International Journal of Research in Advent Technology, Special Issue, NCRCEST 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Survey On Security Issues In Cloud Computing

[1]Dr. R. Viswanathan, [2]Dr.R.Anandan, [3]Dr.K.M. Baalamurugan, [4]T.Edison.
[1,3,4]Professor at computer Science of Engineering in Galgotias University,
[2]Professor at Computer Science in Vels University in Chennai,
[1]rvnathan06@gmail.com, [2]anandan.se@velsuniv.ac.in, [3]baalamurugankm11@gmail.com, [4]edison.gis@gmail.com

Abstract: Cloud computing is prototypical which uses consolidate the concept of "software-as-a-service" and "utility computing" afford convenient and on-demand services to requested end users.Many Organizations, such as bank, healthcare and training institutions are moving towards the cloud due to the competence of services delivered by the pay-per-use pattern.Even though the potential gains attained from the cloud computing, the organizations are slow in accepting it due to security issues and dares associated with it. Security is one of the main issueswhich fetter the growth of cloud. Security in Cloud computing is a vital and critical aspect, and has various issues and problem linked to it. Cloud service providers and the cloud service, customers should make guarantees that the cloud is safe, sufficient from all the external threats so that the customer does not face any difficulties such as loss of data or data theft. There is also a probability where a malicious user can pierce the cloud by imitating a legitimate user, thus contaminating the entire cloud and disturbs many customers who are participating the infected cloud. This Survey paper aims to elaborate and analyze the numerous security issues and threatens of cloud computing.

Keywords: Cloud Service provider(CSP), Security issues, Cloud Computing, Cloud Security issues, Data Issues.

1. INTRODUCTION:

Cloud computing is typical for availability and on-request network access to a common pool of configurable processing resources that can be quickly provisioned and released with nominal management efforts [1-2]. In simple words, Cloud Computing is the blend of a technology, platform that affords hosting and storage service on the Web. Leading goal of the cloud computing is to afford scalable and reasonable on-request computing frameworks with good quality of service levels. Numerous companies developing and proposing cloud computing items and services, but have not accurately considered the implications of processing, storing and retrieving data in a pooled and Virtualized environment. In fact, many inventors of cloud-based applications fight to include security. In different cases, developers basically cannot provide genuine security with currently affordable technological competences. Cloud computing is the distribution of resources on a longer scale which is cost effective and locality independent. Resources on the cloud can be used by the client and arranged with the merchant such as amazon, google, Ibm,Salesforce, Zoho, Rackspace, Microsoft [3]. It also shares necessary software's and on-demand tools for various IT Industries. Cloud is used for Cosmopolitan companies, but it's also being used by Small and medium enterprises.

The Cloud Computing includes numerous cloud segments collaborating with one another about the different data they are hanging on as well, that helping the client to get to the required data at a quicker rate.

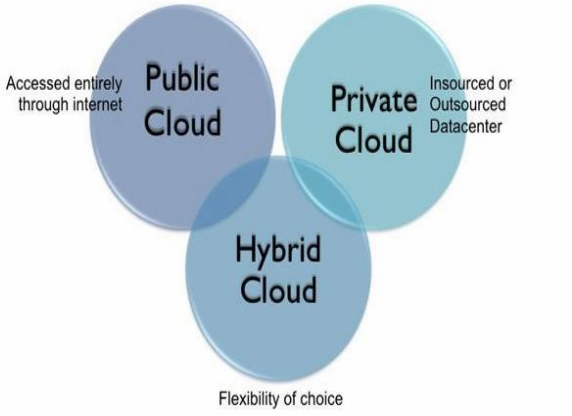

Figure 1 Types of Cloud Computing

With regards to cloud it is more engaged upon the front end and the back end. The front end is the Customer who needs the data, though the back end, is the several data storage gadget, a server which creates the Cloud. There are three sorts of cloud, as indicated by their user. They are private, public and hybrid cloud. The private cloud is possessed by a solitary association and open mists are shared on a bigger scale. Private cloud gives better control and greater adaptability. Hybrid cloud is a mix of Private cloud and Public Cloud which is utilized by the greater part of the industry. The Cloud got numerous issues with regard to security, particularly on Data robbery, Data misfortune and Privacy.

2. LITERATUREREVIEW:

Varsha (2015), discussed that Cloud computing was a huge prospect for both the attackers and the businesses – both parties are capable to possess their own

recompense from cloud computing. An infinite possibility of cloud computing cannot be unseen only for the security issues reason – the unending analysis and research for robust, regular and integrated security models for cloud computing might be the only path of inspiration [8].

