RESEARCH REVIEW JOURNALS
Volume-04
Issue-05
May-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Proposing Solutions for Security Enhancement for Cloud Computing Environment

[1]Kanika Khanna & [2]Dr. Sachin Gupta

[1]Student, MVN University
[2]Supervisor, MVN University

ARTICLE DETAILS

Article History
Published Online: 25 May 2019

Keywords
Cloud computing security, Technology, Cloud Data etc.

ABSTRACT

The cloud computing environment has achieved widespread grasp in contemporary world. Its plushness is expected dominatingly to consumers' capability to utilize cloud enhancements on demand with compensation as you use protocol, which has approved being ideal. The security risks to the cloud framework delimit the advantages of cloud computing like "on-demand, altered asset accessibility and execution the executives". In an ordinary cloud computing various encouraging parts like hardware, software, firmware, networking, and services coordinate to offer diverse computational offices, while Internet or a private network (or VPN) gives the expected spine to convey the services. It is comprehended that present IT and undertaking security arrangements are not sufficient to address the cloud Cloud has as of late increased huge energy yet at the same time is in its earliest stages. It has the potential for noteworthy cost decrease and the expanded working efficiencies in computing. In spite of the fact that security issues are deferring its quick appropriation, cloud computing is a relentless power and we have to give security components to guarantee its protected selection. In this Article, we will propose a security enhancement solutions framework for cloud computing environment.

1. Introduction

Cloud computing is an innovative mode of computing in which powerfully adaptable and regularly virtualized resources are given as an administration by means of the internet. Cloud computing has as of late increased huge force yet at the same time is in its infancy. It has the potential for noteworthy cost decrease and the expanded working efficiencies in computing. In spite of the fact that security issues are deferring its quick reception, cloud computing is a relentless power and we have to give security systems to guarantee its safe selection. In spite of its clear justifies, albeit, numerous enterprises delay to move from one cloud specialist organization to the next, fundamentally as a result of the issues related to information relocation, information lock-in, and security. Cloud

empowerseveryone to place in numerous ways of using the resources. Notwithstanding, numerous security dangers have been related with classified information being spared in open cloud. With augmentation in business endeavor may develop their own one of a kind private storage cloud framework.

1.1 Cloud Computing

In the past 20 years, the possibility of ITSO has been "a genuinely analyzed field inside IS research". ITSO can be described as "the tremendous duty by outside dealers in the physical and additionally HR related with the entire or specific portions of the IT framework in the customer affiliation". The outsourcing of IT administrations "has turned out to be a standout amongst the most imperative hierarchical ideas in late decades". Notable advantages of information technology benefit provisioning can incorporate cost reserve funds, upper hands, adaptability and so on. The most recent turbulent worldwide financial downturn in conjunction with the quick IT development and the accessibility of modest computational resources is requiring that the IT bureaus of numerous associations consider receiving expense and asset productive technology stages. As opposed to embracing a protective methodology and a securing everything, there is potential for associations, to industrialist on the inventive abilities of developing technology stages keeping in mind the end goal to accomplish an upper hand. A case of a beginning advanced technology is distributed computing. Distributed computing "speaks to an essential change in how IT is provisioned" in that it empowers "computing offices, for example, stockpiling applications,network infrastructure, and figure power, to be conveyed as a metred benefit over the internet, much the same as an utility". Various reviews and reports have featured the developing pattern and prevalence of distributed computing technology. For instance, a report led by Forrester research featured how the worldwide distributed business sector will develop from $58 billion of every 2013 to $191 billion out of2020. At its most primitive, distributed computing is a favorable type of provisioning where equipment and programming computing resources are given by cloud suppliers "as-a-benefit" over a network from substantial scale data focuses. While it has been contended that distributed computing may speak to the followingevolution ofcomputational provisioning, there is proof to propose that the cloud speaks to an essential mechanical outlook change which separates itself from customary IT provisioning through various center attributes (e.g. pay-per-utilize charging models, virtualization, and imaginative plans of action, nuanced security

and protection challenges). As indicated by Schneider and Sunyaev, "distributed computing incites a move in errand obligations amid choice processes and self-benefit obtainment, gives standardized administrations a smaller degree, and empowers new situations of outsourcing and administration game plans, and uses here and now utilization based contracts". In the following segments of this chapter the distributed computing idea is portrayed in more prominent detail as it shapes one of the investigation's focal research areas.

