Journal of Engineering Sciences
Vol 10, Issue 11, Nov /2019
ISSN NO:0377-9254

A Complete Survey Report on Storage and Security Challenges in Cloud Computing Environment

Naga Mallikharjunarao Billa
Asst.Professor, Vignan Degree College, Pedapalakaluru, Guntur, AP, India-522009

ABSTRACT: Over the latest couple of years, the connecting with features of disseminated processing have been invigorating the coordination of cloud circumstances in the business, which has been along these lines driving the investigation on related developments by both the business and the academic network. The probability of paying-as-you-run mixed with an on-ask for adaptable movement is changing the undertaking handling model, proceeding onward premises establishments to off premises server ranches, got to over the Internet and managed by cloud encouraging providers. Notwithstanding its focal points, the change to this enlisting perspective raises security concerns, which are the subject of a couple of examinations. Other than of the issues got from web developments and the Internet, fogs present new issues that should be gotten out first in order to moreover empower the amount of cloud plans to increase. Data security is described as decency, order, insurance and enduring nature of data kept up by an affiliation. Security concerns association with Cloud Computing is extensively described into two groupings: Security issues looked by Cloud providers and Security issues looked by their customers. This paper deals with the organizations given by cloud, chance related with it and security endeavors in Cloud Computing.

Keywords: Cloud Computing, Deployment Models, Service Models, Security Risks, Security Measures.

I. INTRODUCTION

Cloud computing is quickly expanding innovation and it has changes the product from server to administrations. Different cloud specialist organizations, for example, Amazon web administrations (AWS), Microsoft Azure and so on give diverse administrations to client on (PAYG) pay as you go premise. According to the meaning of NIST [2] "Distributed computing is an Internet figuring for pervasive and on interest access to assets conveyed to clients" [2]. The client can get to an assets from anyplace, whenever around the globe. Cloud computing utilizes virtualization innovation and utility figuring. Cloud computing empowers to get to the information from anyplace utilizing Internet. Security of information is one of the serious issue in distributed computing. Because of centralization of information, the information on the cloud server is progressively inclined to hazard and assaults. Security of information is additionally influenced due to multitenant condition. In multitenancy assets are shared among clients [3]. This can be likewise be utilized for versatile and substantial dimension applications. Solid safety efforts must be utilized to deal with such difficulties.

A. Cloud service models

Cloud computing offers a vast assortment of administrations to its clients. The clients can utilize these administrations on the web and they need to pay for what they use. In this segment we will examine different administration models of cloud.

I. Infrastructure as a Service (IaaS)

It is utilized for capacity, organizing and different other figuring assets. It offers access to web engineering, for example, servers, stockpiling, programming and associations. Here both devoted and focal assets are imparted to contracted customers to decrease the underlying expense of setting up the cloud which spares an immense measure of cash from introducing separate servers, preparing power and systems administration gadget. The primary favorable position here is to include or expel any application easily and savvy way [4]. Regardless of cost IaaS gives just the fundamental security and we require a more elevated amount of safety efforts for application moving into the Cloud. IaaS gives an expanded measure of

security control to the client. PaaS and SaaS Clouds are a layer overlaid on IaaS.

Example: -Amazon EC2 and Rock Space Cloud.

II. Software as a Service (SaaS)

SaaS is the upper most layers in the Cloud stock, which encases the product/applications for the clients. In SaaS, we don't compose our very own application program yet we use another person's application. SaaS has the base client control on security. The benefit of SaaS is that there is no compelling reason to introduce any product on their PCs and neither the weight of upkeep of programming. Administrations, for example, programming for working framework, databases, servers, arrange access, power and server farm space, and so forth are shrunk by the CSP[5].

Example: - Web-based Email, Gmail and Sales Force.

III. Platform as a Service (PaaS)

PaaS is utilized for the application made by the client. Here applications are situated without the requirement for overseeing and purchasing the equipment and programming. It is a conveyance of a Computing stage over the Web. PaaS demonstrate offers more prominent extensibility and more prominent client control on security than SaaS however not as much as that of Iaas. It gives the arrangement stock required by the clients to manufacture their very own applications and sort out their very own information.

Example: - use of programming languages such as Python, Java which is supported by the provider and Google Apps.

Figure 1 shows the deployment models and service model in cloud computing environment.

