A Review on Data Protection of Cloud Computing Security, Benefits, Risks and Suggestions

Guddu Kumar
M.Tech, Computer Science & Engineering, VIT, RKDF University, Bhopal, India

***Abstract*—** While cloud computing is picking up notoriety, various security and protection issues are developing that ruin the fast reception of this new computing worldview. What's more, the advancement of protective arrangements is lingering behind. To guarantee a safe and dependable cloud condition it is fundamental to recognize the restrictions of existing arrangements and imagine bearings for future research. Cloud computing changed our general surroundings. Presently individuals are moving their information to the cloud since information is getting greater and should be available from numerous gadgets. In this manner, putting away the information on the cloud turns into a standard. In any case, there are numerous issues that counter information put away in the cloud beginning from virtual machine which is the intend to share assets in cloud and completion on cloud stockpiling itself issues. In this paper, we present those issues that are keeping individuals from receiving the cloud and give a study on arrangements that have been done to limit dangers of these issues. For instance, the information put away in the cloud should be classified, safeguarding honesty and accessible. In addition, sharing the information put away in the cloud among numerous clients is as yet an issue since the cloud specialist organization is dishonest to oversee confirmation and approval. In this paper, we list Cloud computing security, Benefits, Risks and suggestions for data security.

***Keywords*—** cloud computing, data security, security

I. INTRODUCTION

Cloud computing is an informal articulation used to depict a wide range of computing ideas that include countless PCs that are associated through an ongoing correspondence arrange (normally the Internet).[1] Cloud computing is a language term without a generally acknowledged non-uncertain logical or specialized definition. In science, cloud computing is an equivalent word for conveyed computing over a system and means the capacity to run a program on many associated PCs simultaneously. The prevalence of the term can be ascribed to its utilization in advertising to sell facilitated benefits in the feeling of use administration provisioning that run customer server programming on a remote area.

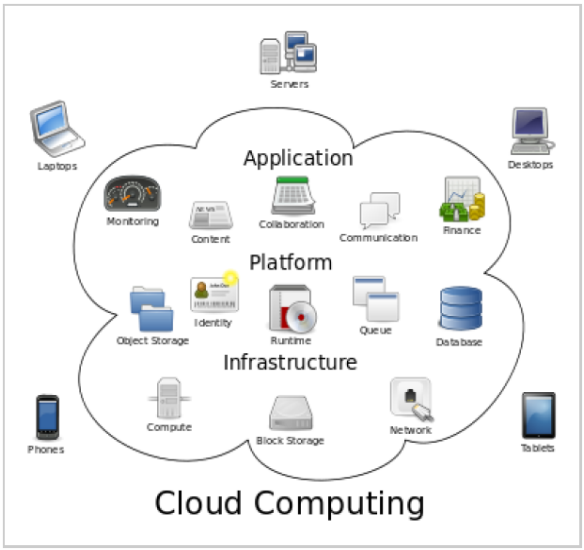

Fig 1. Cloud computing logical diagram

II CLOUD COMPUTING STRUCTURE

One of the most important parts of cloud computing strategy is the coming of cloud stages. As its name recommends, this kind of stage enables designers to compose applications that keep running in the cloud, or use administrations given by the cloud, or both. It is otherwise called on-request stage and stage as an administration (PaaS). The distinction between how application stages are utilized today and cloud stages is that when an advancement group makes an on-premises application (for example one that will keep running inside an association), it just needs to compose a source-code in some kind of programming language.

In the event that the makers of each on-premises application initially needed to manufacture the majority of the supporting software that is, directly from the working frameworks to the constructing agent who unravels the program, then we would have less applications in presence today. Also, if each advancement group that desires to make a cloud application should initially assemble its own cloud stage, we would not see many cloud applications either.

