INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 146-152

e-ISSN : 2583-1062

Impact Factor: 5.725

THE TRIVIAL SHORTCOMINGS AND THE EXTANT RESOLUTION AVAILED IN THE CLOUD REALM

Julian Menezes Rathinam[1], Shirley Maria Beaulah Cyril Raymond[2], Punitha Gnanam[3], Roshni Swathy Suresh[4]

[1]Assistant Professor, Department of Computer Science and Engineering, Loyola Institute of Technology, Chennai, Tamil Nadu, India.

[2,3,4]Final Year Student, Department of Computer Science and Engineering, Loyola Institute of Technology, Chennai, Tamil Nadu, India.

ABSTRACT

The entity termed as Cloud Computing is defined as a blueprint that which utilizes the amalgamation of dual trivial entities termed as Computing based upon Utility and one among the services given out by the cloud defined as Software as A Service, and above all provisions a variant of services on demand as and when requested by a specific Individual. Cloud Computing is defined to be ubiquitous, the sole reason being it is made to be availed 24/7 on account of the connectivity to the Internet and the access point is done by anything and everything, ranging from the Palm tops to devices associated with IOT. Recent surveys by top notch professional bodies indicate that Cloud Computing is the heart and soul of almost all the Technologies which exist already and for the technologies which are yet to come into play. Nevertheless, the Individuals who are willing to hop onto to this technology are quite foreboding in regard to opt this model associated with Computing, why because of the fact that this computing is haunted by concerns which are closely associated with the entity of Security. The issues arising from the Cloud is quite trivial as well as critical on account of the fact that the resources are distributed all across the globe. There exists a confusion between the terminologies Grid as well as the Cloud, the former speaks on physical resources working together to achieve a humongous task which is of trivial and extremely necessary, while the latter speaks of physical servers hosted on a distant region, whose services are accessed by the Individuals for a subscription per month or for the entire year. The entity defined as Security depends on the responsibility of both the Provider as well as the Consumer, wherein both the parties are made to be absolutely sure that the space on the Remote Server is quite buttoned up from any sort of an external threatful entity in such a way that the consumer doesn't need to face any sort of issues associated with the loss of precious digital 0s and 1s. There exists 'n' number of possibilities where in an end user with a negative intention might pose as an authorized user and upload an infected document with a backdoor to a malicious network and embezzle all the data and play around with them. The entity defined as Security remains an unsolvable issue associated with the Cloud computing realm. For the intention of putting the concerns at rest, this manuscript enumerates the criterion that has a negative impact in the domain of Security in the Cloud, after which the exploration of the issues associated with Security gets done followed by the discussion of the annoyance which are undergone by the dual parties Subscriber as well as the Provider w.r.t the traits associated with their digital data like the aspect of concealment, reticence, as well as credibility. The final part of this manuscript presents explications for the purpose of confronting the above said enumerations as well as the concerned complications.

Keywords: Cloud Computing, Data Security, Multitenancy, Security, Cloud Computing Data Protection, Encryption, Digital Signature, Security issues.

1. INTRODUCTION

With reference to the entity defined as the Cloud; is entitled to be the new generation's outstanding coinage of this digital era, on account of its avant-garde paradigmatic associated with the use of computers in the form of utility. Cloud Computing has provisioned an increase in the concept defined as scalability followed by resilience, steadfastness coupled with the subsidized disbursement associated with the duo transaction as well as fostering. The time frame which is required to set up the Cloud and the serenity to increase as well as decrease the hardware and the associated resources, based on the requirement has literally amended the ways and means of how computing and the services associated with communication get utilized whilst forging them to be exceptional, agile and economical [1]. The blueprint associated with the Cloud Computing provisions an admittance onto 'n' number of computing resources which are shared and are availed off the internet and the users who have a subscription may have an opportunity to log and utilize the resources [2][3]. The dual idiosyncratic traits associated with the Cloud consist of:

- There exists a need when it comes to the utilization of computational resources coupled with
- Assigning of the aforementioned resources only when they are required in a dynamic manner.

