IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Security in Cloud Computing: A Survey

Abhishek Gaur[1*], Sohini Bhar[2], Gopal Krishna Shyam [3]

[1,2,3]School of C and IT, REVA University, Bangalore, Karnataka, India

Corresponding Author: abhishekgaur964@gmail.com, Mob.: +91-96637-47325

DOI: https://doi.org/10.26438/ijcse/v7si14.7682 | Available online at: www.ijcseonline.org

***Abstract*—** As per a Forbes' report distributed in 2015, cloud-based security spending is required to increment by 42 percent. As per another examination, the IT security use had expanded to 79.1 percent by 2015, demonstrating an expansion of something beyond than 10 percent every year. Worldwide Data Corporation (IDC) in 2011 demonstrated that 74.6 percent of big business clients positioned security as a noteworthy test. It is a normally acknowledged actuality that since 2008, cloud is a reasonable facilitating stage; be that as it may, the recognition regarding security in the cloud is that it needs critical upgrades to acknowledge higher rates of adaption in the venture scale. As recognized by another examination, a large number of the issues standing up to the distributed computing should be settled direly. The industry has made huge advances in combatting dangers to distributed computing, yet there is something else entirely to be done to accomplish a dimension of development that at present exists with conventional/on-start facilitating. This paper outlines various companion looked into articles on security dangers in cloud figuring and the preventive techniques. The goal of my examination is to comprehend the cloud parts, security issues, and dangers, alongside developing arrangements that may possibly alleviate the vulnerabilities in the cloud.

***Keywords*—**Security Issues, Distributed Computing

I. Introduction

Cloud Computing figuring is progressively being adjusted by an extensive variety of clients beginning from business substances to shoppers. A study by Right Scale1 found that a normal client keeps running somewhere around four cloud-based applications furthermore, anytime is assessing another four. The study likewise discovered that 41 percent of business substances run critical remaining task at hand on open mists. With such an extensive amount our remaining task at hand moving to cloud, security in cloud figuring is under expanded investigation. [2]

This evaluation is likewise bolstered by the 2017 report by Forbes, which says that in 15 months, while 80 percent of all IT spending plans will be resolved to cloud arrangement, 49 percent of the organizations are postponing cloud arrangement because of security abilities hole and concerns. The issue has all the earmarks of being multi-dimensional, with absence of gifted assets, absence of development, clashing accepted procedures, and complex business structures to give some examples.[2]

Adaption of cloud has achieved a tipping point and it is normal that more remaining tasks at hand will move from customary neighborhood stockpiling to cloud from normal Internet clients as well as from most if not every single business element. While there are numerous issues that require distinguishing, dissecting, and tending to, this record endeavors to overview the security in distributed computing and reports on different angles of security vulnerabilities and arrangements. [Discussed in section 3][2]

A few inquiries that require critical answers are: (a) Privileged User Access Management, (b) Regulatory Compliance, (c) Data Location, (d) Data Segregation, (e) Data Assurance and Recovery Support, (f) Investigative Support, and (g) Long-term Viability.
It is exceptionally suggested that these inquiries, alongside different dangers, are evaluated and tended to. A portion of the appraisals could be as per the following:
a. Association capacity and development
b. Innovation and information dangers
c. Application relocation and execution chance
d. Individuals dangers
e. Process dangers
f. Strategy dangers
g. Expanded production network dangers

This article merges different works that address the dangers, vulnerabilities, and potential controls in distributed computing. It likewise gives data on driving cloud models and structures. In addition, the article distinguishes potential future research regions identified with security in distributed computing. [Discussed in section 4][2]

II. Related Work

1. <u>General Vulnerabilities, Threats, and Attacks In Cloud</u>:

Distributed computing, as different territories of IT, experiences various security issues, which should be tended to. These dangers relate to approach and association dangers, specialized dangers, and legitimate and different dangers.[7]