Fortunately, there are a few cloud stage innovations accessible today [2] permitting whole organizations and a large number of representatives to run their computing needs as online leased instruments. The majority of the preparing and record sparing will be

performed in the cloud, and the clients will connect to that cloud each day to do their computing work [3]. Cloud computing has three noteworthy premises:

1. Software as a Service
2. Platform as a Service
3. Infrastructure as a Service

1. Software as a Service

Software as a Service (SaaS) is software appropriations model in which applications are facilitated by a merchant or specialist organization and are made accessible to clients over a system, normally the Internet.

SaaS is turning into an inexorably common administration conveyance model as fundamental advancements that help web administrations and Service Oriented Architecture (SOA) develop, and new formative approaches, for example, Ajax become well known. In the mean time, broadband administration has turned out to be all the more generally accessible to help client access from more areas around the globe.

SaaS is firmly identified with the Application Service Provider (ASP) and the on-request software conveyance models. IDC recognizes two somewhat extraordinary conveyance models for SaaS [4].

The facilitated Application Management (AM) model is like ASP: a supplier has industrially accessible software for clients and conveys it on the Web.

Utilizing the software on-request model, the supplier gives clients arrange based access to a solitary duplicate of an application made explicitly for SaaS circulation. Advantages of the SaaS model include:

- Easier administration
- Automatic updates and patch management
- Compatibility
- Easier collaboration

2. Platform as a Service

Platform as a Service (PaaS) is an approach to lease equipment, working frameworks, stockpiling, and system limit on the Internet. The administration conveyance model permits the client the capacity to lease virtualized servers and related administrations for running existing applications or creating and testing new ones. PaaS is an outgrowth of SaaS, and it is software conveyance model in which facilitated software applications are made accessible to clients on the Internet.

PaaS has a few focal points for designers where working framework highlights might be changed and redesigned much of the time. Topographically appropriated advancement groups may cooperate on software improvement ventures. Administrations might be gotten from various sources that cross global limits. Starting and continuous expenses might be decreased using foundation administrations from a solitary merchant rather than keeping up numerous equipment offices that often perform copy capacities or that experience the ill effects of contrariness issues. Generally, costs may likewise be limited by binding together advancement endeavors [4].

On the disadvantage, PaaS involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

3. Infrastructure as a Service

Infrastructure as a Service (IaaS) once in a while is alluded to as hardware as a service. It is an arrangement model in which an organization re-appropriates the gear used to help operations, including storage, hardware, servers, and systems administration components. The service provider owns the equipment and is responsible for housing, running and maintenance. The client typically pays on a per-use basis. The characteristics and components of IaaS include:

- Value computing service and billing model.
- Computerization of administrative tasks.
- Dynamic scaling.
- Policy-based services.
- Internet connectivity.

Clouds may also be divided into:

1. public: existing widely - any group may subscribe
2. private: facilities built according to cloud computing principles, but accessible only within a private network
3. partner: cloud services offered by a provider to a limited and well-defined number of parties.

In general, the commodity, cost, liability and assurance of clouds vary according to the following figure:

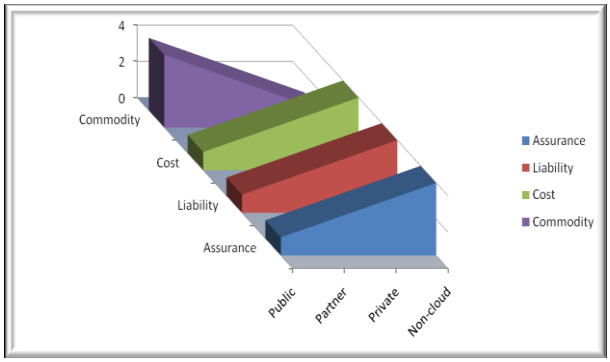

Fig 2. Feature of Public, Partner & Private Clouds

4. Other Services Offered by Cloud Computing

There are also some other services offered by cloud computing that include:

• Data as a Service (DaaS): The user's queries against the provider's data base.