The thumb rule of the Cloud lies in the deportation of the services associated with computing from the device being utilized by the common Individual on to a network filled with state of the art technologies embedding Servers both Physical as well as Virtual which in turn are connected to the Computers [4] represented by the diagram enumerated under 1.

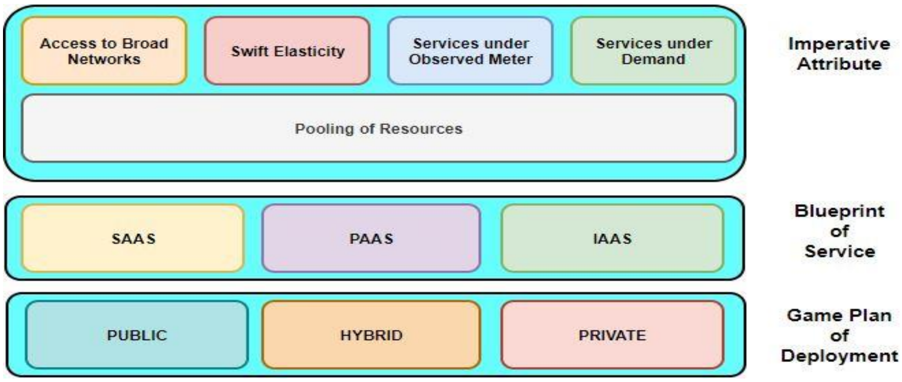

Fig. 1.1: Blue Print Definition of the Cloud

With the reference to the Cloud there exists no requirement for procuring or any need for maintaining any sort of a resource required for setting up a network, heavy gears for hardware, Terabytes for storage, Applications for Computing, and Servicing any sort of a Hardware nor a Network related stuff, etc....instead of the above anything and everything can get utilized from the network associated with the Cloud. There exists several synopsis associated with the Cloud, one among those which was published by the world renowned NIS Technology referenced under the manuscripts [5] and [6] delineates the Cloud as a blueprint that which sanctions wall-to-wall, opportune, as well as full-fledged entry to 'n' number of Computers to perform anything and everything that the user may ponder upon. The above mentioned Computers with processing abilities have the ability to get pushed on to an end user sans any herculean formalities or any sort interactivity from the end of a Service Provider as mentioned under [7]. Nonetheless, many able users are quite circumspect for the purpose of adapting the Cloud on account of the concerns present in the Cloud, as depicted in the manuscripts referred by [7] & [8]. The ineptitude of the user holding the data to have one, hovering governance upon their digital 0s and 1s is one among the trivial concerns associated with the Cloud. With reference to the elevated utilization of devices which are based out of the Internet, the tools for chatting and communicating having become a part and parcel of life have opened the portal leading to menaces off the Web, and in turn accelerating a pathway leading to chaos [9]. Shielding the Data in the circumstance related to the Cloud coupled with Mobility is absolutely trivial. Therefore, there is a need of the hour to focus all the attention to put an end to the concerns associated to security in the environment of Cloud prevailing in all walks of the Corporate Domain [10]. Of late, 'n' number of manuscripts are getting pulled online, that deal with the concern associated with Security, as referenced under [11], [12], [13]. Nonetheless, adequate lucidity with reference to the germane concerns prevailing in the Cloud inclusive of the analogous menaces; hazards, susceptibility, desideratums as well as explications are yet to be accomplished. On top of that, the aspect of security which is related to the entity defined as Virtualization which is associated with Cloud is still in its prime and it is an area that needs inherent research. This manuscript provisions a far-reaching analysis on top of a lot of security concerns. The underlying technology under the Cloud gets bifurcated into triple variant sections with reference to their utilization whilst christening them under the terminologies Private, Hybrid as well as Public. When the aspect of Cloud gets domineered by a one and only firm, the spotlight gets focused on the Private one while the conglomeration of organizations gets their hands on the technology the focus shifts on to the Public, and last but not the least the union of the above two gets named as Hybrid.

