© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Brief Review on Cloud Security Scenarios

C. Kaleeswari*, P. Maheswari, Dr. K. Kuppusamy, Dr. Mahalakshmi Jeyabalu
*Department of Computer Science, Alagappa University, Karaikudi, Tamil Nadu, India

ABSTRACT

Today cloud computing is the most promising technology that allows the users to access the data from anywhere despite of storage issue. It is a public environment for sharing resources, as services via the internet. It provides a high security, virtualization, abstraction, online storage and scalability. Its applications were widely employed both in business and academics. Cloud computing focus mainly on three types of services viz SaaS, PaaS and IaaS. Security issues are with increase in use of cloud. Some security aspects such as multi-tenancy, flexibility, loss of control, loss of data, hacker attacks like irtual threats predominantly gets attention. This paper will picturize a brief view of the current cloud security challenges and risks and also imparting the existing methodologies done by the researchers for cloud security. It is specially suggested as suitable for beginners pursuing their research in cloud security domain to find the basic research problems regarding security and issues found in cloud security.

Keywords : Cloud Computing, Cloud Security, Authentication, Authorization, Risks and Issues.

I. INTRODUCTION

Cloud computing is a promising technology for on-demand internet computing[2]. Its applications and the act of services can run on distributed network, without interference. It provides the advantages to users in aspects of usability, bandwidth, scalability, low-cost, accessibility, backup and recovery, storage capacity, integrating the automatic software and ease of access[5]. Cloud storage is a scalable path to store, access, and transmit the data across the internet. Cloud service providers have their own connected network for hardware and software, while the need of web applications is a Prerequiste. Using the cloud storage platform, management costs of purchasing and maintaining own storage infrastructure lowers considerably and offers global measure considerably.

Cloud computing focus mainly on three types of services viz software, infrastrucutre and Platform. Rather than that various other services such as Database, Encryption, and Security is also a types of services being offered by the Cloud Environment. SaaS focused on user's demands, automatic updates of a softwares and all applications. PaaS provides the database, predefined applications and components[1]. IaaS offers physical data tools(servers, storage, internet…) without purchasing. Cloud storage requirements are durable, with two most important factors likely availability and security. Security issues are increasing with the increase in cloud service usage[6][7].Authorization and authentication plays the major role for security. Authentication is the process of secure the data for user's data protection. Access control plays the major role for data privacy[1]. It can be used to distinguish the privileges, for accessing the data resided in Cloud. Cloud storage was classified into three categories such as object storage, file storage and block storage.

This paper elaborates a breif overview of the cloud security challenges and risks along with the existing methodologies done by the researchers for cloud security.Section 1 shows the basics of Cloud Computing and Cloud Secutiy, issues and risks related to the Cloud Security. Section 2, in detail tabularizes

the recent research work done on the secutiy issues in Cloud Computing with Pros and Cons. Section 3, brings a conclusion to the study done.

II. A SURVEY ON CLOUD SECURITY ISSUES

Table 1. A Survey On Cloud Security Issues

S.No	Year	Author	Proposed Algorithm(s)	Pros	Cons
1.	2011	S.C.Wang et.al.,[3]	Group Key Authentication protocol(GKA)	Concentrates on Authentication time. By this appraoch data traffic is considerable minimized and Quality of Service increased.	Eventhough the Qos increased the Method relics poor scalability, an important component of Cloud Computing.
2.	2013	D.Ranjith et.al.,[10]	Cloud Secaas Model	An Service-Oriented mehod was explained which operates with efficient scalablility, Interoperabliity, in LooselyCoupled systems and also enhances abstraction.	The identity services of this approach remains only two, that was not enough when there is a growth in scalability.
3.	2013	Umer Khalid et.al.,[15]	Authentication & Authorization protocol.	Providing the authenticated access and authorized communication in cloud using the protocol and assign privilieges.	It includes identity theft, data leakage and also integrated with the existing identity management systems.
4.	2013	Vishal Paranjape et.al.,[21]	Mobile One Time Password Authentication Algorithm.	Use of time based OTP's, generates passwords within a certain time interval.	Absence of standard privacy and security techniques.
5.	2013	Jun Hu et.al.,[18]	MAC Acces Control Mechanism	Provides the necessary technical & management strategies, Security of data accessing with new Access control mechanism end in controlled accessing of data by authorized users.	Security protocol has become the key issues.
6.	2013	Iehab AL Rassan et.al.,[22]	Fingerprint Authentication Mechanism.	Providing the security enhancement in mobile, increasing the performance level.	Reduced level of security in authorizatrion.
7.	2013	D.Chandra mohan et.al.,[23]	Petri-net Privacy Preserving Framework(PPPF).	Safeguarding user's privacy, providing consistency & breach-less services.	Some security standards are Not available that leads to issues.
8.	2014	Nitin Nagar &Pradeep K. Jatav et.al.,[25]	LDAP Authentication Mechanism.	Protect user's data and providing the secure framework.	Not focused in different cloud computing tools for implementation.
9.	2014	Younis A.Younis et.al.,[20]	Novel Access Control Model.	Access requirements is dynamic, easy to handle and it is better than MAC and RBAC.	It has to perform high time & huge space complexity is also found.
10.	2014	Ahmad Almulhem et.al.,[16]	Simple graphical authentication system.	MFA in a friendly intuitive system, combines graph & text-based passwords.	Progress on Authorization is considered in minimal level.