• Identity and Policy Management as a Service (IPMaaS): The provider manages identity and/or access control policy for consumer

• Network as a Service (NaaS): The provider offers virtualized networks like a VPN

III. CLOUD COMPUTING SECURITY

In cloud computing, end clients' information put away in the administration

supplier's server farms as opposed to putting away it on client's PC. This will make clients worried about their security.

In addition, moving to brought together cloud services will bring about client's protection and security breaks as examined in [5].

Security dangers may happen during the arrangement; additionally, new dangers are probably going to come into view.

Cloud condition should protect information respectability and client security alongside improving the interoperability over numerous cloud administration suppliers. Accordingly, we might want to examine information trustworthiness, secrecy and accessibility in the cloud. The security identified with information conveyed on three levels in [5]:

Network Level:

The Cloud Service Provider (CSP) will screen, keep up and gather data about the firewalls, Intrusion identification or/and counteractive action frameworks and information stream inside the network.

Host Level:

It is essential to gather data about framework log records. So as to know where and when applications have been logged.

Application Level:

Reviewing application logs, which at that point can be required for episode reaction or advanced criminology. At each level, it is required to fulfill security prerequisites to save information security in the cloud, for example, classification, trustworthiness and accessibility as follows:

A. Confidentiality

Ensuring that client information which dwells in the cloud can't be gotten to by unapproved party. This can be accomplished through legitimate encryption methods thinking about the sort of encryption: symmetric or uneven encryption calculations, likewise key length and key administration if there should arise an occurrence of the symmetric figure. As a matter of fact, it is altogether founded on the CSP. For example, in [5], Mozy Enterprise utilizes encryption strategies to ensure client information while Amazon S3 does not. It additionally relies upon the client mindfulness where they can encode their data preceding transferring it. Likewise, The CSP ought to guarantee appropriate organization of encryption principles utilizing NIST gauges in [6].

B. Integrity:

Cloud clients ought not just stress over the privacy of information put away in the cloud yet in addition the information respectability. Information could be encoded to give secrecy where it won't ensure that the information has not been changed while it is living in the cloud. Chiefly, there are two methodologies which give uprightness, utilizing Message Authentication Code (MAC) and Digital Signature (DS). In MAC, it depends on symmetric key to give a check total that will be attach to the information. Then again, in the DS calculation it relies upon the open key structure (Having open and private pair of keys). As symmetric calculations are a lot quicker than topsy-turvy calculations, for this situation, we accept that Message Authentication Code (MAC) will be the best answer for give the respectability checking component. Studies demonstrate that, PaaS and SaaS doesn't give any honesty insurance, for this situation guaranteeing the uprightness of information is basic.

C. Availability:

Another issue is accessibility of the information when it is mentioned through approved clients. The most dominant method is counteractive action through

maintaining a strategic distance from dangers influencing the accessibility of the administration or information. It is exceptionally hard to identify dangers focusing on the accessibility. Dangers focusing on accessibility can be either Network based assaults, for example, Distributed Denial of Service (DDoS) assaults or CSP accessibility. For instance, Amazon S3 experienced more than two hours' blackout in February 2008 and eight hours' blackout in July 2008. In the following segment, we will talk about the personality and access the board practices of the cloud computing by handling a few conventions, for example, Security Assertion Markup Language (SAML), Open Authentication (OAuth) convention and an examination between these two procedures to finish up the best solution.

IV. SECURITY BENEFITS OF CLOUD COMPUTING

It is not really important to rehash the many downpour backwoods of material which has been composed on the financial, specialized and structural and environmental advantages of distributed computing. Notwithstanding, in the immediate experience of the individuals from our expert gathering, just as per late news from 'this present reality', an assessment of the security dangers of distributed computing must be adjusted by a survey of its particular security benefits. Distributed computing can possibly improve security and versatility. What pursues is a portrayal of the key manners by which it can contribute.