A. VULNERABILITIES AND OPEN ISSUES:
Cloud is an arrangement of innovation, process, individuals, and business develop. Like all other innovation, process, individuals, and business develop, cloud too has vulnerabilities. Coming up next are a portion of the vulnerabilities in a cloud. A portion of the open issues and dangers that needs pressing consideration are as per the following:
a. Shared Technology vulnerabilities: expanded use of assets gives the aggressors a solitary purpose of assault, which can cause harm disproportional to its significance. A case of offer innovation is a hyper-visor or cloud coordination.
b. Information Breach: with information insurance moving from cloud purchaser to cloud specialist organization, the danger of unintentional, malignant, and deliberate information break is high.
c. Record of Service activity seizing: one of the greatest favorable circumstances of cloud is access through Internet, however the equivalent is a danger of record trade off. Loosing access to favored record may mean loss of administration.
d. Refusal of Service (DoS): any forswearing of administration assault on the cloud supplier can influence all fundamentals
e. Vindictive Insider: a decided insider can discover more approaches to assault and cover the track in a cloud situation.
f. Web Protocol: numerous vulnerabilities natural in IP, for example, IP parodying, ARP satirizing, DNS Poisoning are genuine dangers.
g. Infusion Vulnerabilities: vulnerabilities, for example, SQL infusion imperfection, OS infusion, and LDAP infusion at the administration layer can cause significant issues over numerous cloud buyers.
h. Programming interface and Browser Vulnerabilities: Any powerlessness in cloud supplier's API or Interface represents a huge hazard, when combined with social designing or program based assaults; the harm can be huge.
i. Changes to Business Model: distributed computing can be a huge change to a cloud purchaser's plan of action. IT office, and business needs to adjust or confront presentation to chance.
j. Damaging use: certain highlights of distributed computing can be utilized for noxious assault purposes, for example, the utilization of trail time of utilization to dispatch zombie or DDoS assaults.
k. Noxious Insider: a pernicious insider is dependably a noteworthy hazard, notwithstanding, a malevolent insider at the cloud supplier can make critical harm numerous shoppers.
l. Accessibility: the likelihood that a framework will function as required and when required.[7]

B. ASSAULT VECTORS: As indicated by an ongoing exploration, the three noteworthy vectors of assault are arrange, hyper-visor, and equipment. These vectors are mapped to assaults, for example, outer, interior, and cloud supplier or insider assault separately.[7]

2. Need for Security and Privacy in Cloud Computing:
Distributed computing is a merger of a few realized innovations including framework and disseminated processing, using the Internet as an administration conveyance organize. The general population Cloud condition is greatly intricate when contrasted with a customary server farm condition. [3]

Under the worldview of Cloud registering, an association surrenders coordinate authority over real parts of security, presenting a significant dimension of trust onto the Cloud supplier. An ongoing review in regards to the utilization of Cloud administrations made by IDC features that the security is the best test for the appropriation of Cloud.

Shared and dispersed assets in the Cloud frameworks make it difficult to build up a security show for guaranteeing the information security and protection. Because of straightforwardness issues, no Cloud supplier enables its clients to execute interruption recognition or security observing frameworks stretching out into the administration administrations layer behind virtualized Cloud occurrences.

Clients may not know about nitty gritty security occurrences, helplessness, or malware reports. For instance, through back channel, assailants might have the capacity to get to the substance of Cloud cases and fix a bit level rootkit. Assaults on "physical dimension, for example, perusing out the irregular access memory of the virtualized has or subverting the virtualization layer are known to the network. [3]

Indeed, even the host framework giving the information can never again be completely trusted since the Cloud supplier possesses the physical assets. Cloud specialist organizations regularly build up a Service Level Agreement (SLA) to feature security and protection of the related administrations. To a degree, there is an absence of a standard strategy to plan a SLA. The creators in introduced SLA identified with gave administrations and the waivers. These waivers don't generally help the clients satisfying their misfortunes.