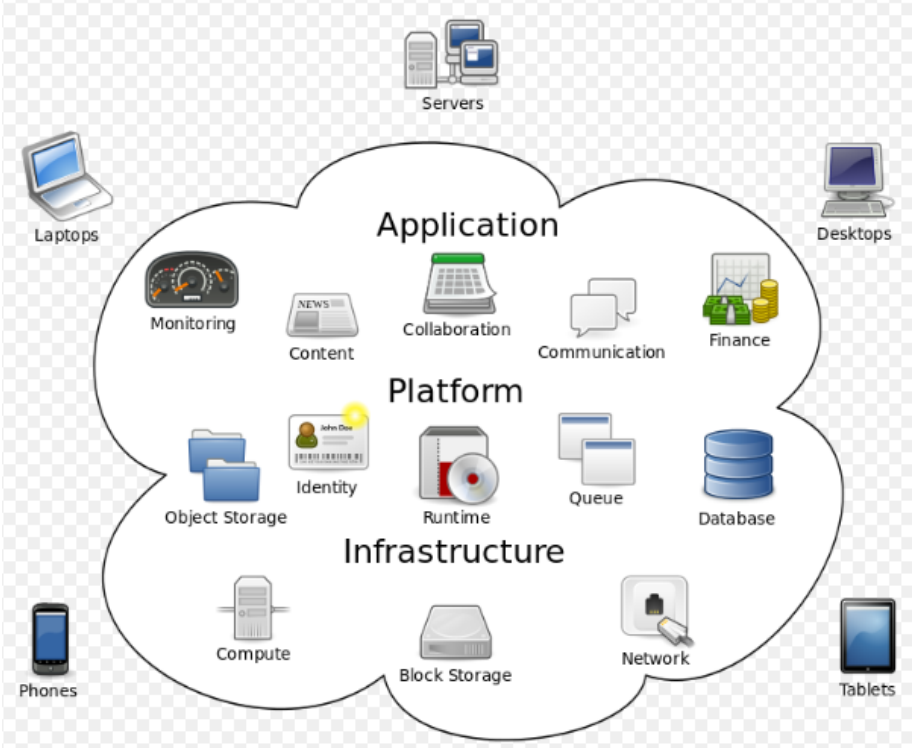


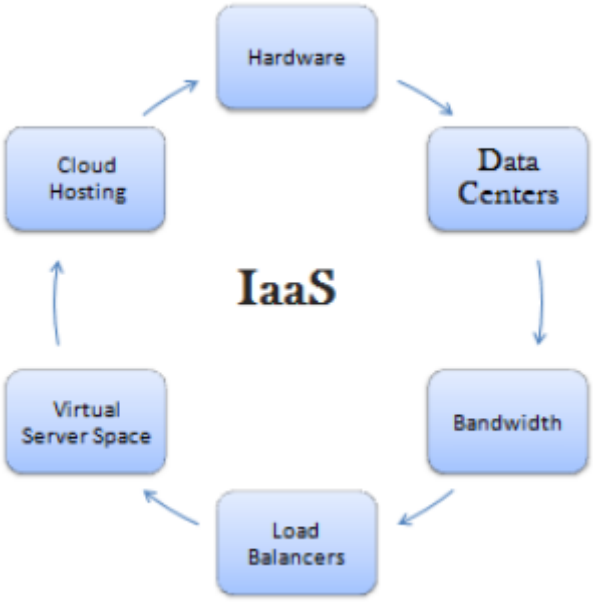
Figure 1: Cloud Computing Framework

1.2 Cloud Computing Framework

Service Models: There are three service models of cloud computing:

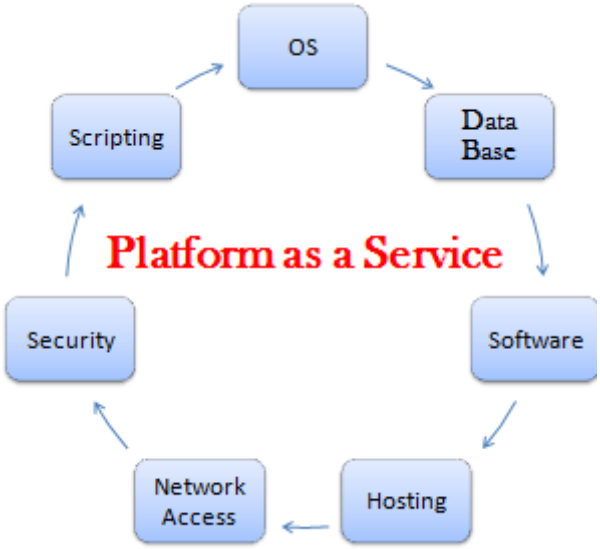
Infrastructure as a Service Infrastructure-as-a-Service (IaaS): Infrastructure as an administration conveys a stage virtualization condition as an administration. Rather than hardware network or space data center, software, buying servers, users can purchase these resources as re-appropriated administration. At the end of the day the customer utilizes the outsider infrastructure services to help its activities including storage, hardware, servers and networking segments

.



Software as a service (SaaS): For this situation the supplier permits the client just to utilize its applications. The software collaborates with the client to utilize its applications. The software collaborates with the client through a UI. These applications can be anything from electronic email to applications like Twitter. The SaaS supplier gives endorsers access to the two resources and applications. SaaS makes it pointless for you to have a physical duplicate of software to introduce on your devices.

Platform as a Service (PaaS): A PaaS supplier gives endorsers access to the parts that they require to create and work applications over the internet. It is a lot of software and advancement apparatuses facilitated on the providers servers. Google applications is one of the most acclaimed Platform as a Service providers. Paas is an application advancement and deployment stage conveyed as an administration to engineers over the Web. Paas services incorporate application design, application advancement, testing, deployment and hosting just as application services, for example, group coordinated effort, web administration reconciliation and database combination, security, adaptability, storage, ingenuity, state the board, application forming.



1.3 Cloud Computing Evolution

The distributed computing idea has risen up out of the evolution of two particular strands as mechanical advancements (e.g. virtualization, data focus computerization and elite networks) and a more articulated accentuation on the administration point of view of IT arrangement (e.g. the specialist co-ops center had moved from the management of IT advantages for guaranteeing that clients infer the most extreme measure of significant worth from utilizing their administrations). The idea of distributed computing is not new and has experienced a metamorphosis in the course of the most recent 50 years. As can be seen distributed computing has its origins going back to the mid 1960's. In 1961, John McCarthy imagined that, calculation may some time or another be composed as an open utility, and the distributed computing worldview might be seen as a major stride toward his dream".

Distributed computing might be seen as the "second happening to distributed computing where more than 50

years prior a comparable change was seen with the appearance of administration agencies and time-sharing systems". Cloud computing has its "origins in the 1990's telecommunication world when suppliers initiated using virtual private network administrations for data communications". The present incarnation of distributed computing initially came to noticeable quality and open consideration in 2007 when IBM and Google declared their accomplices

2. Challenges in cloud computing security

The applications of cloud services are working in the cloud computing infrastructures by utilizing the internet or internal network. The idea of trust in the association can be alluded as the clients guarantee the abilities of the association that it gives the required services dependably and precisely. Trust in cloud computing environment dependent on the chose cloud deployment models in which the applications are designated and re-appropriated to the control of the proprietor. Trust has required a productive and viable security policy in the customary engineering that tended to the utilitarian imperatives and streams between them. Outside systems get to the imperatives that assault the projects which impact the entrance or control on the client data. In cloud deployment models, the network or public clouds doled out control to the association that claimed the cloud infrastructure. At the point when the public cloud-deployed, the control enables the proprietor of the infrastructure to carefully apply sufficient security policy which guarantees the proper security exercises played out that decreases the threats and risks. Fundamentally, the cloud security is related to trust on computing and services utilized by the infrastructure proprietor. The cloud infrastructure in private cloud is overseen and worked inside the premises of private association wherein no extra security challenges presented, so the trust stayed inside the association. It is accepted that transfer of data or any relationship of association or systems to the outside association that opening an approach to increase unapproved access to the information resources.