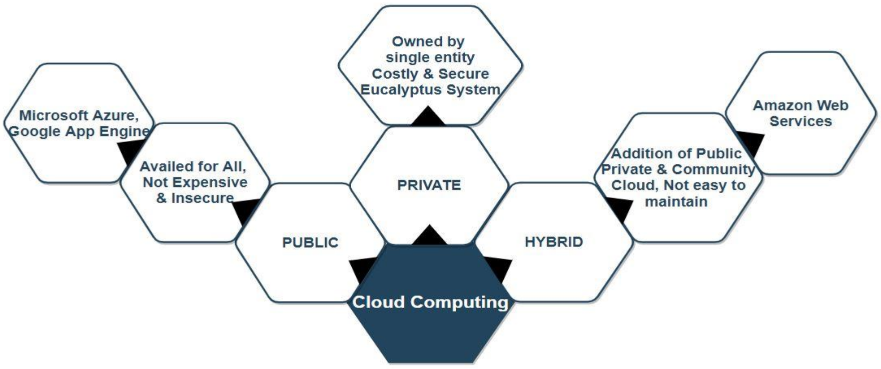
Owned by single entity Costly & Secure Eucalyptus System
Microsoft Azure, Google App Engine
Amazon Web Services
Availed for All, Not Expensive & Insecure
PRIVATE
Addition of Public Private & Community Cloud, Not easy to maintain
PUBLIC
HYBRID
Cloud Computing

Fig. 1.2: Deployment Models in the Cloud

The boon of the Cloud might be engaging, on the contrary everything has a loop hole even on the Cloud on account of loss and theft of digital information as well as Privacy; referencing manuscript number [14]. Additionally, the manuscript attends to the variant aspects like quantification, identification, classification as well as organizing the humongous security related issues coupled with the ways and means of tackling the corresponding issues with the Cloud.

2. THE CRITERIONS OVERWHELMING THE SECURITY IN THE CLOUD

There exists 'n' number of concerns associated with Security in terms of the Cloud, on account of the Cloud being the epicenter of variant Computer based Networks, Multiple Operating Systems, Backend Databases from several vendors, Allocation of several Resources, Processing of disparate transactions, Balancing the Load in terms of Virtualization, last but not the least we have the Management of Memory coupled with Control over the entity defined as Concurrency as described under the manuscript numbered under [15].

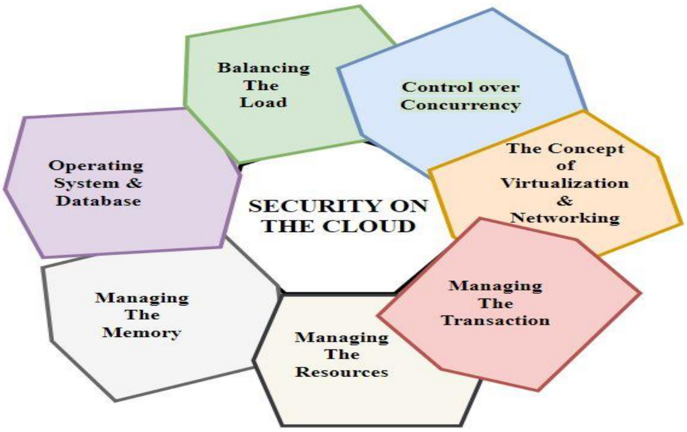

Fig. 2.1: Criterions overwhelming the aegis in the Cloud

The discordant concerns associated with Security associated with the orderliness as well as automations are quite pertinent to the systems inherent in Cloud. For an instance, the conglomeration of Routers, Hubs and Switches which are making the Computers to talk to each other in the Cloud ought to be shielded from outside menaces and threats. Furthermore, the paradigm associated with the entity defined as Virtualization gives rise to variant controversies associated with Security. To quote an instance, the alignment of the Computing systems from the Virtual domain to the Physical realm ought to be carried out in a neat and an impregnable manner. The act of shielding the data is closely associated with enciphering coupled with making sure that the required compelling game plan are under effect for the purpose of sharing the digital 0s and 1s, on the line. Additionally, the Algorithms which are associated with entities like Allocation of Resources as well as Management of Memory ought to be bulwarked. Last but not the least, the mode of operation associated with Mining the digital 0s and 1s might get applied for the detection of unwanted malicious wares in the realm of the Cloud.

