International Journal of Engineering & Technology, 7 (3.27) (2018) 200-205

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Issues in Cloud Computing and Existing Solutions- a Survey

M. Revathi[1*], R. Priya[2]

[1]*Ph.D Research Scholar, Department of Computer Application, Vels University, Chennai.*
[2]*Associate Professor, Department of Computer Application, Vels University, Chennai. E-mail:priyaa.research@gmail.com*
**Corresponding author E-mail:vm_revathi@yahoo.co.in*

Abstract

Cloud computing is turning into an outstanding fluff word these days. It is an appealing innovation for long-haul benefits through cost diminishment and change in business results. It additionally tackles numerous issues of stereotyped processing, including taking care of more volume of burdens, introducing programming updates, and, utilizing overabundance figuring cycles. Regardless, the contemporary advancement has new troubles, for instance, data security, information inborn, and trans-code data storing. Cloud computing is consumed and compared to the modern transformation. Cloud administrations are conveyed from server farms, for example, Amazon, Google, Microsoft et cetera, all through the world. The quick blast in the territory of "Cloud computing" moreover expands outrageous wellbeing concerns. This paper review cloud structure and the monstrous evaluation of Cloud computing with the essential consideration on holes and security issues. We perceive the best security dangers and their present arrangements.

Keywords: *Cloud computing, security challenges, denial of service, sniffer attack, CAPTCHA breaking, data leakage.*

1. Introduction

Cloud computing is the movement of registering administrations which fuse servers, storage, database, networking, programming project and more conspicuous over the internet("the cloud"). companies subscribing these figuring administrations are called "cloud Providers" which charge for Cloud processing organizations in light of use. The best focal points of Cloud processing organizations consolidate cost, speed, overall scale, productivity, execution, constancy. Cloud computing administrations work a near the ground diversely allowed on specific terms of the supplier, in any case, numerous laid at one foot an okay, program based dashboards that make it less demanding for IT experts and designers to complete a quite a piece of work their records. The Clouds are seen as five segment architecture that includes customers, applications platforms, infrastructure, and servers. Mists restrict the prerequisite for customer relationship by making particular unobtrusive components such as licenses, bolster from its customers. As Cloud computing is accomplishing expanded notoriety in the business, then again, security concerns are starting to develop about how safe a situation is. Regardless of the significant number of focal points of the cloud, customers are up 'til now reluctant to send their business to the cloud. Security issues play a noteworthy obstruction to the improvement and acknowledgment of the cloud.

2. Cloud Computing Framework

Cloud engineering could be classified based on the services and deployment model.

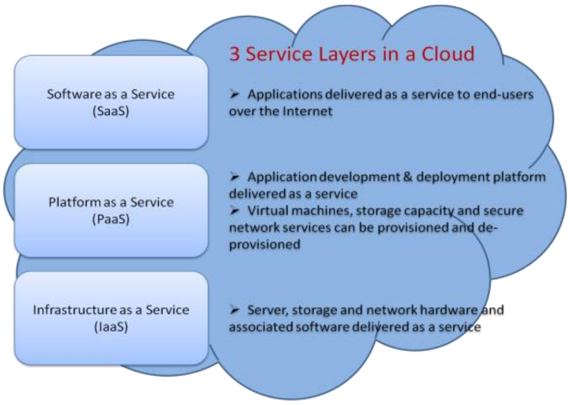
3 Service Layers in a Cloud
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
➢ Applications delivered as a service to end-users over the Internet
➢ Application development & deployment platform delivered as a service
➢ Virtual machines, storage capacity and secure network services can be provisioned and de-provisioned
➢ Server, storage and network hardware and associated software delivered as a service

Fig. 1: Cloud service model

Service Models

Software as a service (SaaS)

SaaS display incorporates surpass provider presenting, keeping up programming in cloud and customers continually the item from the cloud customers around the Internet. SaaS is flexible, course directors make sense of how to overwhelm the applications on part of servers. Before every customer would attempt to purchase and load their own duplicate of the application to every one of their own servers, however by the entire of the SaaS, the customer can achieve the audit without introducing the product locally. SaaS generously includes a month to month or infrequent expense. Programming as a business gives the proportionate of available by PC applications in the conventional spread of utilization.