Cloud computing infrastructure needs the appraisal of risk in zones, for example, integrity, secrecy, privacy, auditing, reliability and accessibility. Basically, the security has significant parts of integrity, privacy and accessibility that are used in designing the satisfactory security system. These real security viewpoints are required to verify the data, hardware and software resources. Cloud computing enables the providers to run, convey and create applications that can be work quickly (execution), versatility, maintainability and reliability with no worries about the areas and properties of the basic infrastructure. The outcomes to benefit these properties of the cloud when we store or transfer private data of various organizations and get services from the cloud specialist co-ops by utilizing the internet that emerges the privacy and security issues. To verify cloud Information Systems (IS) which include to recognizing the challenges and threats that should be tended to utilizing the proper countermeasures execution.

The security challenges of cloud computing infrastructure that can be considered in detail as follows:

2.1 Trusted Third Party (TTP)

Trusted third party in cryptography encourages the cooperation among the two parties and surveys every single urgent activity among them. The cloud computing environment required the TTP services that shows to build up the fundamental trust level and offers a perfect answer for keep up the authenticity, integrity and confidentiality of correspondence and data. TTP can deliver the trusted security area with the explicitly addresses the misfortune or missing of the traditional security limit. It is a fair-minded association which conveys the certainty of business by technical and business security highlights to electronic transactions. TTP services are endorsed and offered alongside the technical yet additionally through the basic, money related and legitimate methods. It is operationally connected with the chain of trust (certificate ways) to give a web believe that building up the idea of Public Key Infrastructure (PKI). PKI offers lawfully satisfactory and technically solid intend to actualize data integrity, data confidentiality, approval, solid verification, and non-repudiation. In a circulated information system, PKI gets profits by coupling through the catalog that is a lot of items having same qualities that are composed in various leveled and legitimate way. Lightweight index get to protocol has turned into the fundamental protocol that supports to get to PKI registry services for the Certificate Revocation List (CRL) and utilized by web services for the confirmation. PKI is combined with index can be used to appropriate: 1) certificate status information (CRL); 2) application certificate, for example, end-client certificate need to acquire utilizing email before the transfer of scrambled message; and 3) private key, If the clients don't utilize comparable machine each day then the convenientce is required in the environment. The index contains the encoded mystery or private key are unscrambled utilizing the password given by client at the remote workstation.

2.2 Confidentiality

Confidentiality alludes to keeping the client's data secret in the cloud computing system and just the approved clients or systems can ready to get to the data. Cloud computing gives (for example applications and its infrastructures) are essentially in the public clouds have more threads on the systems or applications are uncovered as look at the facilitated in the private data centers. Along these lines, it is the central necessity to keep the client data secret ever the expanding number of applications, clients and devices included. The merchants of cloud computing are widely received the two fundamental methodologies, for example, cryptography and physical disconnection to accomplish the confidentiality. The cloud computing gives services and data that are transmitted through the public network and it can't accomplish physical disengagement. While virtual LAN and center boxes network, for example, parcel channels and firewall ought to be deployed to achieve virtual physical detachment. VPN cubed discharged by Cohesive FT to offers a security limit for the IT infrastructure in spite of the fact that it is inside the single, multiple or hybrid cloud data center ecosystems. Vertica offers VPN and firewall to verify its database and sends on the Amazon EC2. At the point when the Amazon EC2 has provisioned the Vertica database and offers clients to full root get to that enables clients to can verify the systems. They make a VPN association among the enterprise clients and Vertica to the

cloud occurrence and firewall is set for the outside world. Confidentiality is additionally upgrading by scrambled the data before transfer into cloud storage and TC3 is effectively utilized in this methodology. Various concerns emerges with respect to the issues of application security and privacy, multitenancy, and data remanence.