Put essentially, a wide range of safety efforts are cheaper when actualized on a bigger scale. Hence, a similar measure of interest in security purchases better assurance. This incorporates a wide range of protective estimates, for example, separating, fix the board, solidifying of virtual machine occasions and hypervisors, HR and their administration and reviewing, equipment and programming repetition, solid validation, productive job based access control and united personality the board arrangements of course, which additionally improves the system impacts of coordinated effort among different accomplices associated with guard. Different advantages of scale include:

Multiple areas: most cloud suppliers have the monetary assets to recreate content in numerous areas as a matter of course. This builds repetition and autonomy from disappointment and gives a degree of debacle recuperation out-of-the-box.

Edge systems: stockpiling, preparing and conveyance closer to the system edge mean administration unwavering quality and quality is expanded generally and nearby system issues are less inclined to have worldwide reactions.

Improved practicality of reaction: bigger to occurrences: well-run bigger scale frameworks, for instance because of early recognition of new malware arrangements, can grow increasingly successful and effective episode reaction capacities.

Threat the executives: cloud suppliers can likewise bear to procure pros in managing explicit security dangers, while littler organizations can just manage the cost of few generalists.

The advantages of cloud computing can be reasonably accomplished by joining forces with cutting edge private cloud computing suppliers in a manner that doesn't endanger your organization's security. Here are 5 advantages of a top cloud computing security solution:

1. Protection against DDoS-Distributed disavowal of administration assaults are on the ascent, and a top cloud computing security arrangement centers around measures to stop tremendous measures of traffic went for an organization's cloud servers. This involves checking, retaining and scattering DDoS assaults to limit risk.

2. Data security-In the consistently expanding time of information ruptures, a top cloud computing security arrangement has security conventions set up to ensure delicate data and exchanges. This keeps an outsider from listening stealthily or messing with information being transmitted.

3. Regulatory compliance- Top cloud computing security arrangements help organizations in directed ventures by overseeing and keeping up upgraded frameworks for consistence and to ensure individual and money related information.

4. Flexibility- A cloud computing arrangement furnishes you with the security you need whether you're turning up or down limit. You have the adaptability to keep away from server crashes during high traffic periods by scaling up your cloud arrangement. At that point when the high traffic is finished, you can downsize down to lessen costs.

5. High accessibility and backing An accepted procedures cloud computing security arrangement offers consistent help for an organization's advantages. This incorporates live observing 24 hours per day, 7 days seven days, and each day of the year. Redundancies are worked in to guarantee your

organization's site and applications are constantly on the web.

A top-level cloud computing security arrangement gives organizations the accessibility, unwavering quality, and security they have to direct business in a worldwide commercial center. Propelled cybersecurity highlights join with physical framework to make a far reaching, secure answer for your cloud computing needs.

V. SECURITY BENEFITS OF RISK

1. The following points should be noted in relation to the descriptions of risk below:
2. Risk ought to consistently be comprehended in connection to by and large business opportunity and hunger for risk – some of the time risk is repaid by circumstance.
3. Cloud services are not just about advantageous capacity, available by various gadgets, however incorporate significant advantages, for example, increasingly helpful correspondence and moment multi-point coordinated effort. Consequently, a relative analysis needs to look at not just the risks of putting away information in better places (on premises v the cloud) yet in addition the risks when on premises-information put away on premises – for example a spreadsheet - is messaged to different people for their commitments, against the security issues of a spreadsheet put away in the cloud and open to joint effort between those people. Subsequently, the risks of utilizing cloud registering ought to be contrasted with the risks of remaining with conventional arrangements, for example, work area based models.
4. The level of risk will as a rule differ fundamentally with the sort of cloud engineering being considered.
5. It is workable for the cloud client to move risk to the cloud supplier and the risks ought to be considered against the money saving advantage got from the services. Anyway not all risks can be moved: if a risk prompts the disappointment of a business, genuine harm to notoriety or lawful ramifications, it is hard or incomprehensible for some other gathering to make up for this harm.
6. The risk analysis in this paper applies to cloud innovation. It doesn't have any significant bearing to a particular cloud figuring offering or organization. This paper isn't intended to supplant a venture explicit hierarchical risk evaluation.
7. The level of risks is communicated from the point of view of the cloud client. Where the cloud supplier perspective is considered, this is unequivocally expressed.