3. DISPARATE SECURITY CONCERNS FACED BY THE CLOUD

On any given occasion when the discussion in terms of security which is associated with the Cloud takes the centre stage, there arises 'n' number of pros and cons associated with it. Referencing the url https://tinyurl.com/cloudprovisioners there exists the enumeration of top 10 Cloud Providers commencing from Microsoft, Amazon, Google, Alibaba, IBM, Oracle, Salesforce, SAP, Rackspace and ending with VMWare. There is a steady increase in the service providers from day to day life, whilst the former products from Sundar Pichai as well as from Andy Jassy are in a pursuit for the primary position. The user is given an option to opt for any sort of a provider based on the needs and wants of the end user. When the agreement gets signed from both the parties, the CSP ought to take care that there exists neither discomfort nor any sort of an issue that might affect the end user in terms of loss or theft to their digital 0s and 1s. With the reference to manuscript number [7] there might arise a situation that an end user might have written his/her user key on a sticky note on account of memory slip, and an intruder might have taken a note of the same and access the Cloud with an intention to cause chaos, by injecting the space with malicious codes leading to compromise of digital 0s and 1s. Whilst deliberating on the aspect of security in the Cloud, there arise discussions which in turn terminate with quadruple concerns. They are as follows

- Concerns relevant to the Digital 0s and 1s.
- Issues associated with Concealment.
- Applications intruded with malicious Coding.
- Complications associated with Aegis.