Platform as a service (PaaS)

PaaS provides clients all of utilization stages and databases as an administration. This is indistinguishable to middleware in the conventional conveyance of use stages and databases. By the entire of PaaS, engineers can manufacture web applications without introducing whole apparatuses on their PCs.

Infrastructure as a service (IaaS)

IaaS nailed the physical hardware and going over virtual. This is relating to the average citizens and equipment in the customary technique running in the cloud. In differing words, organizations work out perk (month to month or every year) to challenge virtual servers, systems, stockpiling from the cloud. This will alleviate the want a server farm, sizzling, cooling, and keeping up equipment at the nearby level.

Deployment Models

Deployment model broadly categorized into four ways depending upon the customers' requirement.

Public cloud: This kind of cloud is outstanding to which the physical establishment and computational resources are made open to the general populace. It is also asserted and administered by the expert center.

Private Cloud: A cloud is one in which the registering framework is worked only for a particular association. It is additionally possessed and overseen by an outsider or might be facilitated by the association.

Community Cloud: This sort of cloud is fragrant to a private cloud, in any case, the foundation and computational assets are shared by a few associations that have normal security administration, practice, and consistence contemplations. It is claimed and overseen by the consortium of the association.

Hybrid Cloud: A cross breed cloud is the blend of the past three models (Public, Private, Community), connected in a way that information exchange happens between them without influencing each other. It is the most complex model among all organization models.

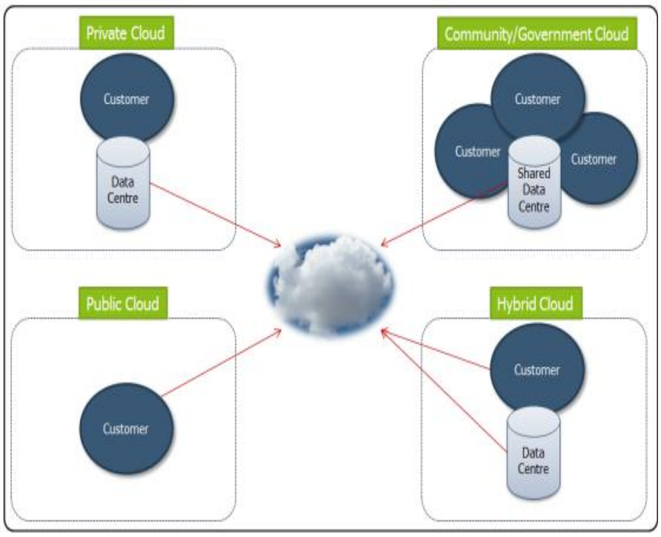

Fig. 2: Cloud deployment model

3. Cloud Computing Security Challenges

The new ideas presented by the cloud, for instance, outsourcing, asset sharing, outside information warehousing and so on builds the security concern and make new security challenges. Security issues related on cloud computing put into 2 general classifications:

- Security issues looked by cloud Suppliers.
- Security issues looked by their Customers.

Most grounded safety efforts are to be executed by perceiving security difficulties and respond in due order regarding handle these challenges. From Fig.3 Data security is the most imperative and essential factor to be considered.

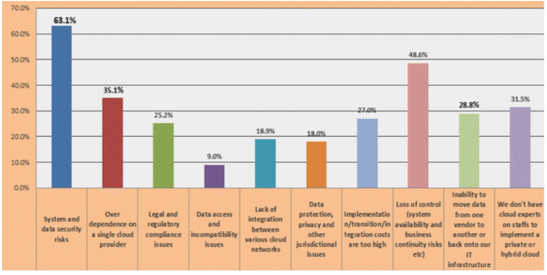

Fig.3

We categorize the security issues into 5 classes, such as Network Security, Cloud infrastructure, Data level Security, Application level Security, Security Standards.