Cloud suppliers like Amazon, Google, and Sales-force alike depend on point by point SLA’s to ensure security and different parameters to their clients, for instance, Amazon's EC2 gives deliberation of virtual equipment to its clients, covering a wide range of disappointments including administrator hub disappointment and programming hub disappointment. In future, SLA based Google App Engine would prone to deal with all reasons for disappointments.[3]

III. METHODOLOGY

- Vulnerabilities In Internet Protocol:

Vulnerabilities in Internet conventions may turn out to be a verifiable method for assaulting the Cloud framework that incorporate basic kinds of assaults like man-in-the-center assault, IP caricaturing, ARP ridiculing, DNS harming, RIP assaults, and flooding. ARP harming is one of the outstanding vulnerabilities in Internet conventions. Utilizing this defenselessness, noxious VM can divert all the inbound and outbound activity of a co-found VM to the vindictive VM since ARP does not require Proof-of-Origin. [2]

Then again, there are vulnerabilities of the HTTP convention. HTTP is a web application convention that requires the session state. Numerous systems are utilized for session dealing with. Nonetheless, they are defenseless against session-riding and session seizing. These vulnerabilities are positively pertinent to Cloud. TCP/IP has some "unfix-able imperfections, for example, "confided in machine" status of machines that have been in contact with one another, and the implied presumption that directing tables on switches won't be malevolently changed. Such assault situations ends up basic for open Clouds, as the general spine for Cloud arrangement is the Internet. [2]

- Security Issues At Various Layers In Cloud:

In Fig. 1, we investigate each layer of Cloud with related security concerns. Along these lines, I grouped security concerns dependent on various layers of the Cloud foundation viz; application level, organize level, information stockpiling level, virtualization level, verification and access control level, trust level, consistence, review and directions level. Application level dangers straightforwardly influence the security of Cloud applications at the client layer. System level dangers or interruptions influence the general security of Cloud administrations, information and also physical assets. One can without much of a stretch access another client's assets or administrations by checking the system traffic in the Cloud.

Assaults on information stockpiling specifically influence the security of the client's information (very still or in-travel) including application information and delicate information. Virtualization level dangers specifically influence the information stockpiling level security and application level security. Verification and access control level dangers influence the security of authentic client's administrations and assets. Trust level dangers straightforwardly influence the security of information in-travel and relocating applications. Inspecting, consistence, and controls levels dangers straightforwardly influence the client's information protection, secrecy, and uprightness. I will discuss about four major issues which is application, network, data storage and virtualization level security issues.[2]

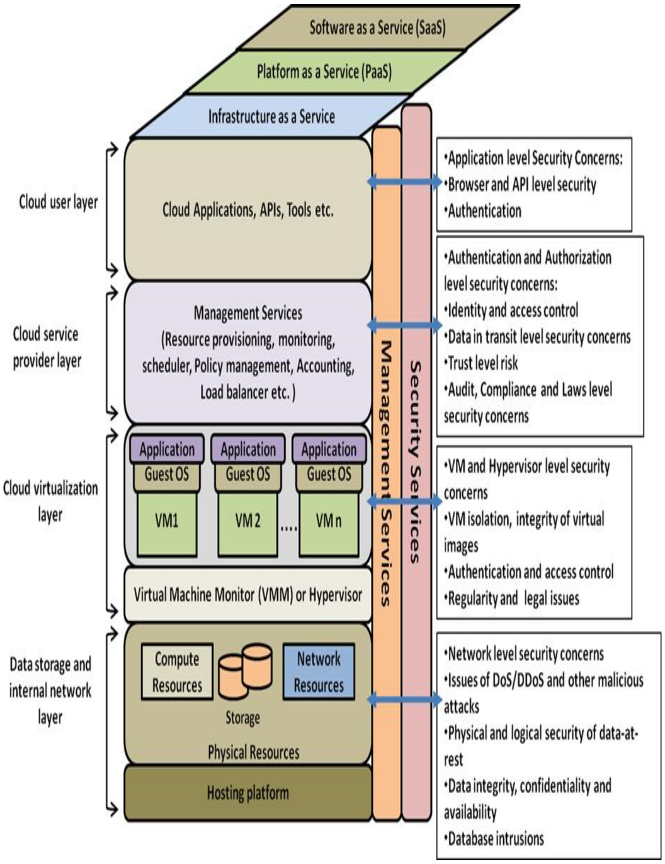
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service
Cloud user layer
Cloud Applications, APIs, Tools etc.
Cloud service provider layer
Management Services (Resource provisioning, monitoring, scheduler, Policy management, Accounting, Load balancer etc.)
Cloud virtualization layer
Application
Guest OS
VM1
Application
Guest OS
VM 2
....
Application
Guest OS
VM n
Virtual Machine Monitor (VMM) or Hypervisor
Data storage and internal network layer
Compute Resources
Storage
Network Resources
Physical Resources
Hosting platform
Management Services
Security Services
•Application level Security Concerns:
•Browser and API level security
•Authentication
•Authentication and Authorization level security concerns:
•Identity and access control
•Data in transit level security concerns
•Trust level risk
•Audit, Compliance and Laws level security concerns
•VM and Hypervisor level security concerns
•VM isolation, integrity of virtual images
•Authentication and access control
•Regularity and legal issues
•Network level security concerns
•Issues of DoS/DDoS and other malicious attacks
•Physical and logical security of data-at-rest
•Data integrity, confidentiality and availability
•Database intrusions