2.3 Availability

Accessibility in cloud computing including applications and its infrastructure is to guarantee that the approved clients can get to the property of system at unsurpassed on demand. Cloud computing models (IaaS, PaaS and SaaS) enables its clients to get to the services and applications from wherever whenever. Vendors of cloud computing offers the cloud stage and infrastructure that depends on VM. The Amazon web services offer S3, EC2 that depends on VM called Skytap and Xen gives virtual lab the executives application relies upon the hypervisor (Xen, VMware and Microsoft Hyper-V). For instance, Xen virtual machine offered by Amazon can give isolated storage virtualization, memory virtualization, machine/CPU virtualization and so forth where the enormous number of ware PCs facilitated. This is the reason the specialist co-ops can part resources (memory, limit, storage, CPU cycle) on demand from Amazon dependent on utilization cost as every unit. Right now, the vendors of the cloud are offering stages and infrastructures rely upon the VM (Skytab, Amazon) give the capacity to channel and square the traffic dependent on port and IP address to verify systems yet these services are not equivalent to the network security controls in generally cloud enterprises.

The information system design used to check the identities of numerous systems that offer shared fundamental security prerequisites and decide the specific demands for information security and data assurance. Most cloud vendors (Google, Amazon) give geographic redundancy in their cloud and ideally permitting high accessibility on a single supplier. The cloud system is able to convey activities even in the security ruptures potential outcomes or experts act up. Cloud administration demonstrates a substantial dependence on the network and infrastructure resources accessible whenever.

2.4 Integrity

Data integrity in cloud computing is the protection of data that is put away in cloud server to confirm the data isn't altered or lost by utilizing the services of the third party. Associations can accomplish more certainty to keep system and data integrity from unauthorized access. They give such instruments having more noteworthy perceivability to figure out what or who may adjust the system information or data that possibly influences their integrity. Approval component is used to decide the system what or which level of access to an explicitly approved client ought to need to ensured resources controlled through the system. Approval is basic to guarantee just the legitimate customers can access or communicate with the data because of expanding the quantity of access focuses and customers in cloud computing environment. The auspicious distinguishing proof of any data erasure or debasement by utilizing the data integrity plan and takes fundamental measures for the recuperation of data. The data integrity includes the three primary substances: 1) a cloud storage supplier to whom re-appropriated the data; 2) proprietor of data redistribute his data; and 3) auditor who guarantees the data integrity. The auditor might be the proprietor of data or he can dole out obligation to a third party.

3. Security issues in cloud computing

Cloud security is the arrangement of control-based approaches, consistence and innovations designed to send the insurance of applications, data and infrastructure related with the cloud. Cloud is utilized by more associations and related providers for working data have turned into the need to contract for appropriate security and conceivably helpless regions. Cloud computing security is the real concerns when shared resources, access control, privacy and identity management needs. A portion of the worries are talked about as pursues:

Cloud-based data might be mistakenly altered and defenseless against erase (lost unintentionally) by the specialist organization.

The data store in the cloud can be purposely uncovered by the cloud providers, representatives and its temporary workers.

The resources in the cloud are ordinarily imparted to various inhabitants that might be assaulted.

In the public network, the data might be conceivably accessible through the uncertain APIs and protocols.

In spite of the fact that, the security of data is in-certainty testing when data transfer to the cloud. This segment quickly examines the security concerns as follows:

Cloud Infrastructure Security: Cloud computing empowering the circulated workforce and gives numerous advantages to the customers however it is basic to figure out how to work the cloud infrastructure that guarantees and check the safe deployment of services, storage of data, correspondence and safe activity through organization. With the quick appropriation of cloud services, the worries (privacy, security and reliability) have risen as potential hindrances. Information security experts ordinarily characterize the security rule, principles and routine with regards to cloud infrastructure of the association at the application, host and network levels.

Cloud Storage Security: The prevalence and selection of cloud storage is rising that produce numerous security challenges for the cloud providers just as for the customers. IT specialists to caution that each sort of innovations even virtual or physical, it contains inborn risks when utilizing record sharing applications and cloud storage. Client's store their data in the cloud have never again owns the data since it will transfer through the third party that implies the privacy setting of data is outside the ability to control of service provider or enterprises. Customers need to guarantee the nature of service and security of the data in the cloud. The security worries about storage are data spillage, BYOD (Bring Your Own Data), snooping, cloud credentials and key management.

