degree one access to the host disk of the VM to require an black-market copy of the entire system.

3.3 Data Integrity

Corruption of information will happen at any level of storage.
So Integrity monitoring is must in cloud storage. Data Integrity in a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation, durability).
Data generated by cloud computing services square measure unbroken within the clouds.
Keeping knowledge within the clouds, users may lose control of their data and rely on cloud operators to enforce access control.

3.4 Data Location

Cloud users don't seem to be alert to the precise location of the knowledge center and additionally they don't have any management over the physical access thereto data.
Most of the cloud providers have datacenters around the world.
In several countries bound styles of knowledge cannot leave the country thanks to doubtless sensitive info.

Next within the quality chain there are a unit distributed systems during which there are a unit multiple databases and multiple applications.

Based on the study, we tend to found that there are a unit several problems in cloud computing however security is that the major issue that is related to cloud computing.
Top seven security problems in cloud computing surroundings as discovered by "Cloud Security Alliance" CSA are:
• Misuse and reprehensible use of Cloud Computing.
• Insecure API.
• Wicked Insiders.
• Shared Technology issues / multi-tenancy nature.
• Data Crash.
• Account, Service & Traffic Hijacking.
• Unidentified risk report.

3.5 Misuse and reprehensible Use of Cloud Computing
Hackers, spammers and different criminals cash in of the appropriate registration, simple
Procedures and relatively unspecified access to cloud services to launch varied attacks like key cracking, Arcanum etc.

3.6 Insecure Application Programming Interfaces (API)
Customers handle and move with cloud services through API's.
Providers should make sure that security is integrated into their service models, while users must be aware of security risks.

3.7 Wicked Insiders
Malicious insiders produce a large threat in cloud computing surroundings, since consumers do not have a clear sight of provider policies and procedures.
Malicious insiders will gain unauthorized access into organization and their assets.

3.8 Shared Technology issues/multi-tenancy nature
this is essentially supported shared infrastructure, which is not designed to accommodate a multi-tenant architecture.

3.9 Data Crash
Comprised data may include deleted or altered data without making a backup, unlinking a record from a huge environment, loss of an encoding key and illegal access of sensitive data.

3.10 Account, Service & Traffic Hijacking
Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities.
Attackers will access essential areas of cloud computing services like confidentiality, integrity and availability of services.

3.11 Unidentified Risk Report
Cloud services implies that organizations square measure less involved software system and hardware, so organizations should not be aware with these issues such as internal security, security compliance, auditing and logging
may be overlooked.

IV. RESEARCH CHALLENGES[2]

Cloud computing analysis addresses the challenges of meeting the necessities of next generation personal, public and hybrid cloud computing architectures and also the challenges of allowing applications and development platforms
to take advantage of the advantages of cloud computing.
Many existing problems haven't been absolutely self-addressed, while new challenges keep emerging from industry applications.

Some of the difficult analysis problems in cloud computing square measure given below.
• Service Level Agreements (SLA's)
• Cloud Data Management & Security
• Interoperability
• Multi-tenancy
• Server Consolidation
• Common Cloud Standards
• Platform Management

4.1 Service Level Agreements (SLA's) [2]
Cloud is administrated by service level agreements that permit many instances of 1 application to be duplicated on multiple servers if would like arises; passionate about a priority theme, the cloud may minimize or finish off a lower level application.
A big challenge for the cloud customers is to gauge SLA's of cloud vendors.
Most of the cloud vendors produce SLA's to form a defensive defend against action at law whereas giving assurances to customers.

So there square measure some problems like information protection, outages and value structures that has got to be taken into account by the shoppers before language a contract with the seller.
And is also there any SLA related to backup, archive, or preservation of data?
So it's a crucial analysis space in cloud computing.

4.2 Cloud Data Management[2]
Cloud knowledge is vast, unstructured and typically append only with rare updates.

As service vendors don't have access to the physical security system of information centers, they need to think about the infrastructure supplier to attain full information security.
In a virtualized atmosphere just like the clouds, VMs will dynamically migrate from one location to another; therefore directly victimization remote attestation isn't spare.
In such case, it's vital to make trust mechanisms at each subject field layer of the cloud.
Software frameworks like Map Reduce and its numerous implementations like Hadoop is a unit designed for distributed process of knowledge intensive tasks, these frameworks typically operate on Internet scale file system.

4.3 Interoperability
It is the power of a computing system to run application programs from totally different vendors and to act with different computers across local are a network or WAN freelance of their physical design
and operating systems.
Many public cloud networks square measure organized as closed systems and don't seem to be designed to act with one another.
To overcome this challenge, business standards should be developed to assist cloud service suppliers style practical platforms and alter information movableness.
Organizations need to automatically provision services, manage VM instances, and work with both cloud-based and enterprise-based applications using a single tool set that can function across existing programs and multiple cloud providers.

4.4 MULTI-TENANCY[5]
Multi-tenancy is a major concern in cloud computing.
Multi-tenancy happens once multiple customers uses identical cloud, same package, on identical hardware, with identical knowledge-storage system to share the knowledge and data or runs on a single server.