Figure 1: A detailed architecture of Cloud with security concerns at each layer [7]

- Application Level Security Issues:

Application level security alludes to the use of programming and equipment assets for giving security to applications with the end goal that the assailants are not ready to gain power over applications and roll out alluring improvements to their configuration. Since Web applications and SaaS are firmly combined with giving Cloud benefits, the security and accessibility of general cloud administrations are reliant upon the security of Web programs, API's and powerlessness free applications. A Web program is the stage autonomous customer program that is for the most part used to get to the Cloud administrations (SaaS), web applications, site pages, or web 2.0. It utilizes SSL/TLS conventions for secure transmission and validation of information. In this way, assaults on program based Cloud validation straightforwardly influence the security of Cloud applications. [2]

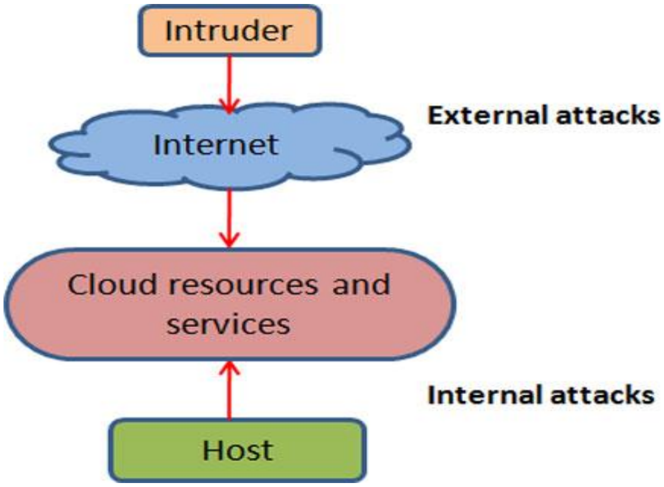

Figure 2: A detailed architecture of Cloud with security concerns at each layer [2]

- Network Level Security Issues:

The system is the foundation of Cloud, and henceforth vulnerabilities in system specifically influence the security of Cloud. As appeared in Fig. 2, security issues at system level ought to be considered regarding both outer and inside systems. A foe outside the Cloud organize frequently performs DoS or DDoS assaults to influence the accessibility of Cloud administrations and assets. DoS/DDoS assaults lessen the transfer speed furthermore, builds the clog making poor administration the clients. Due to the conveyed nature of the Cloud, it is difficult to avoid DoS/DDoS and Economic Denial of Sustainability (EDoS can be called as HTTP and XML based DDoS) assaults.[2]

- Data Storage Level Security Issues:

The accompanying parts of information security are as yet open difficulties: information in-travel, information very still, information genealogy, information remanence, information provenance, information recuperation, information area, information ruptures, and analytical help. [2]

If there should arise an occurrence of **information in-travel**, foe in system influences the privacy and honesty of information. The greatest dangers for information in-travel incorporate poor encryption innovation and system conventions. Basically going for an encryption innovation does not fill the need.

Information very still (put away in Cloud stockpiling) needs physical, consistent, and work force get to control approaches. A few models identified with Cloud disappointments on information security are: Data focus of Hosting.com at New Jersey went down for couple of hours because of programming bug in a Cisco switch.

Following the information way is known as **information genealogy** and it is vital for examining purposes in the cloud. It is a testing assignment to give information ancestry. Since the information stream is never again straight in a virtualized situation inside the Cloud, it confuses the way toward mapping the information stream to guarantee respectability of the information.