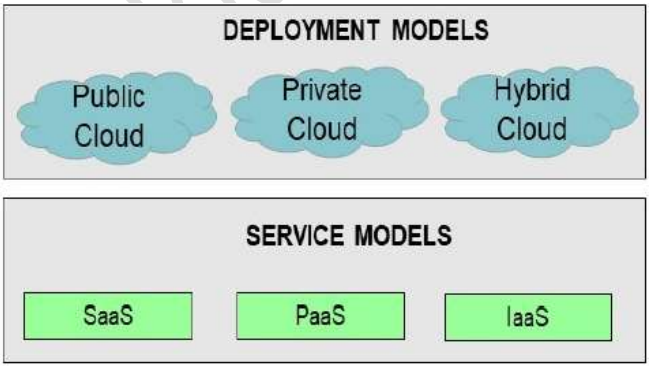

Fig.1. Cloud Computing solution based on deployment and service models

B. Cloud Deployment Models

The deployment model tells the nature of cloud. Consistency of data is achieved by resource sharing.

I. Public Clouds

At the point when the cloud administrations are given over a system that is open for open use, it is called open cloud. Open cloud specialist organizations utilize the web to give assets, for example, stockpiling and application on an open cloud. Here the Cloud foundation is worked by any outsider specialist co-ops or any outside association. A few instances of open mists are: - Sun cloud, Amazon web services, Oracle, Google app engine and Microsoft etc.,

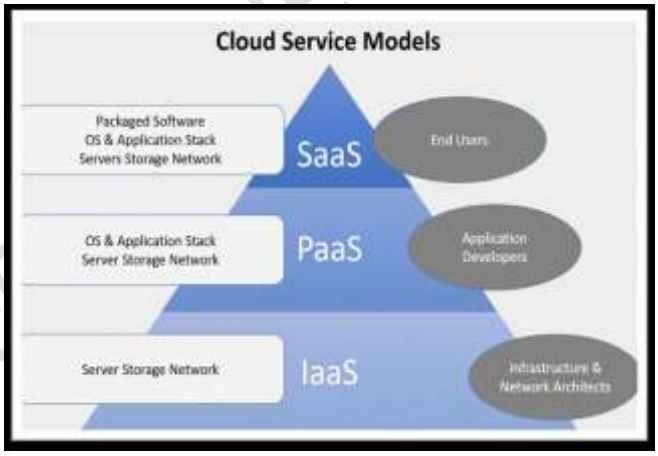

Fig.2.The Basic Cloud Service Models.

II. Private Clouds

In Private Cloud the Cloud framework is worked only for a solitary association. It is more anchored in view of its interior utilization as just determined clients and possess association can get to the administrations given by the Cloud foundation. Private mists can be costly with regularly unobtrusive economies of scale [6].

III. Hybrid Clouds

A Hybrid Cloud is any mix of at least two particular cloud framework. It might be a private cloud and at least one open cloud. There ought to be assets shared among the mists. Example: -Cloud Bursting.

IV. Community Clouds

A Community Cloud is explicitly intended to meet the characterized needs of a Community. It very well may be overseen, worked and claimed by at least one association

in the Community, a blend of them or a third part. Outsider specialist co-op chiefs the common plan of framework which is assigned by a few associations [5]. Network cloud can be considered as the bunch of private mists [4].

II. RELATED WORK

The security state has been and as of now is generally talked about in both the business and the scholarly community. A few global meetings have concentrated regarding this matter alone, for example, the ACM Workshop on Cloud Computing Security, the International Conference on Cloud Security Management, and the main European gathering regarding the matter, Secure Cloud, which previously had three versions. Subsequently, a few logical commitments have been distributed on gatherings procedures, as well as in global diaries. Accordingly, a few reviews on this subject matter have additionally been distributed, which will be depicted in this segment.

Zhou et al. [7] explained a study on the security and protection worries of many distributed computing suppliers. Security and protection were talked about exclusively. While the first was concentrated with spotlight on accessibility, secrecy, uprightness, control and evaluating attributes, the second was talked about by posting outof-date protection acts. What's more, a couple of issues related with multi-area stockpiling were likewise talked about.