There square measure multiple kinds of cloud applications that users will access through the web, from tiny net based mostly} widgets to massive enterprise software system applications that have inflated security needs based on the kind of information being keep on the software system vendor's infrastructure.

These application requests need multi-tenancy for several reasons, the foremost vital is price.

Multiple customers accessing a similar hardware, application servers, and databases may affect response times and performance for other customers.
For application-layer multi-tenancy specifically, resources square measure shared at every infrastructure layer and have valid security and performance issues.
For example, multiple service requests accessing resources at the same time increase wait times but not necessarily CPU time, or the number of connections to an HTTP server has been exhausted, and also the service should wait till it will use Associate in Nursing obtainable association or in a very worst-case state of affairs drops the service request.

4.4.1 Architecture
This design totally separates your info from different customer's info, while allowing us to roll out rapidly the latest functionality to each, all at once. This approach offers the foremost configurability and permits you to extract deep insight from your info Oracle delivers a modern Multitenant design that enables multitenant instrumentality information to understand various pluggable databases. An existing info will merely be adopted with no application changes necessary.

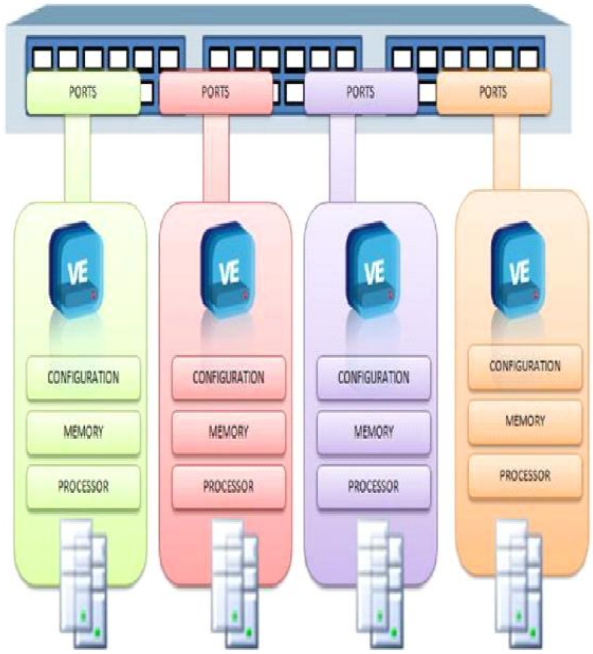

Figure 4

4.4.2 What Multi-Tenancy is Able To Do?
Simplify knowledge Mining: rather than being composed from varied sources, all the data for shoppers is keep in a very single information theme.
Decreases expenditure: Multi-tenancy reduces the overhead by amortizing it over several users, like they can charge for the certified software because everyone

can run it on a single system,
so only single certify will need to purchase. **More elasticity:** It provides the flexibility of importing and exporting your information

V. CONCLUSION AND FUTURE WORK

Cloud computing has monumental prospects, but with equal number of security threats.

One of the most important security worries with the cloud computing model is that the multi-tenancy.

Multi-tenancy is major issue for Cloud Computing Security.
There is a unit many alternative security challenges that embrace security aspects of network and virtualization. The infinite potentialities of cloud computing cannot be unseen just for the protection problems -the endless analysis and analysis for sturdy, regular and integrated security models for cloud computing might be the only path of inspiration.
Based on this proven fact that the impact of security problems in cloud computing may be decreased by multi-tenancy design.
Regardless of the character of security problems, it can be undoubtedly concluded that the deployment of any form of cloud computing should deal with the security concerns corresponding to those of the safety critical systems.
We believe that because of the complexness of the cloud, it will be difficult to achieve end-to-end security. New security techniques got to be developed and older security techniques are a unit required to be radically tweaked to be ready to work with the clouds design.
We hope our work can offer a more robust understanding of the planning challenges of cloud computing, and pave the trail for more analysis during this space.

REFERENCES

[1] Abbadi, I.M. and Martin, A. (2011). "Trust in the Cloud". Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006
[2] Agarwal, A. and Agarwal, A. (2011). "The Security Risks Associated with Cloud Computing". International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.
[3] Arshad, J, Townsend, P. and Xu, J. (2013)."A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems", 29, 416–428. doi:10.1016/j.future.2011.08.009.
[4] Atayero, A.A. and Feyisetan, O. (2011). "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption". Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.
[5] Bisong, A. and Rahman, S.S.M. (2011). "An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications", 3(1), 30-45. doi:10.5121/ijnsa.2011.3103
[6] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems", 25, 599–616.
[7] Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). "The CloudGrid approach: Security analysis and performance evaluation. Future Generation Computer Systems", 29, 387–401. doi:10.1016/j.future.2011.08.008
[8] Celesti, A., Fazio, M., Villari, M. and Puliafito, A. (2012). "Virtual machine provisioning through satellite communications in federated Cloud environments. Future Generation Computer Systems", 28, 85–93. doi:10.1016/j.future.2011.05.021

