International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

A Systematic Review Paper on Cloud Security

Kirti Sharma*, Bharti Nagpal
CSE, AIACT & R, GGSIPU, Delhi, India

ABSTRACT

Cloud computing is a rising method for processing in software engineering. It expands different registering systems like framework figuring, dispersed processing. Today cloud computing is utilized as a part of both mechanical field and scholarly field. Cloud encourages its clients by giving virtual assets by means of web. As the field of cloud computing is spreading the new systems are creating. This expansion in cloud processing condition likewise expands security challenges for cloud engineers. Clients of cloud spare their information in the cloud subsequently the absence of security in cloud can lose the client's trust. This paper presents a systematic review on different cloud security issues with their respective pros and cons and imparting the existing methodologies done by the researchers for cloud security.

Keywords : Cloud Security, Saas, Paas, And Iaas, Virtual Assets, Cloud Computing, Hadoop, Cryptography File Systems, HDFS System

I. INTRODUCTION

Security in conveyed processing is a critical concern. Data in cloud should be secured fit as a fiddle. To bind client from getting to the common data direct, mediator and lender organizations should be used. Cloud computing is an arrangement of assets and administrations that are offered by the system or web. Cloud computing broadens different figuring methods like framework processing, circulated registering. Today cloud computing is utilized as a part of both mechanical field and scholarly field. Cloud encourages its clients by giving virtual assets by means of web. Conveyed registering and limit outfits customers with capacities to store and process their data in untouchable server ranches.

Associations utilize the cloud in a wide range of administration models (with acronyms, for example, SaaS, PaaS, and IaaS) and arrangement models (private, public, hybrid, and community). Security concerns related with distributed computing fall into two general classes: security issues looked by cloud suppliers and security issues looked by their clients. The supplier must guarantee that their framework is secure and that their customers information and applications are ensured, while the client must take measures to invigorate their application and utilize solid passwords and validation measures. Cloud security considers mainly two factors better defense as shown in fig. 1 below.

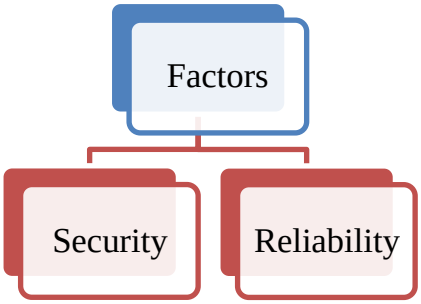

Figure 1. Factors of cloud security

II. ELEMENTARY STUDY MATERIAL

Cloud computing is an arrangement of existing procedures and advances, bundled inside another foundation worldview that offers enhanced adaptability, flexibility, business nimbleness,

speedier startup time, lessened administration costs, and in the nick of time accessibility of assets.

1. **Features:**
- ✓ Use of web based administrations to help business process.
- ✓ Rent IT-benefits on an utility-like premise.

2. **Properties:**
- ✓ Rapid organization
- ✓ Low startup costs/capital speculations
- ✓ Costs in view of utilization or membership
- ✓ Multi-occupant sharing of administrations/assets

3. **Basic qualities:**
- ✓ On request self-benefit
- ✓ Ubiquitous arrangement
- ✓ Location autonomous asset pooling
- ✓ Rapid versatility
- ✓ Measured benefit

4. **Cloud models:**
   a. **Delivery Models-**
   - ✓ SaaS
   - ✓ PaaS
   - ✓ IaaS

   b. **Deployment Models:-**
   - ✓ Private cloud
   - ✓ Community cloud
   - ✓ Public cloud
   - ✓ Hybrid cloud

III. SURVEY OF CLOUD SECURITY CONCERN

A survey as shown in table 1 listing various methodologies that were proposed by various authors via executing different algorithms in previous years. Table includes the pros and cons regarding with each proposed algorithm.

TABLE 1
SURVEY OF CLOUD SECURITY CONCERN

S.No	Year	Author	Proposed Algorithm(s)	Pros	Cons
1.	2015	Primoz cigoj [13]	SSO(Single Sign On) Approach	Unified access point of a management in cloud and a secure strong Authentication.	It attempts to remove some vulnerability only. It need more flexible, secure interfaces, control of the user data & privacy and not focusing in the technology development
2.	2015	R.Tamilaras I [14]	DIM's(Data and Image Mechanism) Three-tier Architecture used in partitioning method.	Data security, Authentication, confidentiality, prevents data leakage, CSA.	Only the suitable data is valid for this mechanism not for all type of data.