V. SUGGESTION FOR DATA SECURITY

With the expansion in information volumes, information taking care of has turned into all the rage. As associations move to the cloud, there is a higher accentuation guaranteeing everything is protected and secure, and that there is no risk of information hacking or ruptures. Since the cloud enables individuals to work without equipment and programming ventures, clients can pick up adaptability and information spryness. Be that as it may, since the Cloud is regularly shared between a ton of clients, security turns into a quick worry for Cloud owners.

Security Issues Within the Cloud:

Cloud merchants give a layer of security to client's information. In any case, it is as yet insufficient since the privacy of information can regularly be at risk. There are different kinds of assaults, which range from secret word speculating assaults and man-in-the-center assaults to insider assaults, shoulder surfing assaults, and phishing assaults. Here is a rundown of the security challenges which are available inside the cloud.

Data Protection and Misuse:

At the point when various associations utilize the cloud to store their information, there is regularly a risk of information abuse. To evade this risk, there is an up and coming need to verify the information stores. To accomplish this undertaking, one can utilize confirmation and limit access control for the cloud's information.

Locality:

Inside the cloud world, information is frequently appropriated over a progression of districts; it is very testing to locate the precise area of the information stockpiling. Be that as it may, as information is moved starting with one nation then onto the next, the standards administering the information stockpiling likewise change; this brings consistence issues and information security laws into the image, which relate to the capacity of information inside the cloud. As a cloud specialist co-op, the specialist organization needs to illuminate the clients regarding their information stockpiling laws, and the careful area of the data storage server.

Integrity:

The framework should be fixed in such a way so to give security and access limitations. At the end of the day, information access should lie with approved staff as it were. In a cloud situation, information

trustworthiness ought to be kept up consistently to stay away from any inborn information misfortune. Aside from confining access, the authorizations to make changes to the information ought to be restricted to explicit individuals, so that there is no far reaching access issue at a later stage.

Access:
Information security approaches concerning the entrance and control of information are fundamental over the long haul. Approved information proprietors are required to give part access to people so everybody gets just the required access for parts of the information put away inside the information bazaar. By controlling and confining access, there is a great deal of control and information security which can be imposed to guarantee maximums security for the put away information.

Confidentiality:
There is a ton of delicate information which may be put away in the cloud. This information must have additional layers of security on it to diminish the odds of breaks and phishing assaults; this should be possible by the specialist co-op, just as the association. Be that as it may, as a safety measure, information classification ought to be of most extreme need for delicate material.

Breaches:
Ruptures inside the cloud are not unheard. Programmers can rupture security parameters inside the cloud, and take the information which may somehow or another be viewed as secret for associations. In actuality, a rupture can be an interior assault, so associations need to lay specific accentuation in following representative activities to stay away from any undesirable assaults on put away information.

Storage:
For associations, the information is being put away and made accessible for all intents and purposes. Notwithstanding, for specialist co-ops, it is important to store the information in physical foundations, which makes the information defenseless and helpful for physical assaults.

These are a portion of the security issues which come as a piece of the cloud condition. Be that as it may, these are not actually hard to survive, particularly with the accessible degrees of mechanical assets nowadays. There is a ton of accentuation on guaranteeing greatest security for the put away information so it consents to the standards and guidelines, just as the association's inside consistence approaches.

VI. RELATED WORKS

Cloud computing has changed the IT idea into administration [7], [10], [11], [12], [14], [20] with building up a creative PC administration redemption model for the IT improvement necessity. It has improved IT execution capacities in the public eye and has remade every IT developments influencing the execution, unwavering quality, effectiveness, and security of the cloud information framework. Notwithstanding, as the highlights of Cloud Assignment models contrast broadly initiating the current usage of the specialist organization, which must be progressively worried about the information insurance frameworks.