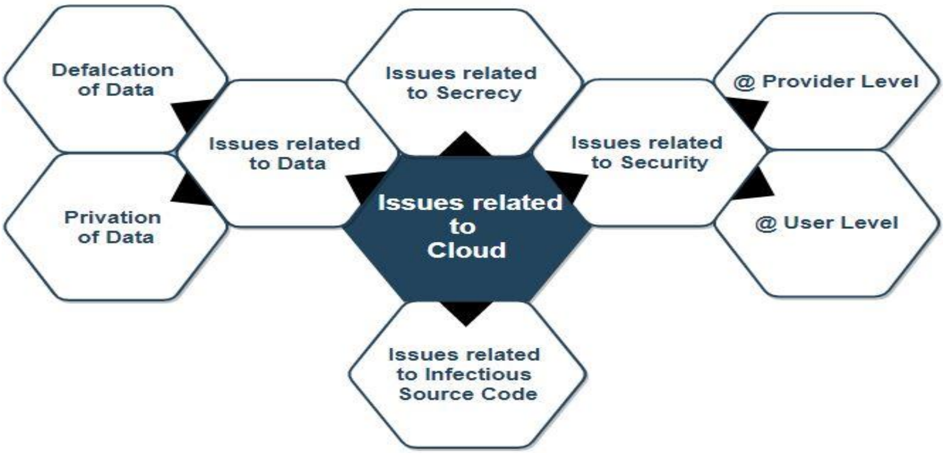

Fig. 3.1: Issues associated with the Cloud

A. CONCERNS RELEVANT TO THE DIGITAL 0S AND 1S

With the reference to the question of security associated with that of a file being sensitive and stored in the Cloud, gives rise to a trivial issue that is so sensitive, that it is quite difficult to scrap it beneath a carpet. First and foremost, whenever the digital files get pushed on to the Cloud from the user's remote machine to the space allocated to the end user, with the click of a button or the touch of a screen anyone can have a fair share of the file from the Cloud. The digital data might be or may not be private or sensitive. In the event of the data getting accessed by the end user, they might get accessed from the CSP as well as they might get modified also. Then there arises a question of data being embedded with the entity of rectitude in the ambiance of the Cloud. To continue, data larceny is defined to be the next ongoing constraint in the Cloud. The CSPs who are well off have their own Servers for providing the required services to the consumers, whilst other competitors who have started as entrepreneurs tend to rent out the servers from other service providers on account of cost efficiency. Therefore, there exists a contingency for the digital files and information to get swiped off from these so called Servers. Tertiarily, the forfeiture of data seems to be a bourgeois issue in the Cloud. On any occasion the CSPs foreclose the services rendered by them on account of some constraints related to juridical or pecuniary, which in turn leads to the forfeiture of data. Furthermore, the digital 0s and 1s can get depraved on account of certain mishaps, inclusive of nature's fury coupled with uncontrollable fire which recently made headlines in National Television. Last but not the least, the environment coupled with the turf upon which the digital 0s and 1s get fortressed under, gets defined to be the trivial as well as the prevalent menace to the concept of aegis; needs assiduity in the environment associated to the Cloud. The argumentation behind the previous statement has risen because of the fact that the consumers are in need of a disclosure of the latitude and longitude of the location where their information is going to get stored and retrieved. They demand their data to remain transparent in terms of the place and position of the hardwares arsenaling them in any point in this Planet. A few years back Microsoft sunk twelve racks of servers beneath the Scotland Sea, for better protection, privacy as well as saving the bills to keep the Hardwares cool and sustainable.

B. ISSUES ASSOCIATED WITH RETICENCE

The Organizations that which are responsible for provisioning the services rendered from the Cloud to the consumers, ought to comprehend the fact that the digital 0s and 1s which are related to each and every Individual ought to be kept quarantined with reference to their competitive providers associated with Cloud as well as their subscriber's data and the Individuals who are associated to the respective data. Since most of the Hardwares as well as the parts which get utilized for storing as well as calculating coupled with Networking get fired up from a distant remote location, the CSPs ought to fathom which entity has an uninterrupted admittance to the digital data and who gets to perpetuate the Hardware fortressing the data so at the end of the day the CSP is in a position to provision a strong hold over the subscriber's recherché data.

C. VITIATED SOURCE CODES

Door knob techniques are widely utilized by Individuals with a negated intention, to break into secured walls of firewalls and IPS for the purpose of reading and stealing; a targeted end user's personal Files for selfish motives. Whenever there is advancement in technology, so are the loopholes to take an upper hand and exploit the technology. With reference to the above statements the CSPs ought to have a perfect dominance over their hardwares and equipments, which get used for the Individuals who are opting for the Cloud. When the concept of authority prevails over the Hardwares, the CSPs get armed with full-fledged governance over the admittance to data over the Remote Servers.

D. THE CONTROVERSY ASSOCIATED WITH AEGIS

There is a mnemonic which goes like the terminology Security cannot be spelled sans 'U', likewise the dominance of security over the Cloud isn't based out of a single entity but out of duality, one being the Organization provisioning the Cloud and two being the Individuals who would like to opt for utilizing the concept of Security in the Cloud. The team deputed for conceiving the idea for blueprinting the Cloud, should take care and make proper arrangements in such a way that the Hardware and the associated gadgets are impenetrable from any form of an attack that may arise from an end user with a malicious intent. It is the responsibility of the team to provide a virtual layer of protection for shielding the end user's data from any menace that might appear from a remote and an isolated network. The responsibility extends towards the end user as well in terms of verifying the data, is free from any sort of a corruption, it is also the duty of the subscriber to analyze their data, so that it is free from duplication and it should not be a hindrance to the data of other end users in the Cloud. The Cloud is as good as the features in terms of the Security are in its place. Therefore, it is the duty of the CSP to ensure that the Security aspects are in proper order, so that the data which is getting pushed on to the Cloud is safe from any sort of unwanted malicious activity.

4. EXPLICATIONS TO THE CONTROVERSIES PREVALENT TO THE CLOUD

There exists an appalling requirement for a state-of-the-art automated technical knowledge, suppositions as well as methodologies which point out a path way for the purpose of shielding the Cloud. There is availability for a blueprint which is attainable in a layered format in turn aids in provisioning the entity of security in the Cloud. The blueprint defined above is provisioned with quadruple mantles [15]. The primary mantle is infested with Virtual Machineries, whilst the secondary entity is christened as the Storage associated with Cloud. This layer or the mantle possesses a blueprint related to an arsenal that in turn clubs up variant assets associated to disparate CSPs, thus fabricating a cumbersome orderliness concorded with the entity of virtualized repertory. With reference to the developer of a manuscript enumerated by the numeral [15] the quaternary mantle entitled as Virtualized Network Audit, functions by conglomerating dual entities correlated with Hardware gadgets coupled with the relevant Softwares to take down any unwanted menace that might arise in the virtualized systems. Nonetheless, there exist divergent conclaves who toil round the clock in bringing out certain norms as well as game plans involving security embracing the Cloud. The entity termed as the provisioner of CSA ought to illustrate the game plans as well as be assured the technological advancement residing in the Cloud gets hovered upon by users with the prerogatives.