Network Security

The Network insinuates the medium through which the customers connect with the cloud condition to play out the pined for a task. Systems are ordered into various sorts of shared and non-shared, private or open and so forth. While considering the system level security it is first to determinate amongst public and private cloud in light of the reality that the private cloud is less helpless against the general public cloud. Network related issues are accepted to be the main security challenges in the cloud since cloud computing is exceedingly arranged to organize related assaults, added cloud operations are profoundly associated with networks. The scale of network attacks dangerously boost organizations prefer to move their data into clouds. Issues related to Network security are DOS, DNS, Sniffer attacks, Distributed Denial Of Service(DDOS), Reused IP issue, flooding attacks and so forth.

Sniffer Attacks: These sorts of assaults floated in applications that can read, screen and capture network packets. If the packets are most certainly not blended, sniffer gives a perspective of information inside the packet. An assailant can dissect system and pick up data that may make the system end up degenerate.

Reused IP address: Every Computer in a system has assigned an IP address if the client of one computer exit from the system then the similar IP address is given to new clients. In this way, it will make a security hazard in light of the way that the old IP address is being dispensed to another client there exists a guess of getting to the information by another client as the address still exists in Domain name system.

Replay Attack: An attack within which the transmission of knowledge is maliciously slowed.

DNS (Domain Name System): It impacts a clarification of the area name to an IP address since the space name is less requesting to review rather than IP address. In any case, in some DDOS cases called the server by name. The customer has been controlled to some different malevolent cloud as opposed to the one he asked for and from this time forward using IP address isn't feasible.

Denial of Service: It is propelled by recognizing vulnerabilities in Internet Protocols. It powers the framework part to breaking point or stops. The system is inaccessible by flooding it, disturbing it, sticking it. The issue in DOS on the web is difficult to forestall. These assaults can be obstructed by a firewall.

Distributed Denial of Service: DDOS is a kind of DOS assault where numerous associated online administrations used to overpower an objective site with counterfeit activity. DDOS can likewise be used as a smokescreen for different malicious exercises. DDOS strikes routinely continue going for a significantly long time, weeks and even months a period, making them incredibly risky to any online affiliation. DDOs strikes can provoke a loss of pay.

Cloud Infrastructure

Cloud service providers assume a noteworthy part of a cloud domain. They are amazingly accountable for controlling the system of the cloud. clients consider specialist organization issues are the broad danger to distributed computing. A few issues related with cloud foundation incorporates unreliable interfaces of Application programming interface(API), Sharing technical defects, Reliability of providers, Quality of services, Server location, and backup, Multi-tenancy and so forth.

Insecure interfaces of API: Cloud APIs are utilized to speak with different administrations in the cloud foundation and the security of cloud benefits simply confide in the APIs security. Cloud suppliers offer their APIs to the outsider to give administrations to clients. The meager APIs can enable the outsider to get to the basic data in the cloud.

Quality of Service: It is contemned issues as long a similar number of cloud expert organizations concentrate just on quick execution and minimal effort. In this work, we consider QoS in the space of any capacity or action that straightforwardly or by implication influence security. A basic blunder in the setups could be shared by numerous administrations.

Reliability of suppliers: It is an essential segment in the cloud condition as it requires an intensive examination of the staff to control information and equipment get to. It is profoundly proposed that service providers ought to examine its staff remembering the ultimate objective to guarantee its benefits and information to pick up client's trust

Technical Flaws: Technical flaws are otherwise called notoriety destiny sharing, in which mistakes exchange from ruined server to a virtual machine that turns out to be awful when the debasement exchanges through the tainted portable VM to different servers. In this way, it is critical to distinguish and settle destiny sharing occurrences and execute best practices to keep them from reoccurring.

Multi-Tenancy: This Multi-Tenancy ability could prompt data spillage from one inhabitant to other server mates. Assaults, for example, VM-to-VM and bargained VM are turning into a center for future assaults.

Data Security

As we are moving into the web based cloud display, it requires extraordinary accentuation on information security. At the point when various association share assets there is a danger of information misuse. Protection of information is the essential difficulties in cloud computing. The data security threats include data breaches, data loss, data recovery and privacy, availability, and data protection.

Data breaches: The effusion of clients' information to an unapproved client. Information break from the association can hugely affect business with respect to finance, trust and loss of clients .this may happen coincidentally because of imperfections in a foundation, application outlining and so on.