Security is one of the real difficulties confronting the cloud condition. The 88% of cloud purchasers solicitation access to their information and solicitation more noteworthy thought to turns around, for example, conceivable cloud customers [8], [9], [18], [21] physical area, information the executives and security organization of their cloud information in virtual situations.

This demonstrates clients perceive clearness and security over cloud data. The specialist organization might be completely constrained by dealing with the cloud administration of a cloud administration, yet some cloud specialist co-ops don't enable the client to utilize cloud data in the cloud.

Wei Li et. al. [9] presents ‘Property Based Encryption (ABE)’ is viewed as a competent cryptographic administration device that guarantees direct control of the information proprietor on information in open cloud stockpiling.

The previous ABE tasks have the sole intensity of dealing with the whole property set, which gets one-point hindrances both security and execution. It runs a multi-exclusive CP-AE access control plan for open cloud stockpiling named TMACS, in which numerous officials together deal with the uniform properties. As far as possible multi-tyrant TMACS proposes the compelling usage of the customary multi-legitimate undertaking with TMACS.

This makes a half and half undertaking that is fitting in the genuine circumstance, in which the trademark sets comprise of various attributes and highlights from different specialists mutually play out the whole property subdivision. It doesn't clarify the explanations behind choosing the ace key for the objective incentive for shrouded sharing, include set, and focused on correspondence plan conventions.

V.Chang et. al [11] proposed a CCAF multi-layer security ensures ongoing information, and it has three layers of security: 1) 'firewall and access control'; 2) 'Distinguishing proof Management and Intervention Prevention', and 3) 'Transformation Encryption'. It has taken two arrangements of moral hacking tests in interest testing. The CCAF multi-layer security shields information from expedient information development in view of security abuses. This strategy gives ongoing assurance to every one of the information, forestalls more dangers and expels the methodical framework in the server farm and gives a far reaching clarification of cloud security upheld by an intelligible structure that influences the exhibition of client got to support, business procedure displaying. It very well may be additionally assessed progressively situations to quantify productivity.

M. Anisettiet. Al [10] gives an intense and durable assurance procedure dependent on confirmation, which totally resolves cloud prerequisites. The Authentication Scheme gives an answer for the administration of the endorsement lifecycle, which is a robotized and expanding technique for accreditation changing the cloud multi-layer and elements nature. Each bit of cloud carries on true to form and builds the certainty of cloud buyers as indicated by their necessities. This characterizes a computerized way to deal with dependability examination among prerequisites and models, in light of the chain's trust upheld by the affirmation plot. The task does not consider administration blends dependent on offshoot administration affirmation and cost-proficient accreditation to empower a confirmation based mix that supports cost streamlining in favor of Cloud Providers.

S. Linset. Al [13] constantly investigates dynamic affirmation prerequisites to guarantee secure and dependable cloud services and introduces solid cloud administration accreditations. Cloud administration frameworks and procedures are generally received, and utilitarian accreditation of cloud services is in fact and monetarily feasible. Most purchasers request straightforward, solid guaranteed cloud services, and the supplier can begin opening up for dynamic certifications.

Chi Chen et. Al [16] proposes a hunt instrument in the cipher text cloud stockpiling. It investigates the trouble of protecting a semantic relationship among different basic reports in connection to the encoded archives and gives a strategy to improve the exhibition of the semantic pursuit. The proposed strategy has a favorable position over the ordinary technique for positioning protection and the importance of the recovered records, as it breaks down hunt fitness and security underneath two appreciated risk designs. The work is centered uniquely around information security however the viability and availability of different inquiry clients are not talked about.