Sugata Sanyal, Nabendu Chaki, et.al., (2014), surveyed to maintain [2] the Cloud protected, security threats must be controlled. Besides, data existing in the cloud are as well facing a number of dangers and different issues like privacy and reliability of data ought to be considered when buying storage administrations from a cloud service supporter. Moreover, analyze the cloud administration providers make sure that all the SLA's are met and minimizing the errors made by humans, enabling smooth execution.

Mohammad Ashraf and Hossain, (2014), analyzed the Security issues of Cloud Computing, technical and epistemological components are equally significant to take into consideration. Service oriented framework and other distinctiveness of cloud computing recommends that the cloud computing concept would need to examine the practicality in procession with business, social, legal as well as technical perspectives [5].

RajarshiRoy Chowdhury, (2014), discussed about the alleviation of risks and problems is the significant part and described the probable way to lessen risks such as: to implement proper access control, monitoring, auditing and some standard data security mechanism. Finally, provide some recommendations based on literature review on a number of papers in recent years. Cloud technology is still now in cloud for users [9].

R. H. Goudar, Santosh Kumar, (2012), discussed the architecture and popular platforms of cloud computing. It also addressed challenges and issues of cloud computing in detail [4]. Regardless of the several restrictions and the need for improved methodology forms, cloud computing is fetching a hugely striking paradigm, especially for large enterprises. Cloud Computing activities could affect the undertakings within a few years as it has the prospective to significantly modify IT.

Mohsin Nazir (2012), discussed that, There are so many new technologies emerging at an express rate, each with technical advancements and through the prospective of making human's lives easier. Cloud service providers need to inform their customers about the level of security that they provide on their cloud. It also presented an overview of the structural blocks of Cloud Computing which includes different models of cloud computing, overview of the Cloud Computing architecture and Cloud Computing entities [7].

S. Shanmugapriya, Arokia Paul Rajan (2012), proposed that the Cloud can be communicated to a lot of things, but without the basic storage pieces, which is contributed as a service called as Cloud Storage, no other applications are viable. Cloud Storage, which covers the important techniques in cloud computing, various types of cloud services, management behaviors about cloud computing, the advantages and disputes of cloud storage, motivating services of cloud storage and cloud computing [10].

Rituparna Chaki, RohitBhadauria, et al., (2011) analyzed the data existing in the cloud is liable to a number of dangers and various problems like privacy and reliability of data can be considered when buying storage administrations from a cloud service administrator. Various security matters for Cloud computing situation from numerous perspective and the clarifications to prevent them has been listed classified and compared.

B.S Choudary, F. A. Alvi1, et al., (2011), reviewed that the Cloud computing bears the probability for cost savings, efficiency and improved presentation to the organizations, governments, private and individual users [3]. It also offers an exclusive opportunity for developing countries to get closer to developing countries. Moreover, it addresses the issues that arise during the deployment of cloud services. After identifying the problems some steps are explained to mitigate these challenges and solutions to solve the problems.

3. SECURITY ISSUES FACED BY CLOUD COMPUTING:

Every time, the discussion about cloud security is occurring there will be more to do for it. The cloud service provider (CSP) for cloud ensures the user does not have pressure on any issue, for instance, loss of data or data burglary. There is a chance where a malicious user can breach the cloud by replicating as genuine user, in this way spoiling the whole cloud. This stimulates the influence of several clients those are sharing the cloud, get spoiled [6].There are four kinds of issues raise while talking about the security of a cloud are Security Issues, Data Issues, Infected Application, and Secracy Issues.

Figure 3.1: Cloud Security Issues

Data Issues:

Sensitive information in a cloud computing atmosphere develops as significant issues as to security in a cloud based framework. Primarily, an information is on a cloud, anybody from anyplace whenever can get to information from the cloud since information might be sensitive, common and private information in a cloud. So in the meantime, many cloud computing service consumer and benefactor accesses and alter data. Accordingly, there is a need of a few information, honesty technique in distributed computing. Also, information taking is a one of significant issue in a distributed computing condition.