Information Remanence alludes to the information forgot in the event of information exchange or information evacuation. It causes insignificant security dangers viz; exposure of delicate data, information sold to other people, and so on.

Information recuperation is a standout amongst the most difficult issues. Information can be lost due to unintentional harm or catastrophic event to capacity. It represents a hazard to information accessibility for clients.

Information area is Tracing area of information is troublesome in the Cloud since client's information are powerfully moved from one district (or nation) to another locale (or nation). It expands danger of information protection and security since information proprietor loses the authority over his/her information.

Information breaks and insightful help: It is hard to examine improper or on the other hand unlawful action, since logging and information for numerous clients are co-found and may likewise be spread over a consistently changing arrangement of hosts and server farms. [2]

- Virtualization Level Security Issues:

In the virtualized (multi-inhabitant) condition, various OS's run simultaneously on a have PC utilizing hypervisor. Existing vulnerabilities in a VM that are circulated all through the physical and virtual undertaking assets permit digital aggressor, malware, or different dangers to remotely misuse. VM's collocation likewise expands the security chance.

As the quantity of visitor working frameworks (OS's) running on a hypervisor increment, the security worries with that more current visitor OS's likewise increment. Since it is absurd to expect to monitor all visitor OS's, and subsequently keeping up the security of those OS's is troublesome. It might happen that a visitor framework attempts to run a malignant code on the host framework and cut the framework down or take full control of the framework and square access to other visitor OS's. There are dangers related with having the equivalent physical foundation between a lot of different clients, even one being pernicious can cause dangers to the others utilizing a similar framework.[2]

IV. Results and Discussion

- Results - As Research Based on the Cloud Deployment Models :

The two most essential perspectives that decide the dimension of helplessness in a distributed computing stage is the decision of arrangement and conveyance show. The accompanying sub-segments quickly talk about every one of these models and their security suggestions:

A. Private Cloud:

Description: In a private cloud, the cloud specialist co-op pools together versatile assets and virtual applications and makes them accessible to the cloud purchasers. In this arrangement show, the assets are devoted to a solitary or a lot of associations and treated as an intranet usefulness. The charging more often than not is on a membership premise with a cloud purchaser making least responsibilities.

Implications: Positive security suggestions are moderately high and the association has critical impact on the engineering, procedures, and apparatuses utilized in the sending.

Challenges: Security challenges incorporate surprising expense of usage and the board, aptitudes necessity, and weakness the executives. In this sending model, cost and rate of profitability are key components and the security execution is normally founded on hazard evaluation and henceforth, the security cover isn't extensive.

Parameters To Be Involved In The Security Of Private Cloud:

1. End-To-End Encryption: Gives encryption in-travel, being used, and very still. The cloud server essentially does not approach decoded information so data is ensured notwithstanding when the cloud is ruptured. Most vital of all, PreVeil Email is intended to be anything but difficult to utilize.
2. Scanning of Malicious Activities: Identification of the source of the malicious insider threat.
3. Validation Of Cloud Consumer: The ability gave to the consumer is to arrangement handling, stockpiling, systems, and other key figuring assets where the buyer can send and run subjective programming, which can incorporate working frameworks and applications.
4. Secure Interface and API's: Give back-end engineering to building escalated and highlight rich applications.
5. Insider Attacks: Data security assumes an essential job in distributed computing. Touchy data ought to be kept in secure mode for giving trustworthiness and secrecy from insiders and pariahs.
6. Secure Leveraged Resources: Private distributed storage will almost certain use and be based upon customary information stockpiling and IT foundation.
7. Business Continuity Plans: You could run your test and advancement conditions on the cloud framework in the optional site, and once an occasion triggers the need to move your generation outstanding task at hand, you would down-organize your test and improvement situations and dispense the assets to your creation condition. This option requires the replication of your information from the essential site to the auxiliary site, yet since you control the two endpoints in this situation you are less compelled in your decision of innovation. Visit fail-over testing ought to be performed so as to confirm that the arrangement is operational.
8.

B. Public Cloud:

Description: In an open cloud, assets are powerfully dedicated on a fine-grained, self-benefit premise over the Internet or an entry. Charging is typically utilization put together and is accused of respect to a compensation for every utilization premise.