Cloud Network Security: A cloud service provider has the duty to permit the main legitimate network traffic and square all malignant traffic. Cloud providers are not shared the internal network infrastructure like the access switches and changes utilize to associate cloud VMs to the provider network. The client worried on internal network attacks which incorporate 1) spillage of secret data; 2) unauthorized adjustment; and 3) forswearing of service or accessibility. Network security has worries from both internal and external

attacks in light of the fact that the attacker may legitimately approve from another piece of the network and attack can happen either physical or virtual network.

Data Transfer: Within the enterprise boundaries, data transmission for the most part does not require encryption, or must have a straightforward data encryption measure. For data transmission crosswise over enterprise boundaries, the two data confidentiality and integrity ought to be guaranteed so as to keep data from being tapped and messed with by unauthorized users. At the end of the day, just data encryption isn't sufficient. Data integrity is additionally should have been guaranteed. Along these lines, it ought to guarantee that transport protocols give both confidentiality and integrity.

Software Security: The cloud provider required to shield their applications or software from internal and external string all through from design to generation in all their years cycle. It is imperative to characterize the security procedure and arrangements about the software that empowers the business as opposed to presenting other risk and it stances challenges for the customers and the cloud provider. Software security can be handled or rout by actualizing bugs, design flaws, buffer overflow, error handling agreements.

Data Privacy: Cloud service providers should gather just important information from user and ought to guarantee that the data won't be unveiled to any third party without the user's assent. Along these lines, that the data privacy can be kept up. Private data may now and again be imparted to the outside world to disturb or make issue for the cloud user. Hackers might be the reason for such issue.

Data Loss: Data loss or spillage can have extreme effect on business, brand and notoriety, employee, partner, and client moral and trust. Loss of center protected innovation could have focused and budgetary ramifications moreover. Contingent on the data that is lost or spilled, there may be consistence infringement and lawful repercussions. The data being saved money on the cloud against expenses without a doubt is of significance. The data whenever lost is probably going to cause numerous ramifications, as far as monetary loss, criticize of notoriety, loss of business, legitimate ramifications and so forth. Recovering the data could be a long tedious procedure or it could be conceivable to do as such. Be that as it may, the data can be lost because of breakdown of PC device.

Data Integrity: Clouds require assurance against purposeful disruption or harm of the usefulness of a cloud. Inside a cloud there are partners: an assortment of executives, endorsers and providers. The capacity to parcel access rights to every one of these groups, while keeping malevolent attacks under control, is a key characteristic of keeping up cloud integrity. In a cloud setting, any absence of perceivability into a cloud's systems makes it progressively hard for supporters of check the integrity of cloud-hosted applications. The CSP may have noxious expectation and may not impart the data to the user itself. Accordingly, it might share some portion of data or alter data to make the data pointless. This might be done purposefully or spyware software may play out the action out of sight.

Data Theft: Because of multi-tenancy nature of the cloud it could go about as a 'honey pot' for hackers. On the off chance that hackers could attack the cloud they can access data of the considerable number of organizations hosted on that cloud. Henceforth data can be effectively adjusted or utilized by the hackers. The data whenever stolen from the cloud can be utilized for passionate extortion, monetary transactions or publicized. The data might be deliberately dispersed to undesirable individual or it might be hacked.

4. Solutions for security in cloud computing

4.1 Privacy of Data

As hackers may interfere to access data. It is proposed to have two-tier architecture of data security. Identity and access management is a basic capacity for each association, and a basic desire for customers is that the "standard of least privilege" is allowed to their data. The standard of least privilege expresses that solitary the base access important to play out an activity ought to be without a doubt, and that access ought to be conceded distinctly for the base measure of time fundamental. And this access must be conceded after appropriate verification. Here, another validation model is recommended that utilizations two-tier architecture.

Figure 2: Two Tier Architecture

In this two tier architecture, another authentication PIN is given. After the effective login in the system user is given another validation PIN. And simply after the section of that PIN user is approved to access the data. The PIN can be given to user through two unique mediums:

Mobile Phone/Landline: the protected code can likewise be given to user through SMS or call. The call can be system produced or cloud service provider can enlist a few people to do these sorts of calls.

E-mail: The protected code must be sent to the enlisted email id of the user. This email id is enrolled when the data is put away on the cloud or when user is enlisted on the cloud. It can't be changed when the user is attempting to access data.