Data Loss: Like data breach, data loss is a delicate issue for any association and have a devastating effect on its business. Information misfortune generally happens because of malicious attackers, blames in the capacity framework or catastrophic event.

Data integrity: Data integrity associated with preserving data from unapproved correction or cancellation. Managing a component's enlistment and rights to specific undertaking resources ensure that vital data and organizations are not misused or stolen. Approval is the instrument by which a structure makes sense of what level of access a particular approved customer should need to secured resources controlled by the system.

Data Confidentiality: Data Confidentiality in the cloud compares to customer authentication. Shielding a client's record from burglary is an occasion of a more prominent issue of controlling access to objects including memory, gadgets, programming and so forth.

Data Non-revocation: It is a critical anguish for Data security. It guarantees the transmission of the message among social events and gives the affirmation that some individual can't deny something

Data Availability: Client's data is ordinarily secured in the protuberance on different servers oftentimes staying in different territories or in different mists. For this circumstance, data availability transforms into a critical main problem as the openness of uninterruptible and predictable game plan ends up being modestly troublesome.

Application Level Security

Some affiliation has an application on the web that different clients use without contemplating where, how, by whom the organizations are given, so appropriate security instrument should grasp. Application-level Security recommends the utilization of programming and equipment assets for offer security to the application to such an extent, to the point that aggressors are not set up to deal with this application and take off beguiling changes.

Cookie Poisoning: Cookies used to store client IDs. It includes changing or altering the substance of cookie to have an unapproved access to an application. It basically contain the client's personality-related accreditations, the substance of these cookies can be produced to copy an approved user. This will be overwhelmed by normal cookie cleanup.

SQL infection: Attackers implanted a malignant code into a predominant SQL code and it empowers the unapproved individual to download the entire database.

Google Hacking: It alludes to utilizing Google web crawler to discover touchy information that a programmer can use to his profit while hacking a customer's record. Generally, programmers endeavor to discover the security escape clauses by testing out on Google about the framework they wish to hack. Subsequent to having accumulated the vital data they do the hacking of the concerned framework. Recently a group of hackers stole the login subtle elements of different Gmail clients.

CAPTCHA Breaking: CAPTCHA was created with a specific end goal to forestall spam and overexploitation of system assets. It was discovered that the net clients are given some type of inspiration towards understanding these CAPTCHA's by the computerized framework and in this way CAPTCHA Breaking happens.

Backdoor and debug options: A typical practice by the planners is to engage the research decision while conveying a site.. This empowers them to roll out formative improvements in the code and get actualized on the site. This may give a simple section to a programmer into the website that let him roll out improvements at the website level.

Concealed field Manipulation: While getting to a website page. there are sure fields that are concealed and contain the page related information. In any case, these fields are profoundly inclined to assaults by programmers as they can be altered effortlessly.

Security Standards

Cloud computing lacks appropriate security standards. Regardless of whether security gauges are characterized appropriately numerous security issues are still connected with consistence chances because of the absence of tutor for reviews and appraisals of corporate models.

Lack of Security Standards: Cloud computing starting today needs interoperability measures. There is no institutionalized correspondence between cloud suppliers and customers. There is no regulated information send out configuration and the absence of norms additionally make it hard to set up security structures.

Lack of Auditing: The Cloud environment introduces new difficulties from a review exchange including information that dwells in the cloud should be legitimately made and recorded, with a specific extreme target to ensure the dependability of data .Be that as it may, an arrangement of a full review trial inside the cloud is as yet an unsolved issue

Lack of Legal aspects: The legal framework has been instrumental and the key to the assurance of client's close to home and touchy data. There is as of now an exchange between association, controllers, and partners to assure that the administrative structure adapts to new systems and plans of action without dissolving client's trust. Location matters from a lawful perspective as various laws may apply contingent upon where data exists, In cloud computing, it might be hard to know precisely where the information is or it might be in travel. A convoluting factor is that there are numerous duplicates of information situated in the cloud.