Implications: Positive security suggestions are that because of countless customers and volumes of exchanges included. The cloud specialist organization ordinarily has a far reaching and layered security framework, which can possibly give a high level of security because of its actualize once and utilize on numerous occasions show, which fundamentally lessens the expense of security execution for the buyer.

Challenges: Security challenges are increased, as the assets are not dedicated but rather utilized over numerous cloud consumers. This not just includes extra weight of guaranteeing all applications and information got to on general society cloud, yet in addition needs to deal with the huge number of outside impacts, for example, authoritative, information insurance and so forth.

Parameters To Be Involved In The Security Of Public Clouds:

1. End-To-End Encryption: By and by, sender and collector for the most part fall back on an open key foundation. This implies the recipient makes an open key. With this open key, it is just conceivable to encode, not to decode. The sender may now scramble the message with this open key and send the encoded message to the collector. The beneficiary is the just a single possessing the private key vital for unscrambling the message.
2. Scanning Of Malicious Activities: In particular, they begun by inspecting the contrasts among noxious and authentic distributed storage vaults from a topological perspective.
3. Validation Of Cloud Consumers: The cloud foundation is made accessible to the overall population or an extensive industry gathering and is possessed by an association moving cloud administrations.
4. Secure Interface and API's: The utilization of the cloud is presently standard and, regardless of a few concerns, it is

commonly acknowledged that general society cloud isn't inalienably unreliable. Indeed, by and large it is more secure than most server farms. This can be clarified when we think about what number of chances there are for a bit of touchy data that has been messaged, saved money on a USB drive, or generally imparted to partners to fall into the wrong hands. Contrast that with a similar data being made, altered and spared in the cloud. Significant suppliers, for example, Amazon Web Services (AWS) and Google absolutely put their best foot forward to give layered security models to epitomized cloud conditions, with the planned result that clients would then be able to profit by these economies of scale at negligible cost.

5. Insider Attacks: An assault from inside your association may appear to be impossible, yet the insider risk exists. Representatives can utilize their approved access to an association's cloud-based administrations to abuse or access data, for example, client accounts, money related structures, and other touchy data.

6. Secure Leveraged Resources: Adaptability to change the framework dependent on consistently changing business and IT needs of the association.

7. Business Continuity Plans: In this situation, you can imitate your information onto the capacity in general society cloud utilizing one of numerous fit innovations, and just start up the required servers in case of a fiasco. It is imperative to remember the difficulties identified with information replication and the system prerequisites.

C. Hybrid Cloud:

Description: Hybrid cloud is a sending model where a private cloud is connected to at least one outer cloud administrations while being overseen midway. It gives the cloud consumers an adaptable and fit-for-reason arrangement without hardly lifting a finger of tasks. The hybrid mists have a higher level of multifaceted nature as far as charging and advertisements.

Implications: Positive security suggestions are that security can be reason worked for vulnerabilities, dangers, and dangers that are surveyed. This makes it savvy and focused on.

Challenges: Security challenges are moderately high as the organization show is intricate with heterogeneous condition, numerous arrangement, and mechanization apparatuses. This will require extra managerial overhead, with any oversight bringing about huge hazard introduction.

Parameters To Be Involved In The Security Of Hybrid Cloud:

1. End-To-End Encryption: Move Huge Amounts Of Data Rapidly and Predictably, Cleanse and Prepare Data, Conduct Reliable Messaging Communications.

2. Scanning Of Malicious Activities: Hybrid Cloud Security mechanizes security inside your DevOps procedures and conveys different XGen™ danger barrier systems for ensuring runtime physical, virtual, and cloud outstanding tasks at hand, compartments, and examining of holder pictures pre-deployment.Move Huge Amounts Of Data Rapidly and Predictably, Cleanse and Prepare Data, Conduct Reliable Messaging Communications.

3. Validation Of Cloud Consumer: To a common pool of configurable figuring assets (e.g., systems, servers, stockpiling, applications, and administrations) that can be quickly provisioned and discharged with negligible administration exertion or specialist organization cooperation.

4. Secure Interface and API's: Another choice is IT as a Service. Pick a seller that offers expedited, multi-merchant administrations to engage clients to obtain the IT administrations they require, each sent on the ideal cloud display.