S. Wang et. Al [19] presents has overhauled the characteristic based information sharing system in cloud computing. Propelled key convention resolves real escrow issues. It presents the idea of articulation, gave to improve the trait articulation, which extends articulation from the double as well as decreases the multifaceted nature of access approach. KA and CSP administrators and noxious framework untouchables increment information protection and privacy in the cloud framework against semi-unwavering quality of the KA and CSP. What's more, improvement of trait articulation is an additional trademark, which cannot just depict the state qualities of the discretionary however lessens the intricacy of the confirmation strategy. Information protection and security are guaranteed in the proposition however information proprietors and information solicitation can't be evaluated by the trust. This should be possible to assess trust the board models for better cloud security.

Joseph K. Liu et. Al [17] gave a 'two-digit information assurance' report for a cloud insurance framework, which enables the sender of the information to shroud the beneficiary's data, however the beneficiary is his protection key and security to get client data. The arrangement expands the security of the data and gives a gadget recuperation, so that if the gadget is pulled back, the equal ciphertext won't be precisely identified by any information proprietor from the cloud server. The work centers to a great extent around the classification of information and gadget control, however it doesn't assess confided in clients and distorts the client reviews.

S.Subbalakshmi , Dr. K.Madhavi [22] Data protection and security are the fundamental worries of cloud computing. Huge information is an accumulation of huge volumes of information that can't be taken care of by customary design. To beat this, the Cloud Computing engineering is being utilized by numerous associations to store such volumes of information. Anyway the significant concern is in regards to information protection, security and access controls. In this paper, issues identified with information stockpiling security and access control are contemplated. The vast majority of the examination did on information security, protection access cloud in cloud condition. The present methodologies not

function admirably with enormous information. To deal with gigantic measure of information at any case, it expands issues identified with exchange of information, stockpiling support and access issues. Henceforth there is part of degree for research in improving information security, protection and access control.

VII. CONCLUSION AND FUTURE WORK

Cloud computing is growing quickly and is generally accepted to be the eventual fate of the calculation world. Along these lines, there are significant concerns, for example, security that should be tended to completely and inside and out so as to help this improvement. An investigation of the present circumstance demonstrates that the security level of present arrangements isn't at the level that would pull in new endeavors and persuade the ones previously concentrating the innovation to relocate from conventional calculation innovation to cloud computing.

Distinctive record frameworks have tended to the security issue at this point, however they don't appear to be a persuading answer for the issue. Indeed, even the real frameworks, for example, GFS and HDFS, both as of now being used by the biggest suppliers, for example, Google, give off an impression of being fragmented. In GFS/HDFS engineering, issues like that the Master server stores all the metadata related with the lumps and like this, lead the entire framework to be powerless against assaults and disappointments. Assailants simply need to access to Master server/hub server to access information a HDFS document framework occurrence requires one novel server, the name hub. This is a solitary purpose of disappointment for a HDFS establishment. In the event that the name hub goes down, the document framework is offline and this diminishes the framework's accessibility rate.

The creator's proposed model, the Partially Distributed File System with Parity Chunks, addresses every one of the three parts of security, including Confidentiality, Integrity, and Accessibility (CIA). The model is structured in a manner that is adaptable and adjustable to fit into any condition and a particular client need while keeping the spending limit at an ideal level. Sparing the spending limit simultaneously it supports green innovation; with ideal number of record servers.

For future development of this environment, a script that captures the alerts based on their priority and sends them as an email message to the corresponding email address will be advantageous. The log file contains the different steps of any attack. Choosing the alert being sent among all the triggered ones based on the severity level instead of sending the whole log file will reduce the time when looking for an evidence. An intrusion detection system must be combined with a network intrusion prevention system, which will identify, stop and report the abnormal traffic.

REFERENCES

[1] Mariana Carroll, Paula Kotzé, Alta van der Merwe. 2012. Securing Virtual and Cloud Environments. In: Cloud Computing and Services Science, Service Science: Research and Innovations in the Service Economy), edited by I. Ivanov et al., DOI 10.1007/978-1-4614-2326-3 4, © Springer Science+Business Media, LLC 2012.