Trust: When it isn't obvious to people why their own data is asked for, or how and by whom it will be handled, this absence of control will prompt suspicious and eventually doubt. Table 1. Summarizes the cloud computing security issues.

Table I: Cloud Security Classifications and Issues

Category	Issues
Network Security	Sniffer attack Reused IP address DOS Replay attack DNS attack DDOS
Cloud Infrastructure	Quality of Service Reliability of suppliers Insecure interface of API Multi-tenancy Technical flaws
Data Security	Data breaches Data loss Data integrity Data confidentiality Data Non-repudiation Data availability
Application Level Security	Cookie Poisoning SQL infection Google Hacking CAPTCHA breaking Backdoor and debug options Hidden field Manipulation
Security Standards	Lack of auditing Lack of security standards Lack of legal aspects Trust

4. Solutions for Cloud Security Issues

Network Security

Account or service hijacking can be kept away from by embracing distinctive security includes on the cloud network. These incorporate utilizing Intrusion Detection Systems (IDS) in the cloud to screen organize movement and hubs for distinguishing pernicious exercises. Recognize and access administration ought to likewise be executed appropriately to stay away from access to qualifications. To begin with, the client is confirmed by the cloud get to a secret word and in the following level, the administration gets to the watchword of the client is checked. To keep away from DOS assaults it is vital to recognize and actualize all the fundamental security necessities of the cloud organize, applications, databases, and different administrations. The DDOS assaults can be forestalled by having additional system data transfer capacity, utilizing IDS that confirm arrange necessities before achieving cloud server and keeping up a reinforcement of IP pools for critical cases.

Cloud Environment Security

To shield the cloud from unreliable API dangers it is imperative for the engineers to plan these APIs by following the standards of trust computing. The cloud suppliers must guarantee that all APIs executed in the cloud are outlined safely. Solid confirmation components and access controls should likewise be executed to secure information and administrations from uncertain interfaces and APIs. The insurance from malicious insiders can be accomplished by restricting the equipment and foundation get to just to the approved faculty. The specialist organization must execute solid access control and isolation of obligations in the administration layer to confine manager access to just his approved information and programming.

Data Security

Encryption is proposed as a superior answer for secure data. Different safety efforts and systems have been proposed to stay away from the information break in the cloud. An effective key administration calculation is executed to forestall data leakage. To anticipate information misfortune in cloud diverse safety efforts can be received. The essential measure is to keep up a reinforcement of all information in the cloud which can be gotten to if there should be an occurrence of information misfortune. A trusted server can screen the capacities performed on information by cloud server and give the total review answer to the information proprietor.

CPABE (Cipher Text Policy Attribute Encryption) is a system for ensuring the privacy of putting away information and transmitting information data in outer capacity.

Application Level Security

In cloud design, the hypervisor is in charge of interceding communications of virtual machines and the physical equipment. Along these lines, the hypervisor must be secured to guarantee appropriate working of other virtualization segments and executing confinement between VMS. To keep away from shared innovation dangers in the cloud, a methodology must be produced and actualized for all the administration display that incorporates foundation, stage, programming and client security. The service provider screens the vulnerabilities and discharges patches to settle those vulnerabilities frequently.

Security Standards

The implementation of strict beginning enlistment and approval procedures can help in recognizing noxious consumers. The arrangements for the insurance of imperative resources of the association should likewise be made as a piece of Service Level Agreement (SLA) amongst client and service provider. This will acquaints client with the conceivable legitimate activities that can be led against him in the event that he damages the assertion.

5. Famous Cloud Computing Platforms

Eucalyptus

Eucalyptus predominantly used to fabricate private cloud . Eucalyptus empowers pooling to enlist, gathering, and system assets that can be ceaselessly scaled up or down as application workloads change. Clients can in like way move occasions between an Eucalyptus private cloud and the Amazon Cloud to influence a creamer to cloud. Equipment virtualization segregates applications from PC adapt reasons for intrigue. The AWS(Amazon Web Services) API is executed over Eucalyptus, so gadgets in the cloud condition that can talk with AWS can use comparative API with Eucalyptus.