Vaquero et al. [8] gave profound knowledge into IaaS mists security. The investigation concentrated on the security issues that multi-occupancy conveys to distributed computing while at the same time examining them from the Cloud Security Alliance (CSA) perspective, that is, by sorting security ponders as indicated by the CSA top dangers to distributed computing distributed in 2010. Their work included portraying security from the systems administration, virtualization and physical sides of cloud IaaS systems.

Subashini and Kavitha [9] explicitly examined the administration conveyance models security. In the wake of examining the security in the extent of the few models, they dissected them independently, bringing up a more noteworthy number of issues in the SaaS show. An outline of current security arrangements detailed in the writing was likewise exhibited in that article.

Ahuja and Komathukattil [10] introduced an overview on some normal dangers and related dangers to mists. Ways to deal with handle those dangers and dangers and security models of driving cloud suppliers were additionally exhibited.

Rodero-Merino et al. [11] have given an overview on the security state in PaaS cloud conditions. They have concentrated on sharing-based stages, concentrating on the .NET and Java ones with accentuation on seclusion, asset bookkeeping and safe string end properties of the stages.

Xiao and Xiao [12] gave a methodical audit of security issues in mists dependent on a property driven system. The qualities utilized were classification, uprightness, accessibility, responsibility and security preservability. For each characteristic, a couple of dangers were checked on alongside the relating guard arrangements.

Aguiar et al. [13] composed a book part concentrating on the subjects of registering and capacity as to distributed computing security. The examination diagramed a few issues traversing different themes and ongoing advancements with respect to server stockpiling and information calculation security. Such subjects incorporate confirmation and approval, virtualization, web administrations, responsibility, and accessibility. At that point, the discourse puts accentuation on procedures and components for accomplishing appropriate bookkeeping, stockpiling security, and open undeniable nature on re-appropriated information and calculation.

Pearson [14] gave a thorough book part relating the protection, security and trust properties of distributed computing. The section presents essential ideas, however centers for the most part around talking about the present

security condition of cloud frameworks. For that reason, security issues and related countermeasures are incorporated into the work.

Pearce et al. [15] explained a broad review for the virtualization area in a stage autonomous way, and especially on the security issues around it. Their work initially clarifies the nuts and bolts of virtualization to then portray an expansive engineering for framework virtualization, with accentuation on system virtualization. The examination talked about the error with respect to presumptions of secure framework separation, oversight and duplication, and introduced dangers coming about because of solid virtualization properties and from powerless execution of center virtualization necessities. Suggestions for securer virtualization usage were additionally passed out.

Survey	Year	Topics Focused	Security Landscape	Industry References	Security Incidents	Security Issues	Solut.	Summary
Zhou et al. [312]	2010	industry technologies, legal problems, privacy acts	✖	-	-	+	++	✖
Vaquero et al. [296]	2011	IaaS clouds, networking, virtualization, physical	✖	+	✖	+	✖	✓
Subashini and Kavitha [263]	2011	software, Internet, web, storage, access	✖	-	✖	++	+	✖
Ahuja and Krishnakutti [3]	2012	software, perimeter, virtualization, compliance, access, storage	✖	-	✖	++	-	✖
Rodero-Merino et al. [216]	2012	PaaS clouds, isolation, resource accounting and safe thread termination	✖	✖	✖	+	+	✓
Xiao and Xiao [302]	2013	confidentiality, integrity, availability, accountability, privacy-preservability	✖	✖	✖	++	++	✓
Aguiar et al. [2]	2013	access, virtualization, availability, accountability, storage, computation	✖	✖	✖	++	+	✖
Pearson [213]	2013	privacy, trust, legality, laws, compliance, access, storage, software, virtualization	++	++	✖	++	+	✖
Pearce et al. [212]	2013	IaaS clouds, virtualization, hypervisors, virtualized networking	✖	+	✖	+	+	✓
Perez-Botero et al. [214]	2013	IaaS clouds, hypervisors, vulnerabilities	✖	+	✖	+	+	✓
This survey	—	several cloud-related security topics	✓	✓	✓	✓	✓	✓

Table 1 Comparison of the related works with the survey presented herein regarding the security landscape, industry references, security incidents and issues, solutions and summary effort.