4.2 Loss of Data

To stay away from data loss reinforcement component exists with all the cloud service providers. Reflecting of storage devices utilized better transmission media may lessen data loss. Be that as it may, if still the data is lost, it is proposed to have the data protected. Contingent on the size of data and the term the protection might be executed. On data loss the user might be is repaid by giving the protection guarantee. Data protection can be the strategy that is utilized to give security to the data, which implies that user, can make data guaranteed by offering approval to a private association to give security to data other than the cloud service providers. In this model, all the consideration of data is taken by the private association, for

example, where the data is put away, how the data is transferred, and accessibility of data and reinforcement of data. They give fitting security estimates that will ensure their client's data and develop certainty for their services. They likewise place a keep an eye on the cloud service providers with the goal that they additionally can't break the information. This technique countermeasure for data loss and give a degree of satisfaction to the user that his data is in safe hands.

4.3 Data Integrity

To tackle issues relating to data integrity, the data record might be basically broken into parts. Various pieces of data might be saved money on another CSP or might be on various CSPs. Thusly, the CSP may not understand the significance of data. Further, if the data is encoded it defends far and away superior. In the event that a particular CSP does not stick to the user solicitation of data, the user may develop data by social affair data from different CSPs.

4.4 Theft of Data

It ought to be endeavored to dodge the data take. This can be again practiced by the utilization of two-tier architecture as examined before. Likewise adjacent to that encryption of data might be performed. Cryptography could help expanding appropriation of Cloud Computing by doubter or greater security concerned organizations. Cryptography is the most utilized practice to delicate data, completely required by industry, state and government guidelines. The degree of security where cryptography can help cloud computing is secure storage. The multi-tenant nature of the cloud enhances these prerequisites and makes interesting challenges with the accessibility and insurance of encryption credentials used to guarantee data assurance. The real handicap of secure storage is that we can't redistribute the preparing of this data without decoding it previously or without uncovering the keys utilized for encryption.

5. Framework for data security

This study proposes a framework that might be utilized to give security to data in cloud computing. In this framework all the four arrangements given above are joined together to give a progressively secure cloud computing. This framework contains four sections that are data encryption, basically broken data, data protection and two tier architecture. These all can cooperate to give a safe cloud computing. This framework outlines the working of all arrangements together. Right off the bat the data is put away in the cloud by user is encoded in this way, it can't be effectively perused out by anybody, at that point the data is fundamentally broken that guarantees the 'rule of least privilege' that implies each bit of data is sent to various service providers with the goal that they don't finish data and because of this they can't abuse data. Every user has a data guaranteed with service provider so that on the off chance that the data is lost at any rate, at that point it is repaid firm by the protection and for accessing the data user must need to login with an approved ID and password then after effective login he is furnished with PIN, after entering just right PIN the user can access the data. This framework attempts to guarantee the data security to cloud computing.