Nimbus

Nimbus is a software with source code that anyone can modify and enhance. Nimbus is a capable toolbox that, once introduced on a bunch, gives a framework as an administration cloud to its customer by means of WSRF-based.
To open all power and adaptability of IaaS to logical clients Nimbus project engineers focused on the primary three objectives and their open source usage:

- Offer abilities to suppliers of assets for private or group IaaS clouds improvement.
- Offer abilities to clients for IaaS cloud application.
- Offer abilities to engineers for an expansion, experimentation, and customization of IaaS.

Distinctive blends of these apparatuses help clients in the fast improvement of custom group particular arrangements. For instance, Nimbus empowers clients to manufacture various virtual machines and convey them all through the cloud with the objective that they will co-work and supplement each other.

Azure

Microsoft Azure is an expansive arrangement of cloud benefits that specialists and IT specialists use to create applications through our overall arrangement of data centers. Azure is beneficial for developers. Azure incorporated devices, from mobile DevOps to serverless processing bolster your efficiency. azure is the main reliable hybrid cloud. Connect information and applications in the cloud and on-premises-for greatest portability and incentive from your current speculations. [19]Azure offers hybrid consistency in application advancement, administration and security, personality administration and over the information platform. Azure supports a span of operating systems, databases, programming languages and devices. Azure Automation, gives an approach to clients to computerize the manual, long-running, mistake inclined, and every now and again rehashed assignments that are ordinarily performed in a cloud and endeavor condition. It spares time and expands the unwavering quality of standard regulatory assignments and even calendars them to be consequently performed at general interims.[20]

6. Literature Survey

The Survey contains the implications of Cloud processing described by NIST. It is perfectly clear that the security issue has expected the most basic part in hindering the acknowledgment of Cloud Computing. A number of researchers have discussed the security challenges that are raised by distributed computing. Considering security inspiration driving Cloud stockpiling, diverse encryption techniques are being dismembered by the experts.
Pradeep kumar et.al[8] have concentrated on the plan of the security related issues of cloud computing with the help of Hidden Markov Model based Clustering utilizing Data mining Techniques which can be amazingly profitable methodology to perceive any kind of intrusion recognizable proof in the framework.
S.Swarajyam et.al[16] concentrating on designing registering and advancement errands examine secure outsourcing of broadly relevant straight programming (LP) computations. It builds an arrangement of proficient protection saving issue change systems which enable the client to change unique LP issue into subjective one.
S.Hemalatha et.al[17] examining on completely homomorphic encryption to improve the safety efforts of un trusted frameworks that stores and controls touchy information, and furthermore the outline and usage of completely homomorphic encryption(FHE) plot in light of Ring is accounted for.

7. Conclusion

The tremendous security stresses with the cloud framework is the resource sharing. Since every single association is moving its information to the cloud implies it utilizes the capacity benefit gave by the cloud provider. Therefore it is required to ensure the information against unapproved access, change or dissent of administrations and so on. Security specialists forecast that clouds will be the target point of hackers in future because of the centralization of important "assets"(data and calculation) inside the clouds. We have distinguishes a couple of zones that are as yet unattended in cloud computing security.

Table II: Literature Description

Ref.No	Authors	Methodology	Drawback/Future work
[2]	Er. Nisha Yadav et al.[2016]	Authors have explored security for data using CHAP (Challenge-Handshake Authentication Protocol) convention and additionally RSA encryption calculation. This will give authentication and additionally Security to the information.	Only technical privacy and encryption controls were analyzed and developed in this paper.
[4]	Sanjoli Singla et al [2013]	Authors designed a framework that helps to encrypt and decrypt the data at the client side and have used a Rijndael encryption algorithm with EAP-CHAP	A significant direction of their future work is to design different algorithms to avoid data leakage.
[12]	Chandu Vaidya et al. [2016]	In this paper the proposed approach is to detect when the distributor's sensitive data has been leaked by agents, and if possible to identify the agent that leaked the data. SHA algorithm is used to protect data at the time of upload to third party agents	Scope of this framework can be reached out by making arrangements for the age of phony records progressively as indicated by the agent's request.
[15]	Rajesh Manoharan et al [2018]	This paper proposed the distinctive encryption strategies are cloud sensitive data security process.	This paper focuses only on review of existing encryption algorithms.
[18]	Manish M Potey et al [2016]	Author focuses around putting away information in the cloud in encoded shape utilizing completely homomorphic encryption.	Proposed calculation supportive for now' prerequisite just, in future distinctive ways to deal with demonstrate the adequacy of a proposed structure.