Perez-Botero et al. [16] have given an arrangement of vulnerabilities on the Xen and Kernelbased Virtual Machine (KVM) hypervisors with premise on the open-source knowledge accessible in different weakness databases, including the National Vulnerability Database (NVD) and SecurityFocus. Their work centers around three proposed fronts: the hypervisor usefulness, the trigger source, and the assault target. Breakdowns for the vulnerabilities found are incorporated into the article. The security scene concerning mists is wide and the past works center around explicit zones, giving careful consideration to the job that mists play in IT and cybersecurity, however supporting in some cases the profundity of the specialized depiction of the answers for the issues. Table 1 looks at the few previously mentioned works for various viewpoints, in particular the points they are engaged in, the consideration of industry references, the depiction of answers for the issues and the incorporation of a combination towards the end. A few images are utilized in the table pass on various implications. For example, a ✓ is used to denote that a given aspect is covered in the article, while + or ++ are used to emphasize that particular attention is paid to a specific subject. On the other hand, a less detailed discussion on a given aspect is denoted by a –, while ✖ is used to denote aspects not covered in the surveys.

The study presented herein differs from previous works for its broader scope. Rather than paying particular attention and detailing too much over the issues, a broader perspective of the state-of-the-art and high level description is provided. Because of this, it is the only work proposing a taxonomy for the wide security landscape. This work also shows a concern in including pointers to real security incidents for each topic, which is not typically seen in other works. Furthermore, an analysis about the discussion of the security issues[17] is provided at the end of the article, so as to deliver a series of guidelines and recommendations for future work and a discussion on an ideally secure cloud environment. This comprehensive study enables one to quickly catch-up basic concepts, review and understand the current security panorama of current cloud systems, analyze which security issues need to be addressed and, consequently, identify opportunities for future research work. In addition, an analysis of the number and type of publications on the field throughout the years was presented in the previous section. For the sake of consistency, like in

other works, the survey is complemented with key concepts of the cloud computing technology and its security state.

III. STORAGE TECHNIQUES IN CLOUD COMPUTING

In this segment different existing methods has been talked about. Distributed storage is viewed as an arrangement of dispersed server farms that for the most part Utilize virtualization innovation and supplies interface for information stockpiling.

3.1 Implicit Storage Security to Data in Online

Giving understood capacity security to information in online is increasingly gainful in a distributed computing. The utilization of an information dividing plan for executing such security including the underlying foundations of a polynomial in limited field.

In this plan information is divided in such way that each bit is certainly secure and does not to be encoded. These segments are put away on various servers on the system which are known just to the client. Recreation of the information expects access to every server and the learning about which servers the information partition are put away. A few adaptations of this plan are depicted, which incorporate the understood stockpiling of encryption keys instead of the information and where a subset of the segment might be united to reproduce the data[18].

3.2 Identify –Based Authentication

An identify based encryption (IBEA perceive based encryption (IBE) and deciphering and identity based stamp IBS anticipates IBHMCC. Resources and organizations are scattered over different buyer. So there is a chance of various security risks. Thusly affirmation of customers similarly as organizations is a basic need for cloud security.

Exactly when SSH Authentication tradition (SAP)was used to cloud, it ends up being incredible. As a decision to SAP, proposed another affirmation tradition subject to identity which relies upon dynamic model with contrasting imprint and encryption scheme. Perceive based approval tradition forces progression of steps. In step(1) the client C sends the servers a client Hello message. The message contains a fresh discretionary number Cn.session identifier ID and c assurance. In step (2) the server S responds with a server Hello message which contains new fresh unpredictable number Sn.

3.3 Public Auditing with Complete Data Dynamic Support

Check of information honesty at questionable servers is the real worry in distributed storage with open review capacity confided in element with aptitude and abilities information proprietors don't groups can be appointed as an outer review gathering to get to the danger of redistributed information when required. It likewise gives a straightforward yet financially savvy technique for information proprietors to pick up trust in the cloud.

To achieve, dynamic information bolster, the existent edit of PDF (or) POR conspire is enhanced by ridiculing the fundamental Markel Hash tree (MHT).

3.4 Efficient Third Party Auditing (TPA)

Cloud customers spare information in cloud server with the goal that security just as information stockpiling accuracy is essential concern.

The information proprietors having enormous measure of re-appropriated information and the tak of examining the information accuracy in a cloud domain can be troublesome and costly for information proprietors.