3.	2016	Varsha&D. Mali [15]	Cryptographic RBDAC Trust Mechanism.	Security for user's to determine the individual role.	For Dynamic decision making trust evaluation is done.
4.	2016	Punam V.Maitri & Aruna Verma [16]	LSB Steganography technique combined with AES,RC6,Blowfish & BRA Algorithm	Key information security, data integrity, low delay, authentication, confidentiality are considered. Try to accomplish high level security using hybridization of public key cryptography algorithms	Not available high level security and this algorithm need 10%-12% less time respect o the blowfish algorithm.
5.	2016	J.Mahalaksh mi and K.Kuppusa my [17]	Security-as-a-Service for files in Cloud Computing	An application model is developed that encrypts sensitive data and works well against cryptanalytic attacks	Key size is limited and limited parameters are verified.
6.	2017	Malik Irkain [18]	Comprehensive classification.	Verify data location, assumptions regarding CSP behavior.	Addresses only landmark based approaches.
7.	2017	Noelle Rakotondra vony [19]	VMI-based Mechanism's.	Invention of target & direction of attacks, providing the statistical analysis of the report.	Briefs the issues and lack on solutions.
8.	2017	Rongzhi wang [20]	Data Secure Storage based on Tornado Codes (DSBT).	Solve the problem of data tampering.	It brings series of negative issues, data security issues detection &retrieve in the data availability.
9.	2018	Husna Tariq and	Fuzzy keyword	Improve information	Faced problem while

		Parul Agarwal [21]	searching scheme and Coordinated symmetric and asymmetric encryption algorithms	security and enhance the security framework and shield sensitive client's information from unauthorized exposure.	decrypting data by utilizing wild card technique.
10.	2017	Iqjot Singh, Prerna Dwivedi, Taru Gupta and P. G. Shynu [22]	Hashing on Hadoop in big-data	Ensure security while uploading and downloading files. Access files faster and with the help of encryption technology the data stored in the HDFS is safe and secure.	Lacks whenever someone become able to crack the security and view the data, moreover for searching a normal file in data in HDFS system
11.	2017	Mauro Storch, César A. F. de Rose [23]	Cryptography File Systems (CFS) adoption	The model is verified in a real scenario for estimating the total cost when adding security for storage in a cloud environment. It is used to estimate the overhead of a CFS hosting files of an application execution (based on Big Data operations) and the model predictability accuracy was close to 90%.	Not accounting the throughput, cache hierarchy and synchronization mechanisms.
12.	2017	Narander Kumar and Priyanka Chaudhary [24]	Hashing Approach and Rail Fence Technique	Use of bcrypt hashing and rail fence transposition method for password security. It upgrades the security, diminishes the issues	Chances of brute force attack.

				of cyber stalking.	
13.	2017	Ioram S. Sette, David W. Chadwick and Carlos A. G. Ferraz [25]	Accounts with multiple cloud providers	Authorization Policy Federations allow policies to be defined and stored in a common ontology in DNF, and managed from a central PAP, named FAPManS.	Cannot preserve the semantics of the explicit deny rules.
14.	2018	Mylara Reddy Chinnaiah [26]	Fault Tolerant Technique IFrFT(Frequency of Configuration interactions), ChIFrFT (Characteristics & Frequency if interactions).	It achieves reliability & fault tolerance of a software system in a cost efficiency and it is better than NOFT Scheme	Percentage of successful interactions are low(25 & 40%).
15.	2018	Ahmed Nour Moussa [27]	CFaaS Model.	Consumers & providers independently collect, verify the equity of forensic analysis resolve collected results.	Independently collect, verify the equity of forensic analysis resolve collected results. Suitable forensic analysis is not available for accessing the forensic data directly.

IV. CONCLUSION

This paper portrays a portion of the cloud ideas, properties and its elementary material. As the cloud computing is dynamic and complex, the conventional security arrangements gave by cloud condition do not delineate to its virtualized surroundings. This paper described a systematic review on different cloud security issues imparting the existing methodologies done by the researchers for cloud security.

V. REFERENCES

[1] NIST (Authors: P. Mell and T. Grance), "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology Laboratory (October 7 2009).

[2] J. McDermott, (2009) "Security Requirements for Virtualization in Cloud Computing," presented at the ACSAC Cloud Security Workshop, Honolulu, Hawaii, USA, 2009.

[3] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." arXiv preprint arXiv:1609.01107 (2016).

[4] Kalaiprasath, R., R. Elankavi, and Dr R. Udayakumar. "Cloud. Security and Compliance-A Semantic Approach in End to End Security." International Journal Of Mechanical Engineering And Technology (Ijmet) 8.5 (2017).

[5] McGee, Pat. C# 5.0: A Beginner's Guide. McGraw-Hill Education, 2015.