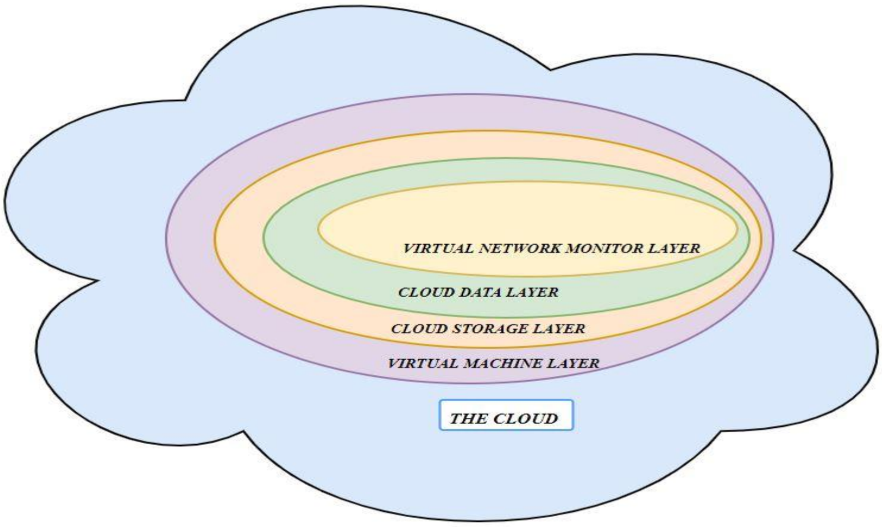

Fig. 4.1: The Layered Architecture of Security in Cloud

4.1 DOMINANCE OF ACCESS ON THE GADGETS UTILIZED BY THE SUBSCRIBERS

The CSPs ought to be incontestable on the fact that the gadgets inclusive of the primitive Desktops, Palmtops, Laptops, and any device that can talk to the Internet inclusive of the latest Apple, Windows as well as Androids which are getting utilized by the subscribers for an entry into the cloud is free from any sort of an insurgency. In the event of a larceny or a theft involving the contraptions which were used by the legal users for accessing their sensitive data on the Cloud, provided the widgets fall on the wrong hands then chaos erupts all across the Globe leading to a catastrophic Hardware coupled with the Software failure. The Security Alliance associated with the Cloud has laid out the required rules and regulations for the execution of the Cloud. The CSPs ought to embrace the appropriate procedures and rules for accessing an account coupled with 'n' factor authentication, print from the thumb, retina scanners and so on for the proper maintenance for ensuring the gadgets aren't misused and nothing is out of line.

4.2 SURVEILLANCE OVER THE ACCESSED DATA

Incontestable, The CSPs ought to be incontestable when it comes to monitor what sort of a data is getting accessed by which subscriber during what part of the day and at what time, by means of a time stamp. The reason for the above statement being inscribed now is on account of the grievances received from a number of subscribers stating the fact that their digital information is getting eavesdropped upon by unauthorized subscribers.

4.3 PROVISION OF AUDIT FILES ON DEMAND

In the event when an occasion arises where the subscriber would like to report any sort of event that might have happened inside the Cloud, it is at this juncture the CSPs ought to be in a position to provision any sort of a confidential material to the consumers on demand. When a end user removes any remnants of his/her file off the Cloud, the CSP is supposed to make sure there does not prevail even the slightest fragment of the files that might linger back in the Cloud.

The reason behind the previous statement is that most of the CSPs don't bother to cleanse the space in the Cloud post deletion leading to the wastage of precious room in the Cloud [16].