To help outsider examining where client securely delegate in respectability checking undertakings to outsider auditors(TPA)this plan can nearly ensure the synchronous restriction of information error(ie the ID of getting rowdy servers).

A tale and homogeneous structure is acquainted with give security to various cloud types. To accomplish information stockpiling security ,BLS(Bonch-Lynn-Sachems)algorithm is accustomed to marking the information hinders before redistributing information into cloud. Reed Solomon strategy is utilized for blunder amendment and to guarantee information stockpiling correction [18].

3.5 Way of Dynamically Store Data in Cloud

Data storage is cloud may not be absolutely trustable in light of the way that the clients did not have

neighborhood copy of data secured in cloud. To address these issues proposed another tradition system using the data scrutinizing tradition estimation to check the data dependability organizations providers drive the clients to chenk the data security by the proposed feasible modified data examining computation. A versatile passed on accumulating dependability assessing framework (FDSIAM)[18],these instrument utilizes the homomorphism tokens, blocking erasure and unblocking factors and flowed destruction coded data.

3.6 Effective and Secure Storage Protocol

Current example is customers redistributing data into pro center who have enough area for limit with lower accumulating cost. A secured and capable amassing tradition is prescribed that guarantees the data storing protection and uprightness. This tradition is structured by using the advancement of elliptic curve cryptography and quiet gathering is used to avow the data reliability. Data and programming process tradition step executed by cloud customers to add the security prerequisite structure to the item and data before trading them to the cloud. Test response tradition is tradition is affirmation with the objective that it won't revealed the substance of the data to pariahs. Data dynamic exercises are moreover used keep a comparable security assertion and besides offer easing to customers from the troublesome of data spillage and corruptions issues.

3.7 Optimal cloud storage systems:

Cloud data storage which requires no effort is increasing more prominent reputation for individual, adventure and foundations data support and synchrozation. The proposed structures depict, at an irregular express, a possible plan for a cryptographic amassing organization. At is focus, the plan contains there portions, a data processor(DP)that frames data before it is sent to the cloud a data verifier(DV)that checks whether the data in the cloud has been wrecks with, and a token generator(TG)that generator tokens which enables the dispersed stockpiling providers to recoup areas of customer data.

IV.TECHNIQUES TO SECURE DATA IN CLOUD

4.1 Authentication and Identity

Authentication of users and even of conferring structures is performed by various systems, anyway the most outstanding is cryptography [19]. Check of customers occurs in various courses like as passwords that is referred to independently, as a security token, or in the shape a quantifiable sum like remarkable stamp. One issue with using ordinary character approaches in a cloud circumstance is defied when the undertaking uses different cloud expert communities (CSPs)[19]. In such a use case, synchronizing character information with the endeavor isn't adaptable. Diverse issues rise with standard identity approaches while pushing structure toward a cloud-based course of action.

4.2 Data Encryption

In the event that you are intending to store touchy data on a substantial information store then you have to utilize information encryption systems. Having passwords and firewalls is great, yet individuals can sidestep them to get to your information. At the point when information is encoded it is in a shape that can't be perused without an encryption key. The information is absolutely futile to the interloper. It is a procedure of interpretation of information into mystery code. On the off chance that you need to peruse the scrambled information, you ought to have the mystery key or secret phrase that is likewise called encryption key.

4.3 Information integrity and Privacy

Cloud computing gives data and assets to substantial clients. Assets can be gotten to through internet browsers and can likewise be gotten to by malevolent aggressors [20]. An advantageous answer for the issue of data honesty is to give shared trust among supplier and client. Another arrangement can be giving legitimate validation, approval and bookkeeping controls so the way toward getting to data ought to experience different multi dimensions of checking to guarantee approved utilization of assets [20]. Some anchored access systems ought to be given like RSA authentications, SSH based passages.

4.4 Availability of Information (SLA)

Non accessibility of data or information is a noteworthy issue in regards to distributed computing administrations. Administration Level understanding is utilized to give the data about whether the system assets are accessible for clients or not. It is a trust bond among shopper and supplier [20].An approach to give accessibility of assets is to have a reinforcement plan for nearby assets just as for most significant data. This empowers the client to have the data about the assets even after their inaccessibility.