[6] slideplayer.com/slide/9476015/

[7] bigdata-madesimple.com/5-advantages-and-disadvantages-of-cloud-storage/

[8] computer.howstuffworks.com/cloud-computing/cloud-storage3.htm

[9] fac.ksu.edu.sa/sites/default/files/chapter_6._fundamental_cloud_security.pdf

[10] https://www.slideshare.net/InderBarara1/security-issues-and-challenges-in-cloud-computing

[11] sciencedirect.com/science/article/pii/S1361372318300058

[12] https://arxiv.org/ftp/arxiv/papers/1403/1403.5627.pdf

[13] Cigoj, Primož, and Borka Jerman Blažič. "An authentication and authorization solution for a multiplatform cloud environment." Information Security Journal: A Global Perspective 24.4-6 (2015): 146-156.

[14] Tamilarasi, R., S. Prabu, and P. Swarnalatha. An Approach for Data and Image Security in Public Cloud using Segmentation and Authentication (CSA) Protocol Suite. MAGNT Research Report 2015. 133-141.

[15] VarshaD.Mali,Prof.Pramod Patil,"Authentication and Access Control for Cloud Computing using RBDAC Mechanism", in International Journal of Innovative Research in Computer and Communicationngineering,vol.4,Issue11,Nov2016,DOI:10.15680/IJIRCCE.2016.

[16] Punam V.Maitri ,Aruna verma ,"Secure File Storage in Cloud Computing using Hybrid Cryptography Algorithm",in IEEE explore on WiSNET Conference, Sep 2013,DOI:10.1109/WiSPNET.2016.7566416.

[17] J.Mahalakshmi and K.Kuppusamy, "Security-As-A-Service for files in Cloud Computing-A Novel application Model", IEEE Digital Xplore, DOI: 10.1109/ISCO.2016.7726889, November 2016, pp: 1-5, IEEE.

[18] Irain, Malik, Jacques Jorda, and Zoubir Mammeri. "Landmark-based data location verification in the cloud: review of approaches and challenges." Journal of Cloud Computing 6.1 (2017): 31.

[19] Rakotondravony, Noëlle, and Hans P. Reiser. "Visualizing and Controlling VMI-based malware analysis in IaaS Cloud." Reliable Distributed Systems (SRDS), 2016 IEEE 35th Symposium on. IEEE, 2016.

[20] Wang, Rongzhi. "Research on Data Security Technology Based on Cloud Storage." Procedia engineering 174 (2017): 1340-1355.

[21] Tariq, Husna, and Parul Agarwal. "Secure keyword search using dual encryption in cloud computing." International Journal of Information Technology: 1-10.

[22] Singh, Iqjot, et al. "Enhanced K-means clustering with encryption on cloud." IOP Conference Series: Materials Science and Engineering. Vol. 263. No. 4. IOP Publishing, 2017.

[23] Storch, Mauro, and César AF De Rose. "Cloud Storage Cost Modeling for Cryptographic File Systems." Parallel, Distributed and Network-based Processing (PDP), 2017 25th Euromicro International Conference on. IEEE, 2017.

[24] Kumar, Narander, and Priyanka Chaudhary. "Diminishing Cyber stalking and Cyber bullying Issues using a Hashing Approach and Rail Fence Technique."

[25] Sette, Ioram S., David W. Chadwick, and Carlos AG Ferraz. "Authorization Policy Federation in Heterogeneous Multicloud Environments." IEEE Cloud Computing 4.4 (2017): 38-47.

[26] Chinnaiah, Mylara Reddy, and Nalini Niranjan. "Fault tolerant software systems using software configurations for cloud computing." Journal of Cloud Computing 7.1 (2018): 3.

[27] Moussa, Ahmed Nour, Norafida Ithnin, and Anazida Zainal. "CFaaS: bilaterally agreed evidence collection." Journal of Cloud Computing 7.1 (2018): 1.

[28] Attrapadung, Nuttapong; Herranz, Javier; Laguillaumie, Fabien; Libert,Benoît; de Panafieu, Elie; Ràfols, Carla (2012-03-09). "Attribute-based encryption schemes with constant-sizeciphertexts" Computer Science. 22: 15–38. doi:10.1016/j.tcs.2011.12.004.

[29] "Cloud Security Front and Center" (http://blogs.forrester.com/srm/2009/11/cloud-security-front-and-center.html). Forrester Research. 2009-11-18. Retrieved 2010-01-25.

[30] Wang, Huang He, Yuan, Liu Xiao, Xi, Xu Jing, Min, "Open Identity Management Framework for SaaS Ecosystem," in ICEBE '09. pp. 512-517.

[31] Aizat Azmi, Ahmad Amsyar Azman, Sallehuddin Ibrahim, and Mohd Amri Md Yunus, “Techniques In Advancing The Capabilities Of Various Nitrate Detection Methods: A Review”, International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 223-261.