Many CSP do not deliver their own server as an alternative they acquire server from additional service providers due to the cost affecting and flexible in the process and the cloud provider. So there is an abundant possibility of data can be pinched from the exterior server. Thirdly, Data loss is a mutual challenging in cloud computing. If the cloud computing service provider's seal down his services owing some monetary or legal problem, then there will be a trouble for the user. Moreover, data can be lost or harm or corrupted due to miss happening, natural ruin, and fire. Due to the above situation, data may not be accessible to others. Fourthly, data locality is one of the problems, what requires focus in a cloud computing atmosphere. Physical area of data storage is very essential. It ought be straightforward to user and customer. The Seller does not disclose where all the information is stored.

Secrecy Issues:

The CSP must make sure that the client private information is well safe from other sources and clients. Further, most of the servers are exterior, the CSP should make sure who is retrieving the information and who is sustaining the server so that it allow the provider to defend the customer's private information.

Infected Application:

CSP ought to have the total access to the server with all rights to monitor and maintenance of the server. So this will restrict any malicious customer from sending any spoiled application into the cloud and that will harshly influence the Cloud computing services and the client.

Security Issues:

Cloud computing security should be completed on two levels. One is on supplier level and another is on client level. The cloud computing service provider must assure that the server is all around secured from all the outside dangers it might go over. In spite of the fact that the service provider has given a decent security layer to the client and user, the client should ensure that there ought not be any loss of information or taking or altering of information for different clients who are utilizing a similar cloud owing of its activity. A cloud is just great when there is a decent security given by the specialist organization to the client.

4. ISSUES IN ORGANIZATIONS:

Cloud computing by all accounts looks to be the future of IT. Cloud-based arrangements and methodologies offer numerous advantages to customers and endeavors alike; these incorporate greater flexibility, diminished costs, expanded reliability and environmental advantages. Additional data and applications are moving towards the cloud, which makes remarkable data security challenges. Here are the Issues that associations confront when utilizing cloud administrations.

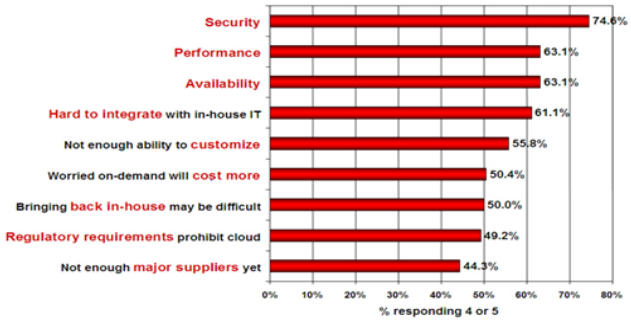

Figure 4.1: Cloud Security survey of an organization

Cloud computing is a developing technology with shared assets, lower cost and depend upon pay per usage as per the demand of the client. Due to many characteristics, it has an effect on Industry budget and also impact on security, privacy and security issues. In this section all these issues are discussed. All those CSPs (Cloud Service provider) who wish to enjoy this new trend should take care of these problems. A CSP should provide their full concentration to the security features of cloud since it is a common pool of assets. Customer not know where the data are stored, who manage data and other vulnerabilities that can occur. Some issues faced by CSP while applying cloud services are as follows:

1. Data Breaches: A data breach may be the essential goal of a focused on the assault or basically the result of human mistake, application vulnerabilities, or poor security methods. It may include any sort of data that was not expected to open discharge, including individual data about the health, budgetary data, by and by identifiable data, exchange privileged insights, and intellectual property. An association's cloud-based information may have an incentive to various gatherings for various reasons. The danger of data breach isn't exceptional to cloud computing, however, it reliably positions as a top concern for cloud clients.

2. Insufficient Identity, Credential, And Access Management: Awful on-screen characters covered up as a certifiable client, administrators, or engineers can read, change, and erase data; issue control plane and administration capacities; sneak on information in transit or

discharge malignant programming which seems to originate from a genuine source.

3. Insecure Interfaces And Application Programming Interfaces (Apis): API security is a top most threat to the cloud environments. Cloud suppliers render a set of APIs that clients use to administer and intermingle with the cloud services. Management, Provisioning and monitoring are all executed, and then the security and accessibility of common cloud services rely on the security of the APIs.

4. System Vulnerabilities: System vulnerabilities are the credulous bugs in the programs that the attackers can utilize to penetrate a system to filch data, by taking control of the system operations.

5. Account Hijacks:If attackers access to a user's identification, they can spy on activities as well as transactions, influence data, return falsified data and redirect customers to illegitimate sites. With stolen identifications, the attackers may have the right to use critical parts of cloud computing administrations, allowing them to conciliate the integrity, availability and confidentiality of those services.