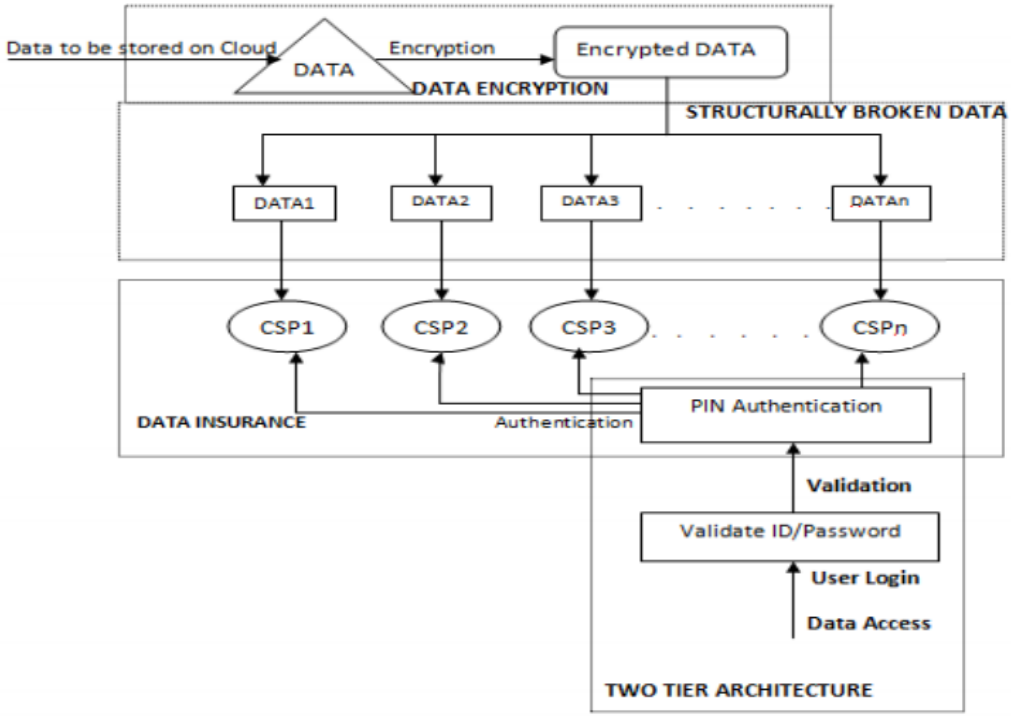


Figure 3: Framework for Data Security

6. Conclusion

Headway of cloud computing advances and expanding number of cloud users, security measurements will consistently increment. In this paper, we fundamentally order and feature the significant security issues in cloud computing systems and help users perceive threats related with their employments. Security issues present a noteworthy issue in information systems embracing and particularly in cloud computing environments in which delicate applications and data are moved into the cloud data centers. Cloud computing presents numerous novel vulnerabilities like virtualization vulnerabilities, data vulnerabilities and software vulnerabilities. Cloud computing is a dispersed architecture that brings together

server resources on an adaptable stage to give on demand computing resources and services. Data security is one of the real security worries in cloud computing as data is the most significant thing that is partaken in cloud computing environment. In this paper, some of data security issues are examined. And four arrangements are recommended that are Two-tier approval architecture, cryptography, basic technique and data protection for users which are utilized to give security to data.

References

1. K. Curran, S. Carlin & M. Adams (2011), “Security issues in cloud computing,” Elixir, 38, 4069-72
2. J. A. Mukundrao& G.P. Vikram (2011), ”Enhancing Security in Cloud Computing,” In Information and Knowledge Management Vol. 1, No. 1, pp. 40-44
3. V. Kumar, M. Swetha, M. S. Muneshwara& S. Prakash (2012),”Cloud Computing: Towards case study of data security mechanism,” International Journal of Advanced Technology & Engineering Research, Vol. 2, Issue 4.
4. V. Kumar, M. Swetha, M. S. Muneshwara& S. Prakash (2012),”Cloud Computing: Towards case study of data security mechanism,” International Journal of Advanced Technology & Engineering Research, Vol. 2, Issue 4.
5. Du Meng (2013): "Data security in cloud computing," Paper presented at Computer Science & Education (ICCSE), 2013 8th International Conference, pp.810,813, 26-28 April 2013
6. P. Bhisikar& A. Sahu (2013),”Security in Data Storage and Transmission in Cloud Computing,” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3.
7. Ali M, Khan SU, Vasilakos AV (2015) Security in Cloud Computing: Opportunities and Challenges. InfSci 305: 357-383.
8. Sushil Kumar Saroj, Sanjeev Kumar Chauhan, Aravendra Kumar Sharma and Sundaram Vats. (2015) "Threshold Cryptography Based Data Security in Cloud Computing.” IEEE International Conference on Computational Intelligence & Communication Technology: 202-207.
9. PreetiGarg and Vineet Sharma. (2014) “An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function.” IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT):334-339.
10. Balasaraswathi V.R. and Manikandan S. (2014) "Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach.”IEEE International Conference on Advanced Communications, Control and Computing Technologies: 1190-1194.
11. MrinalKanti Sarkar and Sanjay Kumar. (2016) "A framework to ensure data storage security in cloud computing.”IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON):1-4.
12. Ahmed Albugmi, Madini O. Alassafi, Robert Walters and Gary Wills. (2016) “Data security in cloud computing.”Fifth International Conference on Future Generation Communication Technologies (FGCT): 55-59.