11.	2015	Primoz cigoj et.al.,[17]	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.
12.	2015	R.Tamilarasi et.al.,[24]	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.
13.	2016	JyothikaChhetiza et.al.,[1]	MFA(Multi Factor Authentication).	Provides the additional layers of security & verification.	So complex, little expensive for naïve users,and this mechanism differs between vendors.
14.	2016	Varsha&D. Mali et.al.,[8]	Cryptographic RBDAC Trust Mechanism.	Security for user's to determine the individual role.	For Dynamic decision making trust evaluation is done.
15.	2016	Punam V.Maitri & Aruna Verma Et.al.,[12]	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.
16.	2017	Malik Irkain et.al.,[14]	Comprehensive classification.	Verify data location, assumptions regarding CSP behavior.	Addresses only landmark-based approaches.
17.	2017	Noelle Rakotondravony et.al.,[26]	VMI-based Mechanism's.	Invention of target & direction of attacks, providing the statistical analysis of the report.	Briefs the issues and lack on solutions.
18.	2017	Rongzhi wang et.al.,[19]	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.
19.	2018	Mylara Reddy Chinnaiah et.al.,[13]	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%).
20.	2018	Ahmed Nour Moussa et.al.,[27]	CFaaS Model.	Consumers & providers independently collect,verify the equity of forensic analysis resolve collected results.	Suitable forensic analysis is not available for accessing the forensic data directly.
21	2018	J.Mahalakshmi and K.Kuppusamy [28]	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.

III. CONCLUSION

Cloud Computing paradigm, and their basic security concepts are breifly explained in this research work. This paper also inludes, various security mechanisms used for the data protection, in cloud computing done by various researchers all over the world. This breif survey paper, remains as a solution for the researchers who are in their beginning phase of the research about cloud security. This paper describes some of the cloud concepts and demonstrates the cloud components such as scalability, platformindependent, low-cost, flexibility and reliability.

IV. REFERENCES

[1]. Jyothikachhetiza,Nagendrakumar,"Emerging security issues and Authentication Mechanism in cloud environment with focus on Multifactor Authentication",in IJARCSSE International Journal of Advanced Research in Computer Science and Software Engineering,Vol .6,Issue 5,May 2016,ISSN:2277 128X.

[2]. Garima gupta P.RLaxmi,Shubhanjali Sharma,"Survey on Cloud Security Issues and Techniques"2011.

[3]. S.C.Wang,M.L,Chiang,K.Q.Yan,S.S.Wang,S.H.Tsai,"A New Group Key Authentication protocol in an insecure cloud computing environment",in International conference on Advanced Information Technologies(AIT),2011.

[4]. Huihui yang, VladamirA.Oleshchuk,"A Dynamic Attribute-Based Authentication Scheme",in Springer International Publishing Switzerland,DOI:10.1007/978-3-319-18681-8-9,pp.106-118,2018.

[5]. S.Ziyad,S.Rehman ," Critical Review of Authentication Mechanisms in Cloud Computing" ",in IJCSI International Journal Of Computer Science Issues,vol.11,Issue 3,No.1,May 2014.

[6]. Dr.NileshMahajan,Mrs.Devyanipatil,"Study of Authentication and Authorization in Cloud Computing",in International Journal on Recent and Innovation Trends in Computing and Communication,Vol.4,Issue 7,ISSN:2321-8169178-180,July 2016.

[7]. Dr.R.Sridevi,Vasavi Bande,"Comparative Study of Various Existing Security Scenarios in Cloud Computing Environment",in JGRCS Journal of Global Research in Computer Science, vol.3,No.9,September 2012,ISSN:2229-371X.

[8]. 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.