6. Malicious Insiders: A framework manager can get to conceivably delicate data, and can have expanding levels of access to the most basic frameworks and in the long run to the data. Systems that depend entirely on cloud service organizations for security are at more serious hazard.

7. Advanced Persistent Threats (Apts): It is a delayed and targeted cyber assault in which an interloper accesses a system and stays undetected for a broadened time frame, from which they take data.

8. Data Loss: Data stored in a cloud could be vanished for many reasons other than cruel attacks.An accidental removal by the cloud service provider, or a physical disaster, for example, a fire accident or an earthquake, may lead to the everlasting loss of a customer.

9. Insufficient Due Diligence*:* At the point when officials make business procedures, service providers and cloud technologies must be acknowledged. Building up a decent guide and agenda for due industriousness while assessing technologies and suppliers is fundamental for the best shot of progress. Associations that race to embrace cloud innovations and pick suppliers without performing due constancy expose themselves to various dangers.

10. Abuse And Nefarious Use Of Cloud Services: Inadequately secured cloud service organizations, free cloud service preliminaries, and fake account sign-ups by means of payment instrument fraud expose cloud computing models to malicious assaults. Awful performers may use cloud computing assets to target clients, associations, or other cloud suppliers. Precedents of abuse of cloud-based assets incorporate propelling appropriated DOS assaults, email spam, and phishing efforts.

11. Denial Of Service (DOS): DOS attacks are intended to keep clients of an administration from having the capacity to access their information or applications. By compelling the focused cloud administration to consume extreme measures of finite system assets, for example, memory, processor power, disk space, or system data transfer capacity, attackers can cause a system slow down and leave all authentic administration clients without access to administrations.

5. CONCLUSION:

The security issues of cloud computing are not associated with the technical and nonstop security breach only; a lot of social irregularities may be resulted still with no 'hard' security rupture having taken place. These issues are somewhat crucial and sensitive on the basis of technological and sociological viewpoints – the mechanical inconsistency that consequences of security breaches in the cloud computing may lead to important sociological effects. As a consequence, when dealing with these security issues, technical and epistemological aspects are equally essential to take into contemplation. In spite of of the temperament of security issues, it can be certainly concluded that the relentless adverse impacts as a result of security breaches in the cloud computing, the deployment of some form of cloud computing should deal with the security concerns corresponding to those of the safety critical systems. The cloud service provider must press forward practical achievements in security and privacy to users. Our study identifies top security concerns of cloud computing, these concerns are security risks, challenges and security issues of cloud computing and organizations.

REFERENCES:

[1] Sugata Sanyal, Nabendu Chaki, "a survey of security issues in cloud computing", Acta Tehnica Corviniensis – bulletin of engineering tome 2014.

[2] Rituparna Chaki, RohitBhadauria, "A Survey on Security Issues in Cloud Computing", https://www.researchgate.net/publication/, 2011

[3] B.S Choudary, F. A. Alvi1, "A review of cloud computing security issues & challenges", Department of Computer Systems Engineering, QUEST Nawabshah, Sindh, Pakistan, 2011.

[4] R. H. Goudar, Santosh Kumar, "A Survey Cloud Computing –: Research Issues, Challenges, Architecture, Platforms and Applications" and International Journal of Future Computer and Communication, Volume 1, 2012.

[5] Mohammad Ashraf and Hossain, "Cloud Computing And Security Issues In The Cloud", International Journal of Network Security & Its Applications, Volume 6, 2014.

[6] Muhammad Aamir Nadeem, "Cloud Computing: Security Issues and Challenges", Journal of Wireless Communications, 2016.

[7] Mohsin Nazir**, "**Challenges Cloud Computing: Overview & Current Research Challenges", IOSR Journal of Computer Engineering, Volume 8, 2012.

[8] Varsha, "Study of Security Issues in Cloud Computing International Journal of Computer Science and Mobile Computing", Volume 4, 2015.

[9] Rajarshi Roy Chowdhury," Security in Cloud Computing**",** International Journal of Computer Applications (0975 – 8887) Volume 96, 2014.

[10] R. Arokia Paul Rajan, S. Shanmugapriyaa, "Evolution of Cloud Storage as Cloud Computing Infrastructure Service"**,** IOSR Journal of Computer Engineering, Volume 1, 2012.