4.4 EVENT CORRELATED WITH AEGIS:

There ought to be an assurance that the CSPs provision ample amount of Information in terms of attaining the entity of assurance, coupled with remedy associated with break, last but not the least provisioning the aspect of contingency. The above events would construe the roles, avowal, as well as the responsibilities associated with the CSPs.

5. CONCLUSION

The CSPs as well as the related subscribers ought to be completely aware that the Cloud Technology which they are opting for is completely secured with reference to all the external menaces or any sort of an outside threat, therefore there would exist a full-fledged dual interpretation co-existing in between CSP as well as the Subscriber. The conduct of a subscriber can get monitored 24/7 for an example an observation can be made if a particular subscriber gives an authority for an automated patching of an Application coupled with automated updation for the definitions associated with Antivirus Applications.

The humongous space prevalent in between Applications associated with the security of Cloud as well as the theoretical research is bolstered on the certitude that certain hunch associated with the entity of research throws out quite a few variations between duo entities titled Aegis affiliated to Virtual Machine as well as the Cloud. The entity defined as inquest ought to take the center stage with reference to the spaces as well as variations coupled with the deletion. One particular fragment related to the blueprint may get required for conceiving a game plan for surveying the software associated with the Cloud, and further may lead to the bringing up of a separate processing related to the programs associated to the Individual unique Clients.

6. REFERENCES

[1] GAP Report. Global Access Partners (GAP) Task Force on Cloud Computing. 2011.http://www.globalaccesspartners.org/Cloud-Computing-GAP-Task-Force-Report-May-2011.pdf.

[2] Buyya R, Broberg J, Goscinsky A. Cloud Computing: Principles and Paradigms. John Wiley and Sons;2011.Crossref.

[3] Sosinksy B. Cloud Computing Bible. John Wiley and Sons; 2011.

[4] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems.2009; 25(6):599–616 Crossref.

[5] NIST. http://csrc.nist.gov/groups/SNS/cloud-computing/2011.

[6] NIST. http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html. 30th Dec 2012.

[7] Sangeetha T, Saranya M. Survey of security auditing issues in cloud computing. International Journal of Electrical Electronics and Computer Science Engineering. 2014;1(5):33–36.

[8] Gokulan V, Kalaikumaran T, Karthik S. Procuring data storage security in cloud environment by using two step secure protocol. International Journal of Software and hardware Research in Engineering.2014; 2 (4):102–7.

[9] Donald A. Cecil, Oli S. Arul, Arockiam L. Mobile cloud security issues and challenges: A perspective. International Journal of Engineering and Innovative Technology.2013;3(1):401–6.

[10] Jaffar Ali, Shareefa Rabiya N. Secure Cloud – A Survey. International Journal of Computer Science and Information Technologies.2014; 5 (4): 5447–49.

[11] Hashizume K, Rosado DG, Fernández-Medina E,Fernandez EB. An analysis of security issues for cloud computing.Journal of Internet Services and Applications. 2013;4(5): 2-13. Crossref.

[12] Gonzalez N, Miers C, Redígolo F, Simplício1 M, CarvalhoT, Näslund M and Pourzandi M. A quantitative analysis ofcurrent security concerns and solutions for cloud computing.Journal of Cloud Computing: Advances, Systems andApplications. 2012; 1(11):2–18.

[13] Balasubramanian V, Mala T.A review on various data security issue in cloud computing environment and its solutions. ARPN Journal of Engineering and Applied Sciences. 2015;10(2):883–9.

[14] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(S. Kuppuswamy, P. B. Shankar Narayan, "The Impact of Social Networking Websites on the Education of Youth", In International Journal of Virtual Communities and Social Networking, Vol. 2, Issue 1, page 67-79, January-March 2010.

[15] http://searchvirtualdatacentre.techtarget.co.uk/news/1510117/Community-cloud-Benefitsand-drawbacks area is Cloud Computing, Software Engineering, and Data Mining.

[16] Problems Faced by Cloud Computing, https://tinyurl.com/y28oxcw2.