[2] Halton G., Deepak S., (2009), “Cloud Computing Essay”, [Accessed 12-04-2010]: http://www.scribd.com/doc/23743963/Cloud Computing-Essay

[3] Gil P., (2010), “What is Cloud Computing”, [Accessed 01-22-2011]: http://netforbeginners.about.com/od/c/f/cloudcomputing.htm

[4] Web site Admin, (2006). “Software as a Service (SaaS) “, [Accessed 09-25-2010]: http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service

[5] T. Mather, S. Kumarasuwamy and S. Latif, “Cloud Security and Privacy”, O’Rielly, ISBN: 978-0-4596-802769, 2009.

[6] L. M. Kaufman, “Data Security in the World of Cloud Computing”, IEEE Security & Privacy, vol. 7, no. 4, 2009.

[7] M. Dieye, M. F. Zhani, H. Elbiaze, "On achieving high data availability In heterogeneous cloud storage systems", IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Pgs. 326 - 334, 2017.

[8] Z. Liu, Z. L. Jiang, X. Wang, S. M. Yiu, C. Zhang, X. Zhao, "Dynamic Attribute-Based Access Control In Cloud Storage Systems", IEEE Trustcom/BigDataSE/ISPA, Pgs. 129 - 137, 2016.

[9] W. Li, K. Xue, Y. Xue, J. Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System In Public Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2016.

[10] M. Anisetti, C. Ardagna E. Damiani, F. Gaudenzi, "A semi-automatic and trustworthy scheme for continuous cloud service certification" IEEE Transactions On Services Computing, 2016.

[11] V. Chang, M. Ramachandran, "Towards achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transactions on Services Computing, 2015.

[12] B. Dong, R. Liu, Hui Wang, "Trust-but-Verify: Verifying Result Correctness of Outsourced Frequent Itemset Mining In Data-mining-as-a-service Paradigm", IEEE Transactions on Services Computing, 2015.

[13] S. LIns, P. Grochol, S. Schneider, and A. Sunyaev, "Dynamic Certification of Cloud Services: Trust, but Verify", IEEE Computer and Reliability Societies, 1540-7993/16, 2016.

[14] T. Noor, Q. Sheng, L. Yao, S. Dustdar and A. Ngu. "CloudArmor: Supporting Reputation-based Trust Management for Cloud Services", IEEE transactions on parallel and distributed systems, Vol. 27, no. 2, Pgs. 367-380, 2015.

[15] M. Xiao, M. Wang, X. Liu, and J. Sun, "Efficient distributed access control for big data in clouds", Proc. - IEEE INFOCOM, vol. 20, no. BigSecurity, pp. 202-207, 2015.

[16] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, A. Y. Zomaya, "An Efficient Privacy-Preserving Ranked Keyword Search Method", IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 4, 2016.

[17] J. K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System", IEEE Transactions on Computers, 2015.

[18] T. Yang, P. Shen, X. Tian, C. Chen, "A Fine-Grained Access Control Scheme for Big Data Based on Classification Attributes", IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) Pgs. 238 - 245, 2017.

[19] S. Wang, K. Liang, Joseph K. Liu, J. Chen, JianpIng Yu, W. Xie, "Attribute-Based Data Sharing Scheme Revisited In Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol. 11, 2016.

[20] A. Bonguet and M. Bellaiche, "A survey of Denial-of- Service and Distributed Denial of Service attacks and defenses in cloud computing", Future Internet, vol. 9, no. 3, 2017.

[21] T. Pasquier, J.Singh, J. Powles, D. Eyers, M. Seltzer, J. Bacon, "Data provenance to audit compliance with the privacy policy in the Internet of Things Personal and Ubiquitous Computing", Vol. 22, pp 333-344, 2018.

[22] S.Subbalakshmi , Dr. K.Madhavi, “Security challenges of Big Data storage in Cloud environment: A Survey” International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 17 (2018) pp. 13237-13244