4.5 Secure Information Management

It is a procedure of information security for a gathering of data into central store. It is contained administrators running on systems that are to be watched and after that sends information to a server that is assigned "Security Console". The security bolster is regulated by overseer who is an individual who reviews the information and takes exercises in light of any alerts. As the cloud customer base, dependence stack increase, the cloud security frameworks to enlighten security issues in like manner augment, this makes cloud security the officials altogether increasingly tangled. It is in like manner implied as a Log Management. Cloud providers moreover give some security standards like PCI DSS, SAS 70[20]. Information Security Management Maturity is another model of Information Security Management System.

4.6 Malware-injection attack solution

This course of action makes a no. of client virtual machines and stores all of them in a central accumulating. It utilizes FAT (File Allocation Table) involving virtual working systems[21]. The application that is constrained by a client can be found in FAT table. All of the events are administered and arranged by Hypervisor. IDT (Interrupt Descriptor Table) is used for reliability checking.

4.7 Flooding Attack Solution

All of the servers in cloud are considered as a naval force of servers. One fleet of server is considered for structure type requests, one for memory the administrators and last one for focus estimation related occupations. All of the servers in naval force can talk with one another. When one of the server is over-load, another server is brought and used in the place of that server and an another server that is called name server has all the record of current states of servers and will be used to invigorate objectives and states. Hypervisor can be used for administering jobs [21]. Hypervisor in like manner do the endorsement and approval of occupations. An affirmed customer's interest can be perceived by PID. RSA can in like manner be used to encode the PID.

V. CLOUD COMPUTING SECURITY STANDARDS

Standards for security describe strategy and methods for realizing a security program. To keep up an ensured area, that gives insurance and security some specific advances are performed by applying cloud related activities by these measures. A thought called "Assurance in Depth" is used in cloud to give security [22]. This thought has layers of opposition. Thusly, if one of the structures misses the mark, covering system can be used to give security as it has no single reason for dissatisfaction. Generally, endpoints have the system to care for security, where get to is obliged by customer.

5.1 Security Assertion Markup Language (SAML)

SAML is basically used in business can anticipate secure correspondence between online accessories. It is a XML based standard used for approval, endorsement among the assistants. SAML describes three employments: the key (a customer), an authority association (SP) and an identity provider (IDP) [22]. SAML gives request and responses to decide customer characteristics endorsement and approval information in XML structure. The requesting gathering is an online page that gets security information.

5.2 Open Authentication (OAuth)

It is a technique utilized for interfacing with secured information. It is essentially used to give information access to designers. Clients can allow access to data to engineers and purchasers without sharing of their personality [22]. OAuth does not give any security without anyone else in actuality it relies upon different conventions like SSL to give security.

5.3 Open ID

Open ID is a solitary sign-on (SSO) technique. It is a typical login process that enables client to login once and after that utilization all the taking part frameworks [22]. It doesn't founded on focal approval for verification of clients.

5.4 SSL/TLS

TLS is utilized to give secure correspondence over TCP/IP. TLS works in essentially three stages: In first stage, arrangement is done between customers to recognize which figures are utilized. In second stage, key trade calculation is utilized for verification [22]. These key trade calculations are open key calculation. The last and third stage includes message encryption and figure encryption.

VI.CONCLUSION

Cloud computing is another computational perspective that offers on innovative arrangement of activity for relationship to grasp It without direct hypothesis. Conveyed figuring moves the application programming and database to the broad server cultivate where the data the administrators and organization may not be totally exemplary. The security is a basic piece of nature of organization. Disseminated stockpiling is generously progressively productive and focal points then the earlier standard limit structure especially in flexibility, cost decline, convenientce and handiness need. we have discussed some of them and moreover the strategies to prevent them, they can be used to keep up the protected correspondence and clear the security issues. This audit is basically done to consider all of the issues like strikes, data hardship and unauthenticated access to data and moreover the systems to remove those issues. As the disseminated processing is dynamic and complex, the customary security courses of action given by cloud condition don't framework to its virtualized environment. This paper showed a survey on limit technique in appropriated figuring a couple of accumulating framework that offer security to data in cloud have been analyzed in nuances.