5. Insider Attacks: Information Outsourcing has developed quickly with the coming of distributed computing wherein outsiders give stockpiling administrations.

6. Secure Leveraged Resources: Hybrid distributed computing empowers an undertaking to send an on-premises private cloud to have touchy or basic outstanding tasks at hand, and utilize an outsider open cloud supplier to have less-basic assets, for example, test and improvement remaining burdens.

7. Business Continuity Plans: The hybrid cloud joins the benefits of a Private and Public Cloud. Associations utilizing a Hybrid Cloud utilize the Private part of the cloud for basic applications and for less basic applications they utilize the Public Cloud.

- Discussions:

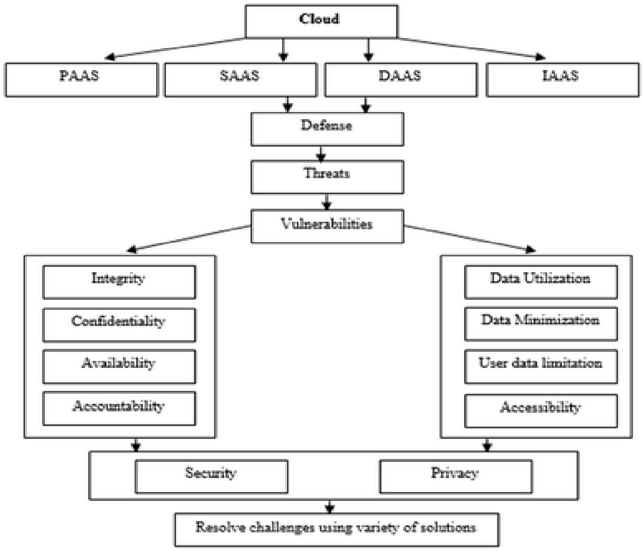

Figure 3: Discussed Security Mechanisms

V. Conclusion

The main conclusions of the study may be presented in a short Conclusion Section. Security in distributed computing is developing in venture with dangers as they are found regularly past the point where it is possible to forestall episodes. Distributed computing because of its troublesome nature, complex design, and utilized assets represent an exceptional and extreme hazard to all performers.

It is basic to all partners and performers to comprehend the hazard and relieve it fittingly. Security should be worked at each layer in a distributed computing stage by consolidating best practices and rising innovations to adequately moderate the hazard.

In addition I want to also conclude with that in the security of the cloud seven factors play's the important role. They are:

1. End-to-End Encryption
2. Scanning Of The Malicious Activities
3. Validation Of Cloud Consumers
4. Secure Interface and API’s
5. Insider Attacks
6. Secure Leveraged Resources
7. Business Continuity Plans

Acknowledgment

This research was partially supported by International Journal of Computer Sciences and Engineering. We thank our colleagues from REVA University who provided insight and expertise that greatly assisted the research.

We would also like to show our gratitude to the Gopal Krishna Shayam, Associate Professor, REVA University for sharing their pearls of wisdom with us during the course of this research, and we thank “anonymous” reviewers for their so-called insights.

References

[1] Qi Jiang, Jianfeng Ma, Fushan Wei, “*On the Security of a Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services*”, 2018,

[2] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, “*A Comprehensive Survey on Security in Cloud Computing*”, 2017.

[3] State of the Cloud Report, 2017.

[4] State of Cloud Adoption And Security, 2017.

[5] Coppolino L, D’Antonio S, Mazzeo G, Romano L, “*Cloud security: Emerging threats and current solutions Computers and Electrical Engineering*”, 2016.

[6] Sharma. R. and Trivedi. R. K, “*Literature review: Cloud Computing –Security Issues, Solution and Technologies*”, International Journal of Engineering Research, Vol. 3, Issue 4, pp. 221-225, 2014.

[7] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, “*A survey on security issues and solutions at different layers of Cloud computing*”, 2012**.**

[8] Amlan Jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim, Hoon Jae-Lee, “*A Strong User Authentication Framework for Cloud Computing*”, 2011.

[9] S. Subashini N, V.Kavitha, “*A survey on security issues in service delivery models of cloud computing*”, 2010.

[10] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono., “*On Technical Security Issues in Cloud Computing*”, 2009.