References

[1] Rajesh M, Kumar KS, Shankar K & Ilayaraja M, "Sensitive Data Security in Cloud Computing Aid of Different Encryption Techniques", *Journal of Advanced Research in Dynamical and Control Systems*, Vol.18, (2017), pp.2888-2899.

[2] Yadav Er. N & Sharma A, "Implementation of data Security in Cloud Computing", *3rd international conference on recent Trends in Engineering Science and Management*, (2016).

[3] Gupta D, Chakraborty PS & Rajput P, "Cloud Security Using Encryption Techniques", *International Journal*, Vol.5, No2,(2015), pp.425-429.

[4] Singla S & Singh J, “Cloud data security using authentication and encryption technique”, *Global Journal of Computer Science and Technology,* (2013).

[5] Bhadauria R, Chaki R, Chaki N & Sanyal S, “A survey on security issues in cloud computing”, *arXiv preprint arXiv:1109.5388,* (2011).

[6] Kavitha, M., & Saravanakumar, V. (2018). Proactive model based testing and evaluation for component-based systems. International Journal of Engineering and Technology(UAE), 7(1.1).

[7] Mathisen E, “A Security Challenges and Solutions in Cloud”, *International Conference on Ecosystems and techniques*, (2011).

[8] Kumar P, Sehgal V, Shah K, Shukla SSP & Chauhan DS, “A novel approach for security in cloud computing using hidden markov model and clustering”, *World Congress on Information and Communication Technologies (WICT),* (2011), pp.810-815.

[9] Padhy RP, Patra MR & Satapathy SC, “Cloud computing: security issues and research challenges”, *International Journal of Computer Science and Information Technology & Security*, Vol.1, No.2, (2011), pp.136-146.

[10] Sreedharan S, “Security and Privacy Issues of Cloud Computing; Solutions and Secure Framework”, *IOSR Journal of Computer Engineering*, (2013).

[11] Peng J, Zhang X, Lei Z, Zhang B, Zhang W & Li Q, “Comparison of several cloud computing platforms”, *Second International Symposium on Information Science and Engineering,* (2009), pp. 23-27.

[12] Vaidya C, Khobragade P & Golghate A, “Data Leakage Detection and Security in Cloud Computing”, *GRD Journals-Global Research Development Journal for Engineering*, Vol.1, No.12,(2016).

[13] Han S & Xing J, “Ensuring data storage security through a novel third party auditor scheme in cloud computing”, *IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS),* (2011), pp.264-268.

[14] Chen ZB & Yang JF, “Cloud Computing Research and Security Issues”, *IEEE International Conference on Computational Intelligence and Software Engineering (CISE)*, (2010), pp.1-3.

[15] National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov)

[16] Swarajyam S, Madhukar E & Sowmya Lakshmi P, “Data Security in cloud Computing using Linear Programming”, *IOSR journal of computer Engineering*, (2012).

[17] Hemalatha S & Manickachezian, R “Performance of Ring based Fully Homomorphic encryption for securing data in cloud computing”, *International Journal of Advanced Research in Computer and Communication Engineering,* Vol.3, No.11,(2014).

[18] Potey MM, Dhote CA & Sharma DH, “Homomorphic encryption for security of cloud data”, *Procedia Computer Science*, Vol.79, (2016), pp.175-181.

[19] G Mussabekova, S Chakanova, A Boranbayeva, A Utebayeva, K Kazybaeva, K Alshynbaev (2018). Structural conceptual model of forming readiness for innovative activity of future teachers in general education school. Opción, Año 33. 217-240

[20] G Cely Galindo (2017) Del Prometeo griego al de la era-biós de la tecnociencia. Reflexiones bioéticas Opción, Año 33, No. 82 (2017):114-133