REFERENCES

[1]. Shahin Fatima, Shish Ahmad, Shadab Siddiqui,: "Security Issues In Cloud Computing :A Survey",International Journal of Advanced Research in Computer Science (ISSN: 0976-5697) CONFERENCE PAPER, Volume 9, Special Issue No. 2, April 2018, ISBN: 978-93-5311-643-9

[2]. NIST defmition of Cloud. NIST 500-292 "NIST Cloud Computing Reference Architecture"

[3]. Abdul Muttalib Khan , Dr. Shish Ahmad , Mohd. Haroon, "A Comparative Study of Trends in Security in Cloud Computing", 2015 Fifth International Conference on Communication Systems and Network Technologies, IEEE 2015.

[4].Prof.(Dr.) Pradeep Kumar Sharma, Prof.(Dr.) Premala Shankar Kaushik, Payal Jain, Shivangi Agarwal, Kamlesh Dixit – Issues and Challenges of Data Security in a Cloud Computing Environment. Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017.

[5]. T. Saxena, V. Chourey, "A Survey Paper on Cloud Security Issues and Challenges", 20 14 IEEE.

[6].Wg Cdr Nimit Kaura, Lt Col Abhishek Lal-Survey Paper on Cloud Computing Security. International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017.

[7]. Zhou, M., Zhang, R., Xie, W., Qian, W., Zhou, A.: Security and Privacy in Cloud Computing: A Survey. In: 6th Int. Conf. on Semantics Knowledge and Grid, pp. 105{ 112. IEEE Computer Society, Washington, D.C., USA (2010).

[8]. Vaquero, L.M., Rodero-Merino, L., Moran, D.: Locking the sky: a survey on IaaS cloud security. Computing 91(1), 93{118 (2011). DOI 10.1007/s00607-010-0140-x.

[9]. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(1), 1{11 (2011). DOI 10.1016/j.jnca.2010.07.006.

[10]. Ahuja, S.P., Komathukattil, D.: A Survey of the State of Cloud Security. Network and Communication Technologies 1(2), 66{75 (2012). DOI 10.5539/nct.v1n2p66.

[11]. Backstrom, L., Dwork, C., Kleinberg, J.: Wherefore Art Thou R3579X?: Anonymized Social Networks, Hidden Patterns, and Structural Steganography. In: Proc. of the 16th

Int. Conf. onWorld WideWeb, pp. 181{190. ACM, New York, NY, USA (2007). DOI 10.1145/1242572. 1242598.

[12]. Xiao, Z., Xiao, Y.: Security and Privacy in Cloud Computing. IEEE Commun. Surveys Tuts. 15(2), 843{859 (2013). DOI 10.1109/SURV.2012.060912.00182.

[13]. Aguiar, E., Zhang, Y., Blanton, M.: An Overview of Issues and Recent Developments in Cloud Computing and Storage Security, pp. 1{31. Springer (2013).

[14]. Pearson, S.: Privacy, Security and Trust in Cloud Computing. In: S. Pearson, G. Yee (eds.) Privacy and Security for Cloud Computing, pp. 3{42. Springer London (2013). DOI 10.1007/978-1-4471-4189-1.

[15]. Pearce, M., Zeadally, S., Hunt, R.: Virtualization: Issues, Security Threats, and Solutions. ACM Comput. Surv. 45(2), 17:1{17:39 (2013). DOI 10.1145/2431211.2431216.

[16]. Perez-Botero, D., Szefer, J., Lee, R.B.: Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers. In: Proc. of the 2013 Int.Workshop on Security in Cloud Computing (SCC), pp. 3{10. ACM, New York, NY, USA (2013). DOI 10.1145/2484402.2484406

[17]. Garima Gupta, P.R.Laxmi and Shubhanjali Sharma. : A Survey on Cloud Security Issues and Techniques.

[18]. T. Sivashakthi, Dr. N Prabakaran,: A Survey on Storage Techniques in Cloud Computing, International Journal of Emerging Technology and Advanced Engineering,(ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 12, December 2013).

[19]. Yashpalsinh jadeja & kirti modi (2012) cloud computing- concepts, architecture and challenges.

[20]. Akhil Behl & Kanika Behl (2012), An Analysis of Cloud Computing Security Issues.

[21]. R. Balasubramanian, Dr.M.Aramuthan (2012) Security Problems and Possible Security Approaches In Cloud Computing.

[22]. Wang Q,Wang C et al(2011).Enabling Public auditability And Data Dynamics For Storage Security in Cloud Computing, IEEE Transactions On Parallel and Distributed Systems,Vol22(5),847-859.