[9]. Ranjit Bose,Xin(Robert) Luo,Yuan Liu,"Roles of Security and Trust :Comparing Cloud Cloud Computing and Banking",in Elsevier on Sciverse ScienceDirect Procedia Social and Behavioral sciences,2013,DOI:10.1016/j.sbspro.201302.015.

[10]. D.Ranjith,.Srinivasan," Identity Security Using Authentication and Authorization in Cloud Computing"in International Journal of Computer & Organization Trends,Vol.3,Issue 4,May 2013,ISSN:2249-2593

[11]. Ronald L.Krutz ,Russell Dean Vines, "CLOUD SECURITY-A Comprehensive Guide to Secure Cloud Computing".

[12]. 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.

[13]. Mylara Reddy , ,Nalini Niranjan,"Fault Tolerant Software Systems using Software Configurations for Cloud Computing",in Springer on Journal of Cloud Computing :Advances Systems and Applications ,2018,DOI:10.1186/s13677-018-0104-9.

[14]. Malik Irain,Jacques Jorda,Zoubir Mammeri,"Landmark-based data location verification in the Cloud :Review of approaches and Challenges",in Springer on Journal of Cloud Computing,Dec 2017.

[15]. Umer Khalid,Misbah Irum,Muhammad Awais Shibli,"Cloud based Secure and Privacy Enhanced Authentication and Authorization Protocol",in Elsevier on ScienceDirect,Vol.22,2013,DOI:10.1016/j.procs. 2013.09.149,pp:680-688.

[16]. Ahmed Almulhem,"A Graphical Password Authentication System",in IEEE explore on Researchgate, Apr 2011.

[17]. Primoz Cigoj,Borka Jerman Blazic,Tomaz Klobucar,"An Authentication and Authorization Solution for a Multiplatform Cloud Environment",in Researchgate on Information Security Journal A Global Perspective,Aug 2015, DOI:10.1080/19393555.2015.1078424.

[18]. Jun Hu,Lei chen,Yunhua wang,Shi-hong chen,"Data Security Access Control Model of Cloud Computing", in IEEE explores International Conference on Computer Sciences and Applications,2013,DOI:10.1109/CSA.2013.15.

[19]. Rongzhi Wang ,"Research on data security Technology based on Cloud Storage", in Elsevier on Procedia Engineering,Vol.174,2017,DOI:10.1016/j.proeng .2017.01.286,pp:1340-1355.

[20]. Younis A.Younis,Kashif kifayat,Madjd merabti,"An Access Control Model for Cloud Computing",in Elsevier,Vol.19,Issue 1,Feb 2014.

[21]. Vishal paranjape,Vimmi pandey,"An Improved Authentication Technique with OTP in Cloud Computing",in International Journal of Scientific Research in Computer Science and Engineering,Vol.1,Issue 3,June 2013,E-ISSn:2320-7639.

[22]. Iehab AL Rassan,Hanan Al Shaher,"Secure Mobile Cloud Computing using Biometric Authentication", in IEEE explore on Academy and Industry Research Collaboration Center(AIRCC),Vol.5,Issue 6,pp:41.

[23]. D.chandramohan,.Vengattaraman,D.Rajaguru,P. Dhavachelven"A New Privacy Preserving Technique for Cloud Service User Endorsement using Multi-agents",in Sciencedirecton Journal of King Saud University-Computer and Information Sciences,Vol.28,Issue 1,Jan 2016,pp:37-54DOI:10.1016/j.jksuci.2014.06.018.

[24]. Tamilarasi R,Prabhu S,Swarnalatha P,"An Approach for Data and Image Security in Public Cloud using Segmentation and Authentication(CSA) Protocol Suite",in MAGNT Research Report,Vol.3(8),pp:133-141,2015,DOI:dx.doi.org/14.9831/1444-8939.2015/3-8/MRR.05.

[25]. Nitin nagar,Pradeep K.Jatav,"A Secure Authenticate Framework for Cloud Computing Environment",in GoogleScholar on International Journal of Advanced Computer Research(IJACR),Vol.4,No.14,2014,pp:266-271.

[26]. Noelle Rakotondravony,Hans P.Reiser," Visualizing and Controlling VMI-Based Malware Analysis in IaaS Cloud",in IEEE explore on 35th Symposium on Reliable Distrbuted Systems,2017,DOI:10.1109/SRDS.2016.33.

[27]. Ahmed Nour Moussa,Norafida ithnin,Anazida zainal,"CFaaS:bilaterally Agreed Evidence Collection",in Springer on Journal of Cloud Computing Advances,Systems and Applications,Jan 2018,DOI:https://doi.org/10.1186.

[28]. 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.